Practice Test - 2 - Results

Collapse all questions

● **Question 1** Skipped

The ability to provision and deprovision cloud resources quickly, with minimal management effort, is known as ________.

Correct answer

○ **Scalability**

Explanation

Scalability is the correct choice as it specifically refers to the ability to quickly provision and deprovision cloud resources with minimal management effort. It allows organizations to easily adjust resource capacity to meet changing demands, making it a key factor in efficient cloud resource management.

○ **Elasticity**

Explanation

Elasticity refers to the ability of a system to automatically adjust resources based on workload fluctuations. While it is related to provisioning and deprovisioning resources, it focuses more on the dynamic nature of resource allocation rather than the speed and management effort involved in the process.

○ **Resiliency**

Explanation

Resiliency is the ability of a system to recover and continue operating in the face of disruptions. While it is an important aspect of cloud infrastructure, it is not directly related to the quick provisioning and deprovisioning of resources with minimal management effort.

○ **Sustainability**

Explanation

Sustainability refers to the environmental impact and long-term viability of resource usage. While sustainability is an important consideration in cloud computing, it is not directly related to the speed and ease of provisioning and deprovisioning resources.

Overall explanation

The correct answer is Scalability. It specifically refers to the ability to provision and deprovision cloud resources quickly and with minimal management effort.

Other options -

- **Resiliency:** It refers to the ability of a system to recover quickly from failures or disruptions. While resiliency is an important attribute of cloud systems, it is not specifically related to the ability to provision and deprovision resources quickly.
- **Elasticity:** It is the ability of a system to scale up or down in response to changes in demand. This is a closely related concept to scalability, but specifically refers to the ability to handle changes in workload or traffic.
- **Sustainability:** It refers to the ability of a system to operate in an environmentally friendly manner, with minimal impact on the planet. While sustainability is an important consideration for cloud providers, it is not specifically related to the ability to provision and deprovision resources quickly.

Reference: https://learn.microsoft.com/en-us/azure/architecture/framework/scalability/design-scale

Domain

Describe cloud concepts (25–30%)

● **Question 2** Skipped

After a junior admin inadvertently provisions oversized VMs, leaves unused disks in place, and neglects to patch a security vulnerability, your Azure bill sees a significant spike. A tool provides insights and recommendations, suggesting actions such as resizing VMs, cleaning up unused resources, and addressing security gaps. Which of Azure Advisor's recommendations are relevant in this situation? (Select all that apply.)

Which of the following Azure Advisor features are involved in this scenario?

□ **Performance, recommending improvements to overall system efficiency**

Explanation

Performance recommendations from Azure Advisor aim to improve overall system efficiency, which may not directly address the specific issues of oversized VMs, unused disks, and security vulnerabilities impacting the Azure bill. Therefore, this recommendation may not be as relevant in this situation compared to Cost Optimization and Security recommendations.

Correct selection

□ **Security, advising on patching vulnerabilities and improving security posture**

Explanation

Security recommendations from Azure Advisor are crucial in this situation as they advise on patching vulnerabilities and improving the overall security posture. This directly addresses the issue of neglecting to patch a security vulnerability, which has led to the spike in the Azure bill.

Correct selection

□ **Cost Optimization, recommending resizing VMs and eliminating unused resources**

Explanation

Cost Optimization is relevant in this scenario as it provides recommendations on resizing VMs to reduce costs and eliminating unused resources to optimize spending. This aligns with the situation where oversized VMs and unused disks are contributing to the significant spike in the Azure bill.

□ **High Availability, ensuring minimal downtime by optimizing VM deployment**

Explanation

High Availability recommendations focus on ensuring minimal downtime by optimizing VM deployment, which is not directly related to the issues of oversized VMs, unused disks, and security vulnerabilities causing the spike in the Azure bill. Therefore, this recommendation is not relevant in this scenario.

Overall explanation

1. **Cost Optimization**: This is the correct answer because Azure Advisor's **Cost Optimization** recommendations help identify opportunities to reduce costs, such as resizing or shutting down underutilized VMs and deleting unused disks.

2. **Security**: This is also correct because **Security** recommendations in Azure Advisor focus on improving the security of the environment by suggesting actions such as patching vulnerabilities, which directly applies to the situation described.

3. **High Availability**: While **High Availability** recommendations are valuable for ensuring uptime, this feature does not directly address cost reduction or security in this scenario.

4. **Performance**: **Performance** recommendations aim at optimizing the efficiency of resources but do not directly address the issues of cost control or security in the scenario provided.

Domain

Describe Azure management and governance (30–35%)

Question 3 Skipped

An Azure ________________ is a connection between two Azure Regions within the same geographic region for disaster recovery purposes.

○ Geography

○ Region

○ Availability Zone

Correct answer

○ **Region Pair**

Overall explanation

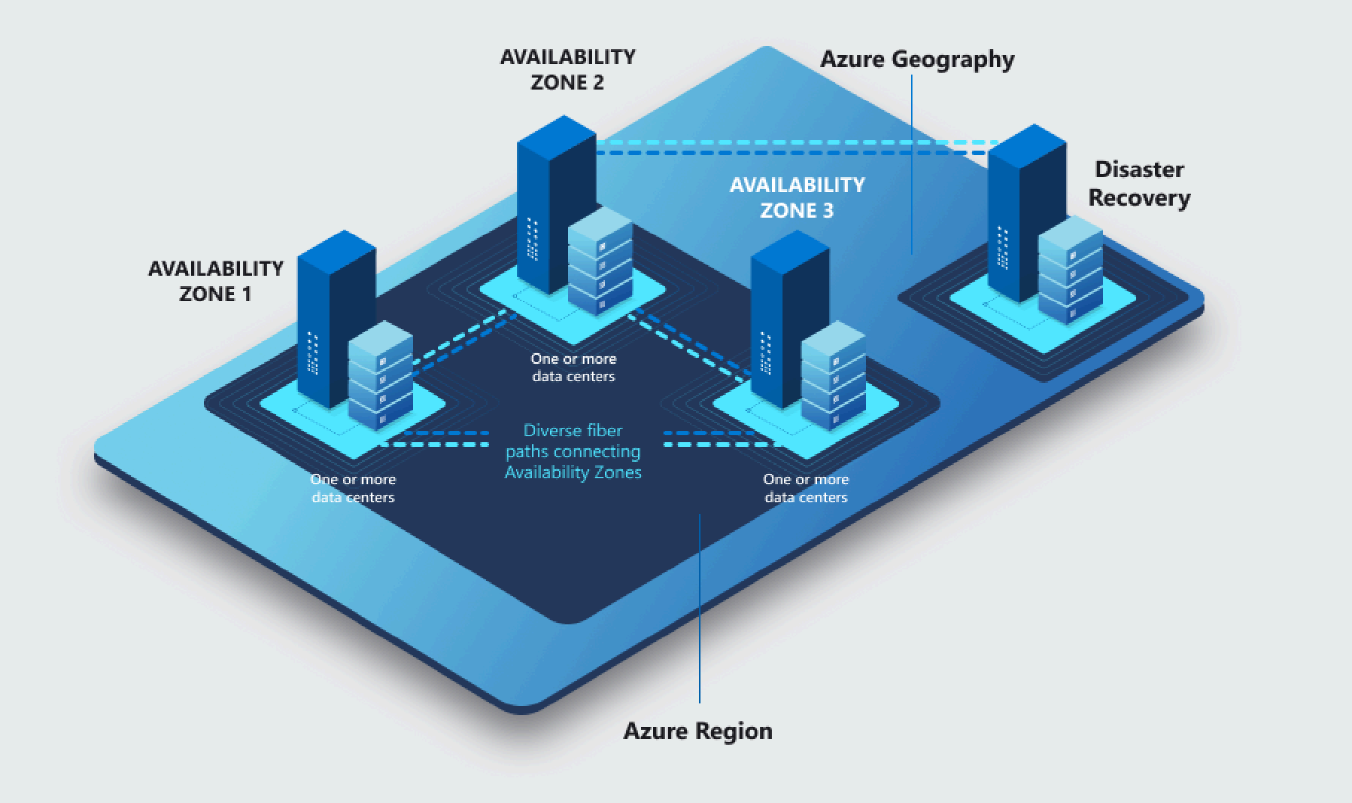
From the Official Azure Documentation:

Regional Pairs are 2 connected Azure Regions for Disaster Recovery within the **same Geography.**

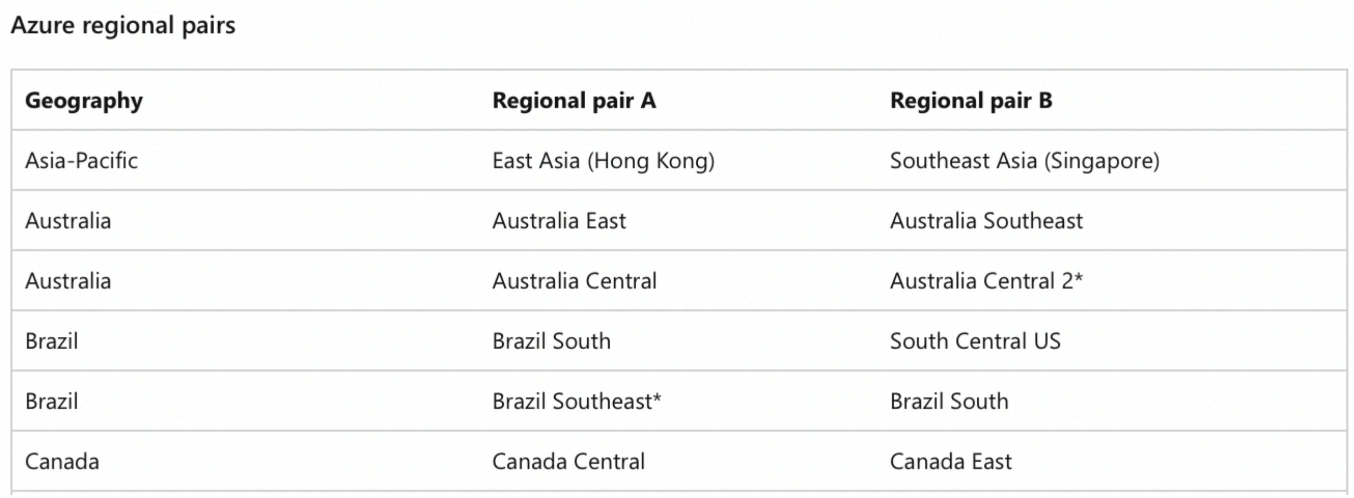
Many organizations require both high availability provided by availability zones that are also supported with protection from large-scale phenomena and regional disasters. As discussed in the resiliency overview for regions and availability zones, Azure regions are designed to offer protection against local disasters with availability zones. But they can also provide protection from regional or large geography disasters with disaster recovery by making use of another region that uses ***cross-region replication*.**

To ensure customers are supported across the world, Azure maintains multiple geographies. These discrete demarcations define a disaster recovery and data residency boundary across one or multiple Azure regions.

Cross-region replication is one of several important pillars in the Azure business continuity and disaster recovery strategy. Cross-region replication builds on the synchronous replication of your applications and data that exists by using availability zones within your primary Azure region for high availability. Cross-region replication asynchronously replicates the same applications and data across other Azure regions for disaster recovery protection.



Example -



Azure regional pairs

Geography	Regional pair A	Regional pair B
Asia-Pacific	East Asia (Hong Kong)	Southeast Asia (Singapore)
Australia	Australia East	Australia Southeast
Australia	Australia Central	Australia Central 2*
Brazil	Brazil South	South Central US
Brazil	Brazil Southeast*	Brazil South
Canada	Canada Central	Canada East

Reference: https://docs.microsoft.com/en-us/azure/availability-zones/cross-region-replication-azure

Domain

Describe Azure architecture and services (35–40%)

Question 4 Skipped

A startup builds an app with lightweight, dependency-bundled compute units for microservices and event-driven code snippets that execute without server management. Which Azure compute options are they using? (Select all that apply.)

□ **Availability Sets**

Explanation

Availability Sets are used to ensure high availability of virtual machines by distributing them across multiple physical servers. They are not relevant to the scenario described in the question, which focuses on lightweight, serverless compute options for microservices and event-driven code snippets.

Correct selection

□ **Azure Functions**

Explanation

Azure Functions enable the startup to run event-driven code snippets without the need for server management. It allows for serverless execution of code in response to events, making it a suitable option for executing lightweight, event-driven code without the overhead of managing servers.

□ **Azure Virtual Desktop**

Explanation

Azure Virtual Desktop is not a suitable option for running lightweight, dependency-bundled compute units for microservices or event-driven code snippets. It is a service that provides virtualized desktops and applications, which is not related to the scenario described in the question.

Correct selection

□ **Azure Container Instances**

Explanation

Azure Container Instances allow the startup to run containers without managing servers. It provides a fast and simple way to run containers in Azure without having to manage the underlying infrastructure, making it a suitable choice for lightweight, dependency-bundled compute units for microservices.

Overall explanation

The correct answers are:

Azure Container Instances
Azure Functions

- **Azure Container Instances**: Azure Container Instances (ACI) is a serverless compute service that enables the deployment of containerized applications without managing virtual machines. It allows for lightweight, isolated environments perfect for microservices and event-driven workloads, aligning with the scenario described where the app uses dependency-bundled compute units.

- **Azure Functions**: Azure Functions is a serverless compute service that lets you run event-driven code snippets without provisioning or managing servers. This fits perfectly with the described scenario where the app uses event-driven code snippets that execute without server management.

Why the other options are incorrect:

- **Azure Virtual Desktop**: Azure Virtual Desktop is a desktop and application virtualization service, not related to the deployment of lightweight compute units or event-driven services. It allows users to access virtual desktops and applications but doesn’t fit the microservice or serverless compute use case described here.

- **Availability Sets**: Availability Sets are used to ensure high availability and fault tolerance of virtual machines (VMs) in Azure. They are not a compute option themselves, but a way of organizing VMs to ensure they are distributed across physical hardware to minimize downtime. Availability Sets are not suitable for the lightweight, serverless, or microservices scenario in the question.

So, the correct compute options in this case are **Azure Container Instances** and **Azure Functions**.

Domain

Describe Azure architecture and services (35–40%)

● **Question 5** Skipped

A firm manages on-premises servers and AWS Kubernetes clusters, applying Azure policies and monitoring them from a single portal. Which Azure feature enables this hybrid management?

○ **Azure Resource Manager**

Explanation

Azure Resource Manager is a management service that allows users to deploy, manage, and organize Azure resources. While it is essential for managing Azure resources, it does not provide the capability to manage on-premises servers or AWS Kubernetes clusters, making it an incorrect choice for enabling hybrid management in this scenario.

○ **Azure Monitor**

Explanation

Azure Monitor is a service for collecting, analyzing, and acting on telemetry data from Azure resources. While it is crucial for monitoring Azure services, it does not provide the capability to manage on-premises servers or AWS Kubernetes clusters, making it an incorrect choice for enabling hybrid management in this scenario.

○ **Azure Cloud Shell**

Explanation

Azure Cloud Shell provides a browser-based shell experience for managing Azure resources. While it is a useful tool for interacting with Azure services, it does not specifically enable hybrid management of on-premises servers and AWS Kubernetes clusters, making it an incorrect choice for this scenario.

Correct answer

○ **Azure Arc**

Explanation

Azure Arc enables organizations to extend Azure management and governance to any infrastructure, including on-premises servers and AWS Kubernetes clusters. It allows for centralized management, policy enforcement, and monitoring from a single Azure portal, making it the correct choice for enabling hybrid management in this scenario.

Overall explanation

The correct answer is: **Azure Arc**

- **Azure Arc**: This is the feature that enables hybrid management of resources. Azure Arc extends Azure's management and governance capabilities to resources that are outside of Azure, such as on-premises servers and resources in other clouds (e.g., AWS). With Azure Arc, you can apply Azure policies, monitor resources, and manage workloads from a single Azure portal, even if those resources are running in different environments.

Other Options:

- **Azure Resource Manager**: This is the management framework for organizing and managing resources in Azure, but it does not extend to managing non-Azure resources (like on-prem or in AWS).

- **Azure Cloud Shell**: This is an integrated, browser-based shell for managing Azure resources. It allows users to run commands, but it does not specifically address hybrid resource management.

- **Azure Monitor**: While Azure Monitor helps with monitoring and tracking the performance of Azure resources, it doesn't extend to managing hybrid or external resources directly. Azure Arc integrates monitoring across hybrid environments.

Domain

Describe Azure management and governance (30–35%)

● **Question 6** Skipped

__________ is made up of one or more datacenters equipped with independent power, cooling, and networking. It is set up to be an *isolation boundary*. If one zone goes down, the other continues working.

○ **Region**

○ **Database racks**

○ **Scale Set**

Correct answer

○ **Availability Zone**

Overall explanation

From the Official Azure Documentation:

What is an Azure region?

An Azure region is a set of datacenters, deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network.

With more global regions than any other cloud provider, Azure gives customers the flexibility to deploy applications where they need. An Azure region has discrete pricing and service availability.

What is an Azure datacenter?

Azure datacenters are unique physical buildings—located all over the globe—that house a group of networked computer servers.

What are Azure Availability Zones?

Azure Availability Zones are unique physical locations within an Azure region and offer high availability to protect your applications and data from datacenter failures. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking.

The physical separation of availability zones within a region protects apps and data from facility-level issues. Zone-redundant services replicate your apps and data across Azure Availability Zones to protect from single points of failure.

Reference : https://docs.microsoft.com/en-us/azure/availability-zones/az-overview

Domain

Describe Azure architecture and services (35–40%)

Question 7 Skipped

Suppose the lead architect in your company has asked your team to implement a IaaS based solution in Azure for a quick Proof-of-Concept (POC) to senior management. One of your colleagues goes ahead and creates an Azure Virtual Network and 3 Azure Virtual machines.

Would you agree with this implementation?

Correct answer

○ Yes

○ No

Overall explanation

Azure Virtual Machines and Azure Virtual Networks both fall under the IaaS category, and therefore this solution would meet the lead architect's ask.

Please refer to this diagram for simplicity.

Reference : https://azure.microsoft.com/en-us/overview/what-is-iaas/

Domain

Describe cloud concepts (25–30%)

● **Question 8** Skipped

A media firm hosts a streaming service in Azure’s West Europe region, ensuring uninterrupted playback by deploying resources across three isolated data centers. A paired region in North Europe holds backups for disaster recovery. Which Azure feature ensures resilience within West Europe?

○ Management Groups

Explanation

Management Groups in Azure are used for organizing and managing Azure resources at scale, providing a way to apply policies and access controls across multiple subscriptions. While useful for governance and management purposes, Management Groups do not directly contribute to ensuring resilience within a specific Azure region like West Europe.

○ **Region Pairs**

Explanation

Region Pairs in Azure are used for disaster recovery purposes, where data and resources are replicated across paired regions for redundancy and failover. While the West Europe region is paired with North Europe for disaster recovery, it does not directly ensure resilience within the West Europe region itself.

○ **Sovereign Regions**

Explanation

Sovereign Regions in Azure refer to regions that are dedicated to specific compliance and regulatory requirements, such as data residency and sovereignty. While important for data governance, Sovereign Regions do not directly contribute to ensuring resilience within a specific Azure region like West Europe.

Correct answer

○ **Availability Zones**

Explanation

Availability Zones in Azure are physically separate data centers within an Azure region that are isolated from each other in terms of power, networking, and cooling. By deploying resources across Availability Zones in West Europe, the media firm ensures high availability and resilience within the region, minimizing the risk of service interruptions.

Overall explanation

The correct answer is: **Availability Zones, isolating resources within West Europe**

Availability Zones are designed to provide **high availability** and **fault tolerance** within a specific **region**, like **West Europe** in this case. Each Availability Zone is a physically separate data center with its own power, cooling, and networking. By deploying resources across **three isolated data centers** (as mentioned in the scenario), the firm ensures that their streaming service remains resilient to failures in a single data center. This isolation within a region helps in minimizing downtime during local failures or outages.

- **Region Pairs**: **Region pairs** provide redundancy by replicating data between two different regions (e.g., **West Europe** and **North Europe**) for **disaster recovery**, but they do not address **resilience within a single region** like the question asks. **Region pairs** are used for cross-region failover, not intra-region isolation.

- **Sovereign Regions**: **Sovereign regions** refer to regions that comply with local regulatory and data sovereignty requirements. They don't directly provide **resilience** within the region.

- **Management Groups**: **Management Groups** are used to organize and manage Azure subscriptions and policies at scale across regions. They do not provide infrastructure resilience or availability.

Domain

Describe Azure architecture and services (35–40%)

Question 9 Skipped

______________ copies your data synchronously three times within a single physical location in the primary region.

Correct answer

○ **Locally redundant storage (LRS)**

Explanation

Locally redundant storage (LRS) copies your data synchronously three times within a single physical location in the primary region. This redundancy option provides a cost-effective way to ensure data durability and high availability within the same data center.

○ **Zone-redundant storage (ZRS)**

Explanation

Zone-redundant storage (ZRS) replicates your data synchronously across multiple availability zones within the same region. While it offers higher durability and availability compared to LRS, it does not copy data three times within a single physical location in the primary region as specified in the question.

○ **Geo-zone-redundant storage (GZRS)**

Explanation

Geo-zone-redundant storage (GZRS) replicates your data synchronously across multiple availability zones and multiple regions. It provides the highest level of durability and availability by spreading data copies across different geographic locations, which goes beyond the single physical location requirement in the question.

○ **Worldwide Redundant Storage (WRS)**

Explanation

Worldwide Redundant Storage (WRS) is not a valid Azure storage redundancy option. Azure does not offer a redundancy option called Worldwide Redundant Storage.

Overall explanation

From the official Azure docs:

Azure Storage always stores multiple copies of your data so that it's protected from planned and unplanned events, including transient hardware failures, network or power outages, and massive natural disasters. Redundancy ensures that your storage account meets its availability and durability targets even in the face of failures.

Redundancy in the primary region

Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage offers two options for how your data is replicated in the primary region:

- **Locally redundant storage (LRS)** copies your data synchronously three times within a single physical location in the primary region. LRS is the least expensive replication option, but isn't recommended for applications requiring high availability or durability.

- **Zone-redundant storage (ZRS)** copies your data synchronously across three Azure availability zones in the primary region. For applications requiring high availability, Microsoft recommends using ZRS in the primary region, and also replicating to a secondary region.

Reference: https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview

Domain

Describe Azure architecture and services (35–40%)

Question 10 Skipped

Azure ____________ is an authorization system built on Azure Resource Manager that provides fine-grained access management to Azure resources.

○ **Policies**

Explanation

Policies in Azure are used to enforce different rules and effects over resources, so they are not directly related to providing fine-grained access management to Azure resources. While policies can be used to enforce certain configurations or restrictions, they do not provide the same level of access control as RBAC.

Correct answer

○ **Role Based Access Control (RBAC)**

Explanation

Role Based Access Control (RBAC) is the correct choice as it is an authorization system in Azure that allows you to manage who has access to Azure resources, what they can do with those resources, and what areas they have access to. RBAC provides fine-grained access management by assigning roles to users, groups, or applications at a certain scope within Azure.

○ **Resource Groups**

Explanation

Resource Groups in Azure are containers that hold related resources for an Azure solution, but they are not an authorization system like RBAC. Resource Groups are used for organizing and managing resources, but they do not provide the fine-grained access management capabilities that RBAC offers.

○ **Locks**

Explanation

Locks in Azure are used to prevent accidental deletion or modification of Azure resources, but they are not an authorization system like RBAC. Locks help protect resources from being changed, but they do not provide the access management features that RBAC does.

Overall explanation

From the official Azure docs:

Access management for cloud resources is a critical function for any organization that is using the cloud. 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.

Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management to Azure resources.

What can you do with Azure RBAC?

Here are some examples of what you can do with Azure RBAC:

- Allow one user to manage virtual machines in a subscription and another user to manage virtual networks

- Allow a DBA group to manage SQL databases in a subscription
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets
- Allow an application to access all resources in a resource group

Reference: https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

Domain

Describe Azure management and governance (30–35%)

● **Question 11** Skipped

The concept of sharing resources among multiple users or tenants, allowing for cost savings and increased efficiency, is known as _______.

○ **Redundancy**

Explanation

Redundancy refers to having duplicate resources or systems in place to ensure reliability and availability in case of failures. It is not related to the concept of sharing resources among multiple users or tenants for cost savings and efficiency.

○ **Autonomy**

Explanation

Autonomy refers to the ability of a system or entity to operate independently without external control. It is not related to the concept of sharing resources among multiple users or tenants for cost savings and efficiency.

Correct answer

○ **Multi-Tenancy**

Explanation

Multi-Tenancy is the correct choice as it refers to the concept of sharing resources among multiple users or tenants on a single platform or infrastructure. This allows for cost savings, increased efficiency, and better resource utilization.

○ **Monolithic architecture**

Explanation

Monolithic architecture refers to a traditional approach where all components of an application are tightly coupled and deployed as a single unit. It is not related to the concept of sharing resources among multiple users or tenants for cost savings and efficiency.

Overall explanation

The concept of sharing resources among multiple users or tenants, allowing for cost savings and increased efficiency, is known as **"multi-tenancy".**

Other options -

- **Redundancy:** It refers to the duplication of critical system components to ensure continued operation in case of a failure. While redundancy is an important attribute of many cloud systems, it is not specifically related to the concept of sharing resources among multiple users.

- **Autonomy:** It refers to the ability of a system or organization to operate independently, with minimal external control or interference. While autonomy can be an important attribute of cloud systems, it is not specifically related to the concept of multi-tenancy.

- **Monolithic architecture:** It architecture refers to a software architecture pattern in which all components of an application are tightly integrated and deployed as a single unit. While monolithic architecture can be used in cloud systems, it is not specifically related to the concept of multi-tenancy, which involves the sharing of resources among multiple users or tenants.

Reference: https://learn.microsoft.com/en-us/azure/architecture/multitenant-identity/

Domain

Describe cloud concepts (25–30%)

Question 12 Skipped

What is the maximum allowed number of tags per Azure resource?

○ 30

○ 15

Correct answer

○ 50

○ 10

Overall explanation

The correct answer is 50.

Azure allows users to assign name-value pairs, called tags, to each resource, resource group, and subscription. The maximum number of tag name-value pairs that can be assigned to each of these entities is 50. If you need to apply more tags than the allowed number, you can use a JSON string to include multiple values for a single tag name. Each resource group or subscription can contain numerous resources, each with their own set of 50 tag name-value pairs.

Reference: https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources

Domain

Describe Azure management and governance (30–35%)

● **Question 13** Skipped

Which of the following is a free tool to conveniently manage your Azure cloud storage resources from your desktop?

○ **Azure FileSync**

Explanation

Azure FileSync is a service that enables organizations to centralize file services in Azure and cache files on-premises for fast access. It is not a tool for managing Azure cloud storage resources from a desktop interface.

○ **Azure AzCopy**

Explanation

Azure AzCopy is a command-line tool designed for high-performance data transfer to and from Azure storage. While it is a useful tool for data migration and synchronization, it is not specifically designed for managing Azure cloud storage resources from a desktop interface.

○ **Azure Migrate**

Explanation

Azure Migrate is a service that helps organizations assess and migrate their on-premises workloads to Azure. It is not a tool for managing Azure cloud storage resources from a desktop interface.

Correct answer

○ **Azure Storage Explorer**

Explanation

Azure Storage Explorer is a free tool that provides a graphical interface for managing Azure cloud storage resources from your desktop. It allows users to easily view, upload, download, and manage storage accounts, containers, and blobs.

○ **Azure Data Box**

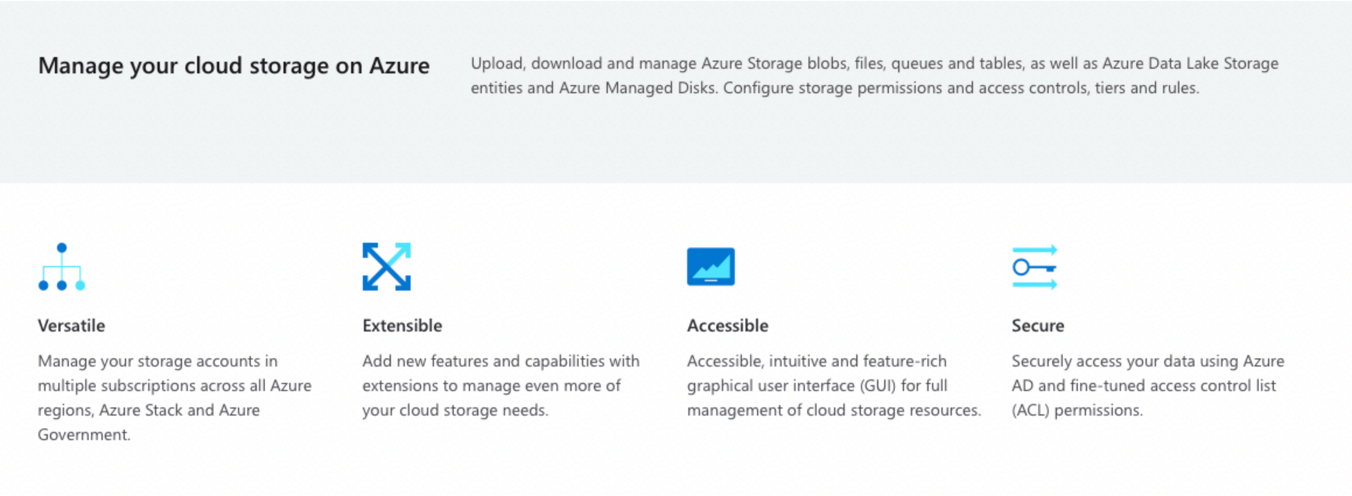
Explanation

Azure Data Box is a physical device used for offline data transfer to Azure cloud storage. It is not a tool for managing Azure cloud storage resources from a desktop interface.

Overall explanation

From the Official Azure Documentation:

Azure Storage Explorer is a free tool to conveniently manage your Azure cloud storage resources from your desktop.



Manage your cloud storage on Azure

Upload, download and manage Azure Storage blobs, files, queues and tables, as well as Azure Data Lake Storage entities and Azure Managed Disks. Configure storage permissions and access controls, tiers and rules.

Versatile

Manage your storage accounts in multiple subscriptions across all Azure regions, Azure Stack and Azure Government.

Extensible

Add new features and capabilities with extensions to manage even more of your cloud storage needs.

Accessible

Accessible, intuitive and feature-rich graphical user interface (GUI) for full management of cloud storage resources.

Secure

Securely access your data using Azure AD and fine-tuned access control list (ACL) permissions.

Reference : https://azure.microsoft.com/en-ca/features/storage-explorer/#overview

Domain

Describe Azure architecture and services (35–40%)

● **Question 14** Skipped

A development team is tasked with deploying a microservices-based application where each service needs to be independently scalable, with minimal management overhead and the ability to run code in response to events. Which Azure services would be best suited for this architecture?

Correct answer

○ **Azure Kubernetes Service (AKS) for container orchestration, and Azure Functions for event-driven code execution**

Explanation

Azure Kubernetes Service (AKS) is a managed Kubernetes service that allows for container orchestration, making it ideal for deploying and managing microservices. Azure Functions, on the other hand, is a serverless compute service that enables event-driven code execution, allowing each microservice to run code in response to events with minimal management overhead.

○ **Azure Virtual Machines for each microservice, and Azure Event Grid for event routing**

Explanation

Azure Virtual Machines may require more management overhead and lack the scalability and independence needed for microservices. Azure Event Grid is an event routing service, but it may not provide the same level of event-driven code execution capabilities as Azure Functions.

○ **Azure Service Fabric for container orchestration, and Azure Functions for event-driven code execution**

Explanation

Azure Service Fabric is a distributed systems platform for deploying and managing microservices, providing container orchestration capabilities. Azure Functions, as a serverless compute service, is suitable for event-driven code execution, making it a good choice for running code in response to events in a microservices architecture.

○ **Azure App Service for deploying the microservices, and Azure Logic Apps for event-driven integration**

Explanation

Azure App Service is a platform-as-a-service (PaaS) offering that simplifies the deployment of microservices, but it may not provide the level of scalability and independence required for each service. Azure Logic Apps, while suitable for event-driven integration, may not offer the same level of scalability and independence as Azure Functions for code execution.

Overall explanation

Azure Kubernetes Service (AKS) provides a fully managed Kubernetes platform to orchestrate and scale containerized applications. Azure Functions can execute code in response to specific events, allowing for highly scalable, event-driven execution with minimal management overhead.

Domain

Describe Azure architecture and services (35–40%)

● **Question 15** Skipped

A company uses a ________ service type to rapidly build and deploy a web application without managing servers, and a ________ service type to access a fully managed email platform for employees.

○ **IaaS, PaaS**

Explanation

IaaS (Infrastructure as a Service) service type provides virtualized computing resources over the internet. It is not the correct service type for rapidly building and deploying web applications without managing servers, as it still requires managing the infrastructure. IaaS doesn't fit either requirement.

Correct answer

○ **PaaS, SaaS**

Explanation

Using a PaaS (Platform as a Service) service type allows the company to quickly build and deploy a web application without the need to manage servers. This service type provides a platform for developers to build, test, and deploy applications without worrying about infrastructure management. SaaS is perfect for a fully managed email platform (think Gmail).

○ **SaaS, IaaS**

Explanation

IaaS (Infrastructure as a Service) service type provides virtualized computing resources over the internet. It is not the correct service type for rapidly building and deploying web applications without managing servers, as it still requires managing the infrastructure. IaaS doesn't fit either requirement.

○ **SaaS, PaaS**

Explanation

While SaaS (Software as a Service) service type is used to access fully managed software applications, it is not the correct service type for rapidly building and deploying web applications without managing servers. PaaS (Platform as a Service) is the appropriate service type for this purpose. Ordering is opposite. PaaS : SaaS is the right order.

Overall explanation

Platform as a Service (PaaS) for Building and Deploying Web Applications

PaaS is a cloud computing service that provides a platform allowing customers to develop, run, and manage applications without having to manage the underlying infrastructure (such as servers, networking, storage, etc.).

- **Example in this case:** If a company wants to build a web application but doesn't want to handle the complexities of managing the servers or the environment on which the app will run, it can use a PaaS. The platform provides the necessary tools, frameworks, and development environments for creating the app.
- **Benefits:**
    - Developers can focus on writing code and building the application without worrying about server management.
    - Automatic scaling and updates are handled by the PaaS provider.
    - It supports fast deployment and often includes integrated tools for testing and monitoring.

Example of PaaS providers: Heroku, Google App Engine, Microsoft Azure App Service.

Software as a Service (SaaS) for Accessing a Fully Managed Email Platform

SaaS is a cloud computing service that provides access to software applications over the internet. These applications are hosted and fully managed by a third-party service provider, which means users don't need to install or maintain any software themselves.

- **Example in this case:** If a company wants an email platform for its employees, but doesn't want to deal with managing email servers, security, or software updates, it can use a SaaS provider that offers a fully managed email platform.
- **Benefits:**
    - Employees can access the email system via a web browser, and the company doesn't have to maintain or configure any hardware or software.
    - The SaaS provider takes care of security, maintenance, and upgrades.
    - It often includes features like spam filtering, mobile access, and collaborative tools.

Example of SaaS providers: Google Workspace (formerly G Suite), Microsoft 365 (Outlook), and Zoho Mail.

Domain

Describe cloud concepts (25–30%)

● **Question 16** Skipped

A company wants to deploy multiple resources in different subnets within the same Azure region, ensuring that some resources can communicate with each other, while others must remain isolated. The goal is to provide network segmentation without the use of a VPN or public IPs. Which Azure network configuration would best meet these requirements?

○ **Azure Virtual Network with Network Security Groups (NSGs) applied to individual VMs**

Explanation

Azure Virtual Network with Network Security Groups (NSGs) applied to individual VMs is not the most efficient choice for achieving network segmentation in this scenario. Applying NSGs to individual VMs can be cumbersome and less scalable compared to applying NSGs to entire subnets, which can provide better control and management of network traffic.

○ **Azure Virtual Network with VPN Gateway for inter-subnet communication**

Explanation

Azure Virtual Network with VPN Gateway for inter-subnet communication is not the best choice for this scenario as the company wants to avoid using a VPN. VPN Gateway is typically used for secure communication between on-premises networks and Azure Virtual Networks, not for network segmentation within the same Azure region.

○ **Azure Virtual Network Peering between different subnets**

Explanation

Azure Virtual Network Peering between different subnets allows resources in different virtual networks to communicate with each other. While this can provide connectivity between subnets, it does not offer the level of network segmentation and control over traffic that NSGs applied to individual subnets can provide.

Correct answer

○ **Azure Virtual Network with Network Security Groups (NSGs) applied to individual subnets**

Explanation

Azure Virtual Network with Network Security Groups (NSGs) applied to individual subnets is the correct choice as NSGs allow you to control inbound and outbound traffic to resources within a subnet. By applying NSGs to individual subnets, you can define specific rules for communication between resources, enabling network segmentation without the need for VPNs or public IPs.

Overall explanation

Using Azure Virtual Network with Network Security Groups (NSGs) allows for segmentation and control of traffic between subnets. NSGs can be applied to subnets to control which resources within those subnets can communicate with each other, effectively providing network segmentation.

Domain

Describe Azure architecture and services (35–40%)

● **Question 17** Skipped

A consulting firm grants Azure portal access to clients using their own company logins, restricted to specific IPs, while internal staff face stricter sign-in rules. Which Azure feature enforces these location-based access policies?

○ **Microsoft Entra B2B**

Explanation

Microsoft Entra B2B is a feature that allows organizations to securely share applications and services with guest users from other organizations. It is not specifically designed to enforce location-based access policies for Azure portal access.

○ **Microsoft Entra B2C**

Explanation

Microsoft Entra B2C is a feature that enables organizations to manage customer identities and access to applications. It is not tailored for enforcing location-based access policies for Azure portal access.

Correct answer

○ **Microsoft Entra Conditional Access**

Explanation

Microsoft Entra Conditional Access is the correct choice as it allows organizations to define and enforce access policies based on specific conditions, such as location, device compliance, and user risk. This feature can be used to restrict access to the Azure portal based on IP addresses for clients and apply stricter sign-in rules for internal staff.

○ **Azure Monitor**

Explanation

Azure Monitor is a monitoring and analytics service in Azure that helps organizations understand how their applications are performing and proactively identify issues. It is not related to enforcing location-based access policies for Azure portal access.

Overall explanation

The correct answer is: **Microsoft Entra Conditional Access**

Microsoft Entra Conditional Access is the Azure feature that allows you to enforce location-based access policies and other conditions for both internal and external users. In this scenario, the firm is restricting access for clients based on specific IPs and applying stricter sign-in rules for internal staff. This type of control, based on conditions like location (IP addresses) and other factors, is managed by **Conditional Access** policies.

Why the other options are incorrect:

- **Microsoft Entra B2B**: **Microsoft Entra B2B** (Business-to-Business) is used for allowing external partners (clients, vendors) to access resources using their own identity providers, but it does not handle the enforcement of location-based or other conditional access policies. It's more about managing external identities.

- **Microsoft Entra B2C**: **Microsoft Entra B2C** (Business-to-Consumer) is used for managing customer identities and enabling consumer-facing applications, but it doesn't specifically handle location-based access policies for internal staff or clients.

- **Azure Monitor**: **Azure Monitor** is a tool for tracking and monitoring the performance and health of Azure resources. While it can log access events, it does not enforce location-based access policies.

Domain

Describe Azure architecture and services (35–40%)

● **Question 18** Skipped

As the Lead Security Engineer of your organization, you're worried that someone may mistakenly delete mission critical resources in Azure. What can you do to prevent this from accidentally happening?

○ **Use Azure Monitor to define policies**

Explanation

Using Azure Monitor to define policies can help in monitoring and enforcing compliance with organizational standards and best practices. While it can help in identifying potential issues, it does not directly prevent accidental deletion of resources.

○ **Apply the DoNotTouch Lock on the resources**

Explanation

Applying the DoNotTouch Lock on the resources is not a standard lock type in Azure. It is important to use the appropriate lock types provided by Azure, such as the CanNotDelete Lock, to prevent accidental deletion of critical resources.

○ **Use Azure ExpressRoute**

Explanation

Azure ExpressRoute is a service that provides a private connection between an organization's on-premises infrastructure and Azure data centers. While it enhances network connectivity, it does not prevent accidental deletion of resources in Azure.

Correct answer

○ **Apply the CanNotDelete Lock on the resources**

Explanation

Applying the CanNotDelete Lock on the resources in Azure prevents users from deleting those resources accidentally. This lock restricts the deletion of the resource, providing an additional layer of protection against unintended actions.

○ **Use an Azure Virtual Subnet**

Explanation

Using an Azure Virtual Subnet does not directly prevent accidental deletion of resources. Virtual subnets are used for network segmentation and isolation, not for resource deletion protection.

Overall explanation

Applying a delete lock to the resource group will prevent the resources inside it from being deleted.

As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.

You can set the lock level to **CanNotDelete** or **ReadOnly**. In the portal, the locks are called **Delete** and **Read-only** respectively:

1) CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.

2) 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.

Reference: https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

Domain

Describe Azure management and governance (30–35%)

● **Question 19** Skipped

Your Azure account contains several policies and you wish to group/organize them. Which of the following can help you achieve this?

○ **Resource Groups**

Explanation

Resource Groups in Azure are used to logically group and manage related resources such as virtual machines, storage accounts, and databases. While resource groups are essential for organizing resources, they are not specifically designed for grouping policies.

Correct answer

○ **Initiatives**

Explanation

Initiatives in Azure allow you to group and organize policies together. They provide a way to manage and enforce compliance for a set of related policies, making it easier to track and monitor the overall compliance status of your resources.

○ **Azure Active Directory**

Explanation

Azure Active Directory is a cloud-based identity and access management service in Azure. While it is crucial for managing user identities and access to resources, it is not specifically designed for organizing policies within Azure.

○ **Network Security Groups**

Explanation

Network Security Groups in Azure are used to control inbound and outbound traffic to network interfaces, VMs, and subnets. They are not intended for organizing policies, but rather for managing network security rules.

Overall explanation

From the official Azure docs:

An initiative definition is a collection of policy definitions that are tailored towards achieving a singular overarching goal. Initiative definitions simplify managing and assigning policy definitions. They simplify by grouping a set of policies as one single item. For example, you could create an initiative titled **Enable Monitoring in Azure Security Center**, with a goal to monitor all the available security recommendations in your Azure Security Center.

Reference : https://docs.microsoft.com/en-us/azure/governance/policy/overview#initiative-definition

Domain

Describe Azure management and governance (30–35%)

Question 20 Skipped

Yes or No:

ExpressRoute connections go over the public Internet, and they offer more reliability, faster speeds, and lower latencies than typical Internet connections.

○ Yes

Explanation

ExpressRoute connections do not go over the public Internet; instead, they provide a private connection to Microsoft Azure services through a dedicated connection. This private connection offers more reliability, faster speeds, and lower latencies compared to typical Internet connections.

Correct answer

○ No

Explanation

This choice is correct because ExpressRoute connections do not rely on the public Internet. They use a private connection to Microsoft Azure services, providing more reliability, faster speeds, and lower latencies than typical Internet connections.

Overall explanation

No, it is **false** that ExpressRoute connections go over the public Internet. However, they do offer more reliability, faster speeds, and lower latencies than typical Internet connections.

From the Official Azure Documentation:

All incoming data into Azure using ExpressRoute is free of charge (as with any other inbound data

transfer to Azure).

Make your connections fast, reliable, and private

Use Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. ExpressRoute connections don't go over the public Internet, and they offer more reliability, faster speeds, and lower latencies than typical Internet connections. In some cases, using ExpressRoute connections to transfer data between on-premises systems and Azure can give you significant cost benefits.

With ExpressRoute, establish connections to Azure at an ExpressRoute location, such as an Exchange provider facility, or directly connect to Azure from your existing WAN network, such as a multiprotocol label switching (MPLS) VPN, provided by a network service provider.

Use a virtual private cloud for storage, backup, and recovery

ExpressRoute gives you a fast and reliable connection to Azure with bandwidths up to 100 Gbps, which makes it excellent for scenarios like periodic data migration, replication for business continuity, disaster recovery, and other high-availability strategies. It can be a cost-effective option for transferring large amounts of data, such as datasets for high-performance computing applications, or moving large virtual machines between your dev-test environment in an Azure virtual private cloud and your on-premises production environments.

Extend and connect your datacenters

Use ExpressRoute to both connect and add compute and storage capacity to your existing datacenters. With high throughput and fast latencies, Azure will feel like a natural extension to or between your datacenters, so you enjoy the scale and economics of the public cloud without having to compromise on network performance.

Build hybrid applications

With predictable, reliable, and high-throughput connections offered by ExpressRoute, build applications that span on-premises infrastructure and Azure without compromising privacy or performance. For example, run a corporate intranet application in Azure that authenticates your customers with an on-premises Active Directory service, and serve all of your corporate customers without traffic ever routing through the public Internet.

Reference: https://azure.microsoft.com/en-us/services/expressroute/#overview

Domain

Describe Azure architecture and services (35–40%)

Question 21 Skipped

A recent unapproved size change to one of the Virtual Machines (VMs) in your company has led to a huge unexpected bill. Which of the following services can help you identify the user who made this unapproved change?

○ Azure Information Protection (AIP)

Explanation

Azure Information Protection (AIP) is a service that helps you classify, label, and protect sensitive data. While it is important for data protection and compliance, it is not directly related to identifying the user who made an unapproved change to a Virtual Machine.

○ **Azure Event Hubs**

Explanation

Azure Event Hubs is a real-time data ingestion service that can collect, transform, and store events. While it can provide insights into the events happening within your Azure environment, it is not specifically designed to track user actions or changes made to resources like Virtual Machines.

○ **Azure Xamarin**

Explanation

Azure Xamarin is a mobile app development platform that allows you to build cross-platform mobile applications. It is not a service that can help you identify the user who made an unapproved change to a Virtual Machine in your Azure environment.

Correct answer

○ **Azure Activity Log**

Explanation

Azure Activity Log tracks all operations performed on resources in your Azure subscription. It logs information about who made the change, what action was taken, and when it occurred. By reviewing the Activity Log, you can easily identify the user responsible for the unapproved size change to the Virtual Machine.

○ **Azure Service Health**

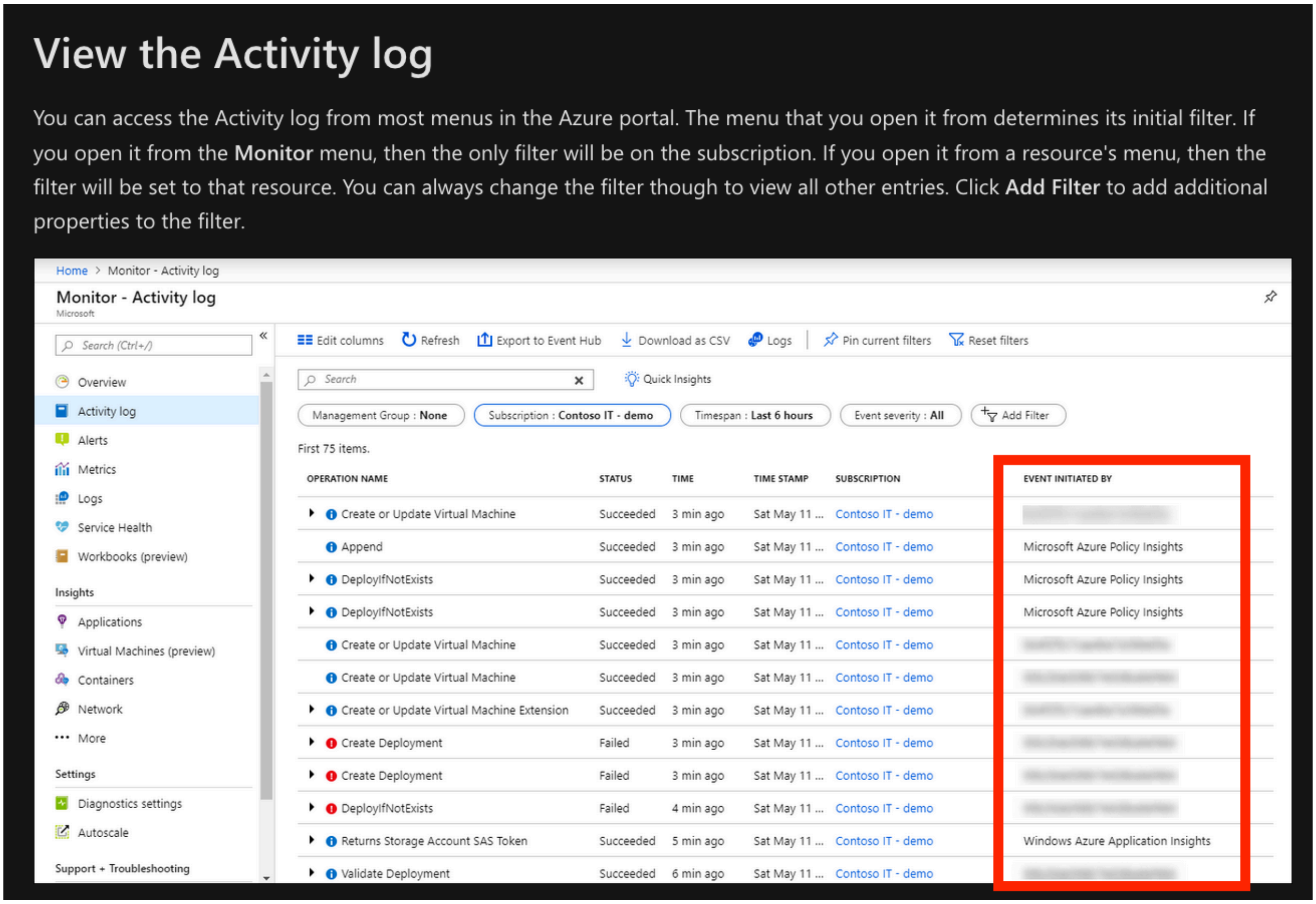
Explanation

Azure Service Health provides personalized guidance and support when Azure services are experiencing issues. While it can help you stay informed about the health of your Azure services, it does not track user actions or changes made to resources like Virtual Machines.

Overall explanation

From the Official Azure Documentation:

The Azure Monitor activity log is a platform log in Azure that provides insight into subscription-level events. The activity log includes information like when a resource is modified or a virtual machine is started. You can view the activity log in the Azure portal or retrieve entries with PowerShell and the Azure CLI. This article provides information on how to view the activity log and send it to different destinations.



View the Activity log

You can access the Activity log from most menus in the Azure portal. The menu that you open it from determines its initial filter. If you open it from the **Monitor** menu, then the only filter will be on the subscription. If you open it from a resource's menu, then the filter will be set to that resource. You can always change the filter though to view all other entries. Click **Add Filter** to add additional properties to the filter.

Management Group : **None** | Subscription : **Contoso IT - demo** | Timespan : **Last 6 hours** | Event severity : **All**

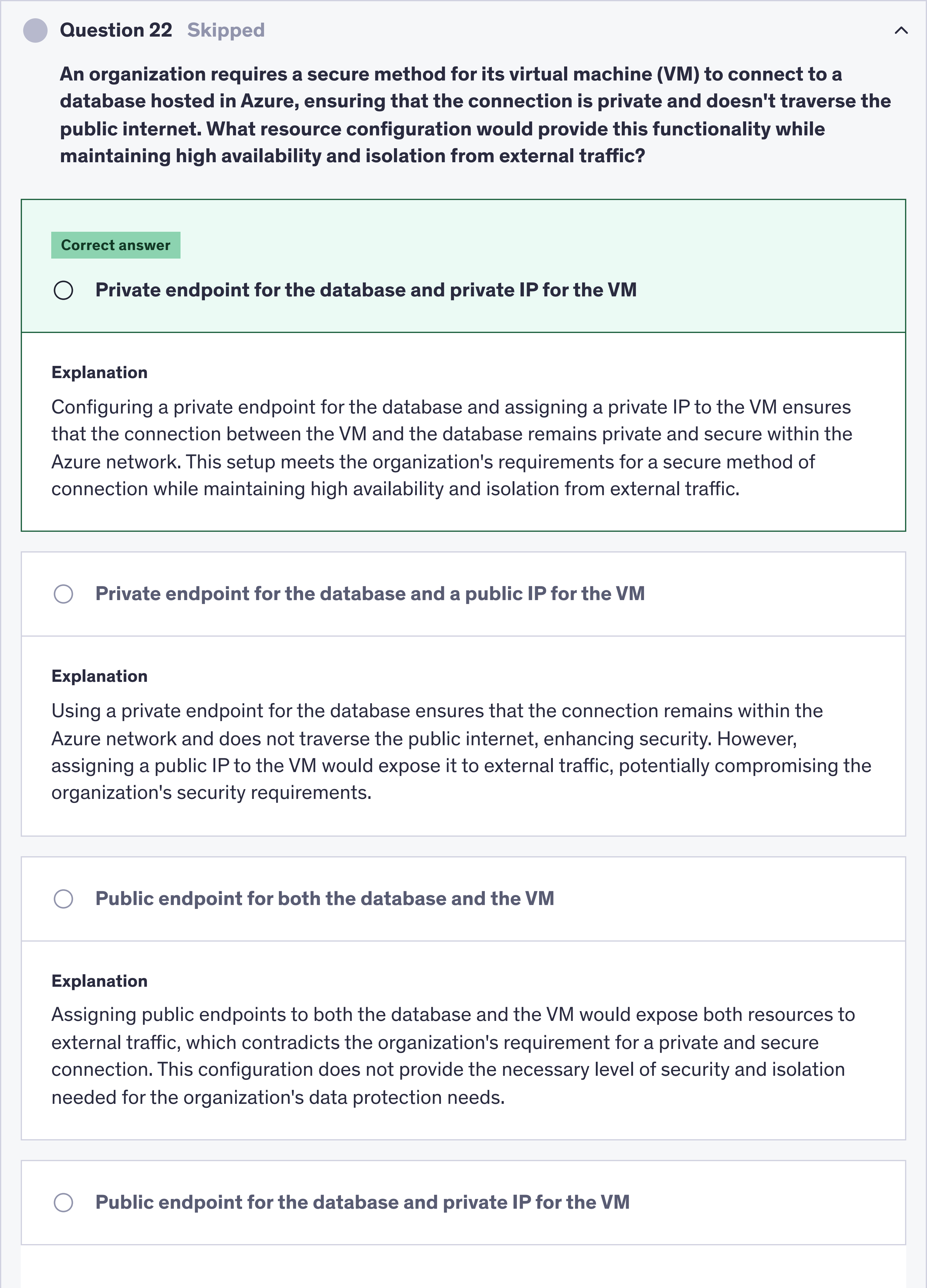
First 75 items.

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
Create or Update Virtual Machine	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	[redacted]
Append	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	Microsoft Azure Policy Insights
DeployIfNotExists	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	Microsoft Azure Policy Insights
DeployIfNotExists	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	Microsoft Azure Policy Insights
Create or Update Virtual Machine	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	[redacted]
Create or Update Virtual Machine	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	[redacted]
Create or Update Virtual Machine Extension	Succeeded	3 min ago	Sat May 11 ...	Contoso IT - demo	[redacted]
Create Deployment	Failed	3 min ago	Sat May 11 ...	Contoso IT - demo	[redacted]
Create Deployment	Failed	3 min ago	Sat May 11 ...	Contoso IT - demo	[redacted]
DeployIfNotExists	Failed	4 min ago	Sat May 11 ...	Contoso IT - demo	[redacted]
Returns Storage Account SAS Token	Succeeded	5 min ago	Sat May 11 ...	Contoso IT - demo	Windows Azure Application Insights
Validate Deployment	Succeeded	6 min ago	Sat May 11 ...	Contoso IT - demo	[redacted]

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log

Domain

Describe Azure management and governance (30–35%)



Question 22 Skipped

An organization requires a secure method for its virtual machine (VM) to connect to a database hosted in Azure, ensuring that the connection is private and doesn't traverse the public internet. What resource configuration would provide this functionality while maintaining high availability and isolation from external traffic?

Correct answer

○ **Private endpoint for the database and private IP for the VM**

Explanation

Configuring a private endpoint for the database and assigning a private IP to the VM ensures that the connection between the VM and the database remains private and secure within the Azure network. This setup meets the organization's requirements for a secure method of connection while maintaining high availability and isolation from external traffic.

○ **Private endpoint for the database and a public IP for the VM**

Explanation

Using a private endpoint for the database ensures that the connection remains within the Azure network and does not traverse the public internet, enhancing security. However, assigning a public IP to the VM would expose it to external traffic, potentially compromising the organization's security requirements.

○ **Public endpoint for both the database and the VM**

Explanation

Assigning public endpoints to both the database and the VM would expose both resources to external traffic, which contradicts the organization's requirement for a private and secure connection. This configuration does not provide the necessary level of security and isolation needed for the organization's data protection needs.

○ **Public endpoint for the database and private IP for the VM**

Explanation

Assigning a public endpoint to the database would expose it to external traffic, which goes against the organization's requirement for a secure and private connection. Additionally, using a private IP for the VM does not guarantee the isolation needed to maintain high availability and security.

Overall explanation

A **private** endpoint for the database ensures that the connection remains **within** the Azure network and is not exposed to the public internet. Coupled with a private IP for the VM, this solution provides a secure and isolated communication path.

Domain

Describe Azure architecture and services (35–40%)

● **Question 23** Skipped

You can link virtual networks together by using ________________.

○ **Virtual Network Hub**

Explanation

Virtual Network Hub is not a method for linking virtual networks together in Azure. A virtual network hub typically refers to a central networking point where multiple connections converge, but it does not specifically facilitate the connection of virtual networks in Azure.

Correct answer

○ **Virtual Network Peering**

Explanation

Virtual Network Peering allows you to connect virtual networks in the same region or different regions through the Azure backbone network. It enables resources in different virtual networks to communicate with each other securely and efficiently.

○ **Virtual Network Proxy**

Explanation

Virtual Network Proxy is not a feature or service in Azure that allows you to link virtual networks together. A proxy typically acts as an intermediary for network communication and does not provide the direct network connectivity needed to link virtual networks.

○ **Virtual Network Seeding**

Explanation

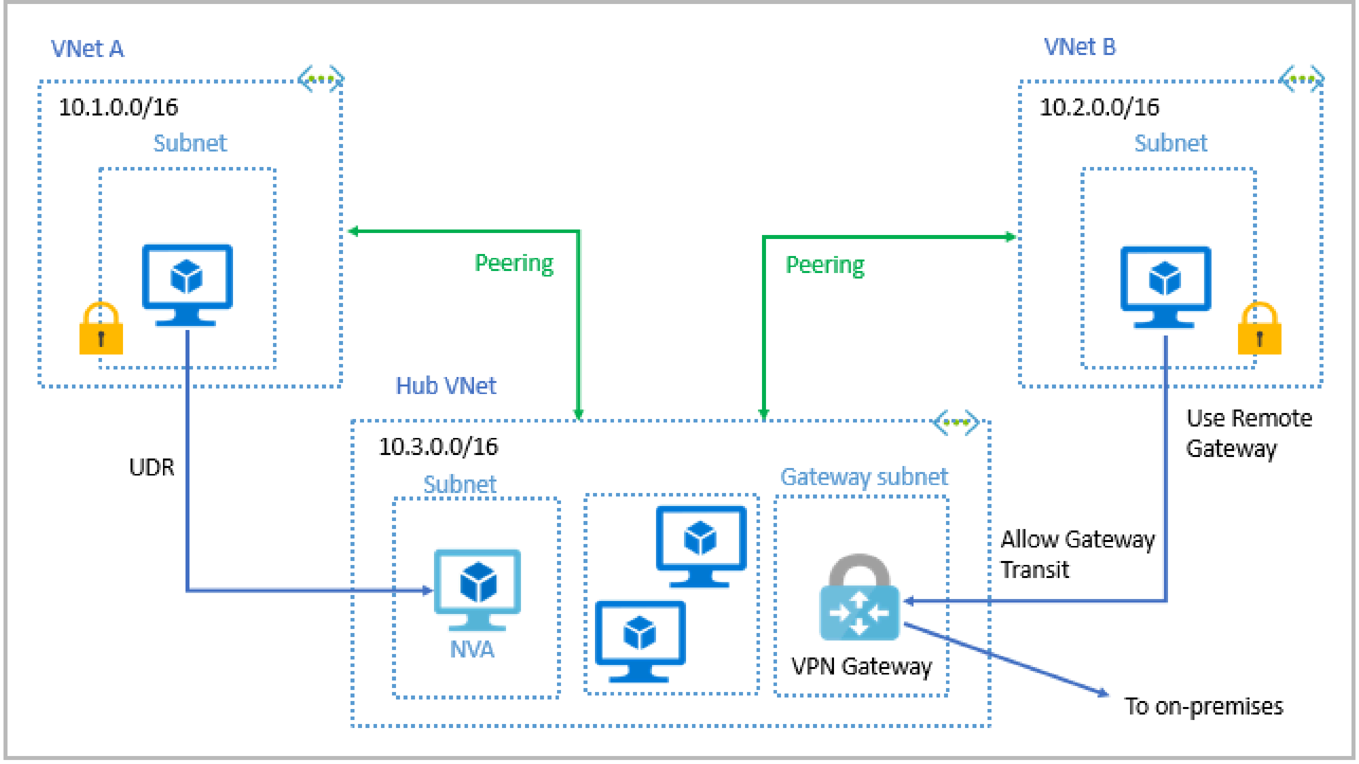
Virtual Network Seeding is not a valid method for linking virtual networks together in Azure. This term does not exist in the context of Azure networking and does not provide a mechanism for connecting virtual networks.

Overall explanation

From the Official Azure Documentation:

You can link virtual networks together by using virtual network **peering**. Peering enables resources in each virtual network to communicate with each other. These virtual networks can be in separate regions, which allows you to create a global interconnected network through Azure.

User-defined routes (UDR) are a significant update to Azure’s Virtual Networks that allows for greater control over network traffic flow. This method allows network administrators to control the routing tables between subnets within a VNet, as well as between VNets.



Reference: https://docs.microsoft.com/en-ca/learn/modules/azure-networking-fundamentals/azure-virtual-network-fundamentals

Domain

Describe Azure architecture and services (35–40%)

Question 24 Skipped

For all cloud deployment types, you own your __________ and ______________. You're also responsible for their security.

○ **information , network controls**

○ **devices, operating system**

○ **data, physical network**

Correct answer

○ **data , identities**

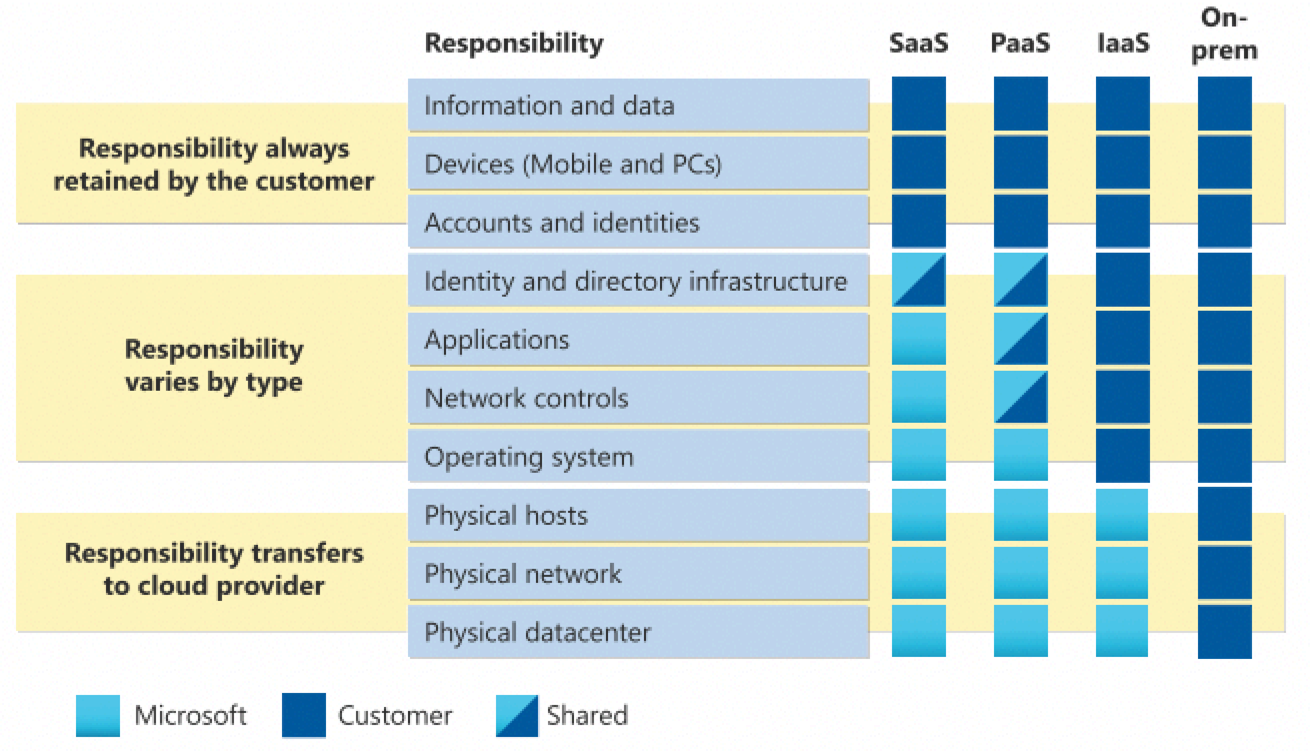
Overall explanation

From the Official Azure Documentation:

As you consider and evaluate public cloud services, it's critical to understand the shared responsibility model and which security tasks are handled by the cloud provider and which tasks are handled by you. The workload responsibilities vary depending on whether the workload is hosted on Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or in an on-premises datacenter.

Division of responsibility

In an on-premises datacenter, you own the whole stack. As you move to the cloud some responsibilities transfer to Microsoft. The following diagram illustrates the areas of responsibility between you and Microsoft, according to the type of deployment of your stack.



	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■
	Accounts and identities	■	■	■	■
Responsibility varies by type	Identity and directory infrastructure	◩	◩	■	■
	Applications	□	◩	■	■
	Network controls	□	◩	■	■
	Operating system	□	□	■	■
Responsibility transfers to cloud provider	Physical hosts	□	□	□	■
	Physical network	□	□	□	■
	Physical datacenter	□	□	□	■

□ Microsoft ■ Customer ◩ Shared

For all cloud deployment types, you own your data and identities. You are responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control (which varies by service type).

Regardless of the type of deployment, the following responsibilities are always retained by you:

- Data
- Endpoints
- Account
- Access management

Reference: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Domain

Describe cloud concepts (25–30%)

Question 25 Skipped

In an Azure virtual network, which of the following is used to filter network traffic between subnets?

○ **Azure Firewall**

Explanation

Azure Firewall is a managed, cloud-based network security service that protects Azure Virtual Network resources. While it can filter network traffic, it is typically used for outbound traffic filtering and network address translation (NAT) rather than filtering traffic between subnets within a virtual network.

Correct answer

○ **Network Security Group**

Explanation

Network Security Group (NSG) is used to filter network traffic between subnets within an Azure virtual network. It acts as a basic firewall that allows or denies inbound and outbound traffic based on rules defined by the user.

○ **Azure Load Balancer**

Explanation

Azure Load Balancer is used to distribute incoming network traffic across multiple virtual machines to ensure high availability and reliability. It is not specifically designed to filter network traffic between subnets within a virtual network.

○ **Azure Application Gateway**

Explanation

Azure Application Gateway is a web traffic load balancer that helps manage and optimize traffic to web applications. It is not used to filter network traffic between subnets within an Azure virtual network.

Overall explanation

Network Security Group is the correct answer.

A Network Security Group (NSG) is a basic form of firewall that can be used to filter network traffic between subnets in an Azure virtual network. NSGs are used to define inbound and outbound traffic rules that control the flow of traffic to and from resources in a virtual network.

Other options -

Azure Firewall: It is a firewall service that can be used to filter network traffic, and is typically used to protect virtual networks from external threats and to enforce network security policies. However, Azure Firewall is not typically used to filter network traffic between subnets in an Azure virtual network. This is because Network Security Group (NSG) is the recommended method for filtering network traffic within a virtual network.

Azure Application Gateway: It provides application-level load balancing and routing, but is not used to filter network traffic between subnets in an Azure virtual network. It is focused on providing routing and load balancing for web traffic, rather than network traffic.

Azure Load Balancer: It can be used to distribute incoming traffic across multiple virtual machines or instances within a Virtual Network, but is not used to filter network traffic between subnets in an Azure virtual network. It provides a load balancing service, rather than a filtering service.

Reference: https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

Domain

Describe Azure architecture and services (35–40%)

● **Question 26** Skipped

Which of the following Azure Storage would you use to store different types of files such as videos, audios, text in a highly cost effective and scalable manner?

○ **Azure SQL Database**

Explanation

Azure SQL Database is a fully managed relational database service that is designed for storing structured data in a relational format. It is not the ideal choice for storing different types of files like videos, audios, and text, as it is optimized for transactional data processing rather than large file storage.

○ **Azure PostgreSQL**

Explanation

Azure PostgreSQL is a fully managed relational database service that is suitable for storing structured data in a relational format. It is not optimized for storing large files such as videos, audios, and text, and may not be the most cost-effective option for this use case.

Correct answer

○ **Azure Blob Storage**

Explanation

Azure Blob Storage is the correct choice for storing different types of files such as videos, audios, and text in a highly cost-effective and scalable manner. It is optimized for storing massive amounts of unstructured data and offers tiered storage options to help manage costs efficiently.

○ **Azure Cosmos DB**

Explanation

Azure Cosmos DB is a globally distributed, multi-model database service designed for scalable and high-performance applications. While it is suitable for storing structured data with low latency requirements, it is not the ideal choice for storing various types of files like videos, audios, and text.

Overall explanation

From the official Azure documentation:

A blob is a binary, large object and a storage option for any type of data that you want to store in a binary format. Learn about blob types.

Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of `unstructured` data. Unstructured data is data that doesn't adhere to a particular data model or definition, such as text or binary data.

Blob storage is designed for:

1) Serving images or documents directly to a browser.
2) Storing files for distributed access.
3) Streaming video and audio.
4) Writing to log files.
5) Storing data for backup and restore, disaster recovery, and archiving.
6) Storing data for analysis by an on-premises or Azure-hosted service.

Reference : https://azure.microsoft.com/en-us/services/storage/blobs/#security

Domain

Describe Azure architecture and services (35–40%)

● **Question 27** Skipped

After taking a lot of courses and understanding cloud fundamentals, you've realized that migrating your business resources to Azure makes the most sense. Based on your understanding, which of the following would you need to create first?

○ **A resource group**

Explanation

While creating a resource group is an essential step in organizing and managing resources within Azure, it is not the first step in the migration process. A subscription must be created first to establish the billing and access control framework.

○ **A virtual network**

Explanation

Creating a virtual network is important for networking and connectivity within Azure, but it is not the initial step in the migration process. A subscription is required before creating any resources, including virtual networks.

Correct answer

○ **A subscription**

Explanation

Creating a subscription is the first step when migrating your business resources to Azure. A subscription is required to access and manage Azure services, resources, and billing. It acts as the billing and access control boundary for Azure services.

○ **A resource lock**

Explanation

Resource locks are used to prevent accidental deletion or modification of Azure resources, but they are not the first step in the migration process. Creating a subscription is necessary to establish the foundation for managing and accessing Azure resources.

Overall explanation

A subscription needs to be created first and foremost.

The Azure account is what lets you access Azure services and Azure subscriptions. It is possible to create multiple subscriptions in our Azure account to create separation for billing or management purposes. In your subscription(s) you can manage resources in resources groups.

The Azure hierarchy looks like :

Tenancy -> Subscription -> Resource Group -> Resource.

Reference: https://techcommunity.microsoft.com/t5/azure/understanding-azure-account-subscription-and-directory/m-p/34800

Domain

Describe Azure management and governance (30–35%)

● **Question 28** Skipped

Yes or No:

Azure Advisor provides a cloud score to assess how well-architected your workloads are AND can also provide 'Step-by-Step' guidance and quick actions for fast remediation.

Correct answer

○ Yes

Explanation

Azure Advisor does provide a cloud score to assess the architectural best practices of your workloads. It also offers 'Step-by-Step' guidance and quick actions for remediation to help improve the overall performance, security, and reliability of your Azure resources.

○ No

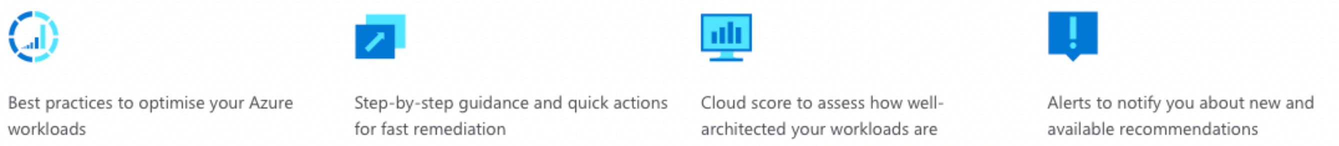
Explanation

This choice is incorrect as Azure Advisor does provide a cloud score to assess workload architecture and offers 'Step-by-Step' guidance for remediation, making the statement true.

Overall explanation

From the Official Azure Documentation:

Azure Advisor helps in quick and easy optimization of your Azure deployments. Azure Advisor analyses your configurations and usage telemetry and offers personalised, actionable recommendations to help you optimise your Azure resources for reliability, security, operational excellence, performance and cost.



Best practices to optimise your Azure workloads

Step-by-step guidance and quick actions for fast remediation

Cloud score to assess how well-architected your workloads are

Alerts to notify you about new and available recommendations

Reference: https://azure.microsoft.com/en-ca/services/advisor/#security

Domain

Describe Azure management and governance (30–35%)

● **Question 29** Skipped

If your application experiences sudden high demand, what type of scaling would involve adding more virtual machines or containers?

Correct answer

○ **Horizontal scaling**

Explanation

Horizontal scaling, also known as scale-out, involves adding more virtual machines or containers to distribute the load and handle sudden spikes in demand. This type of scaling is suitable for increasing capacity quickly and efficiently in response to increased traffic.

○ **Vertical scaling**

Explanation

Vertical scaling involves increasing the resources of a single virtual machine or container, such as adding more CPU, memory, or storage. It does not involve adding more instances to handle high demand, which makes it less suitable for sudden spikes in traffic.

○ **Downscaling**

Explanation

Downscaling refers to reducing the number of virtual machines or containers in response to decreased demand. It is the opposite of adding more instances to handle sudden high demand, which is required in this scenario.

○ **Static scaling**

Explanation

Static scaling refers to a fixed number of virtual machines or containers that do not change dynamically based on demand. It does not allow for the flexibility of adding more instances to handle sudden high demand, making it less suitable for scenarios with fluctuating traffic.

Overall explanation

From the official docs:

Horizontal scaling

With horizontal scaling, if you suddenly experienced a steep jump in demand, your deployed resources could be scaled out (either automatically or manually). For example, you could add additional virtual machines or containers, scaling out. In the same manner, if there was a significant drop in demand, deployed resources could be scaled in (either automatically or manually), scaling in.

Vertical scaling

With vertical scaling, if you were developing an app and you needed more processing power, you could vertically scale up to add more CPUs or RAM to the virtual machine. Conversely, if you realized you had over-specified the needs, you could vertically scale down by lowering the CPU or RAM specifications.

Reference: https://learn.microsoft.com/en-us/training/modules/describe-benefits-use-cloud-services/2-high-availability-scalability-cloud

Domain

Describe cloud concepts (25–30%)

Question 30 Skipped

Yes or No: Cloud services provide greater control over the physical security of your data compared to on-premises infrastructure.

○ Yes

Correct answer

○ **No**

Overall explanation

The answer is No!

Cloud services and on-premises infrastructure have different security models, with unique strengths and weaknesses. While cloud services provide greater control over some aspects of data security, such as network security and access control, they also require a greater degree of trust in the cloud provider to maintain physical security of the data centers where the data is stored. In contrast, on-premises infrastructure provides greater control over physical security, as the organization has direct control over the physical security measures and can ensure that the data is physically secure.

This is why you'll see a lot of large organizations aren't comfortable storing sensitive data on the cloud.

Domain

Describe cloud concepts (25–30%)

● **Question 31** Skipped

________________ copies your data synchronously across three Azure availability zones in the primary region. For applications requiring high availability.

Correct answer

○ **Zone Redundant Storage (ZRS)**

○ **Planet-redundant storage (PRS)**

○ **Locally redundant storage (LRS)**

○ **Geo-zone-redundant storage (GZRS)**

Overall explanation

From the Official Azure Documentation:

Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage offers two options for how your data is replicated in the primary region:

- **Locally redundant storage (LRS)** copies your data synchronously three times within a single physical location in the primary region. LRS is the least expensive replication option, but isn't recommended for applications requiring high availability or durability.

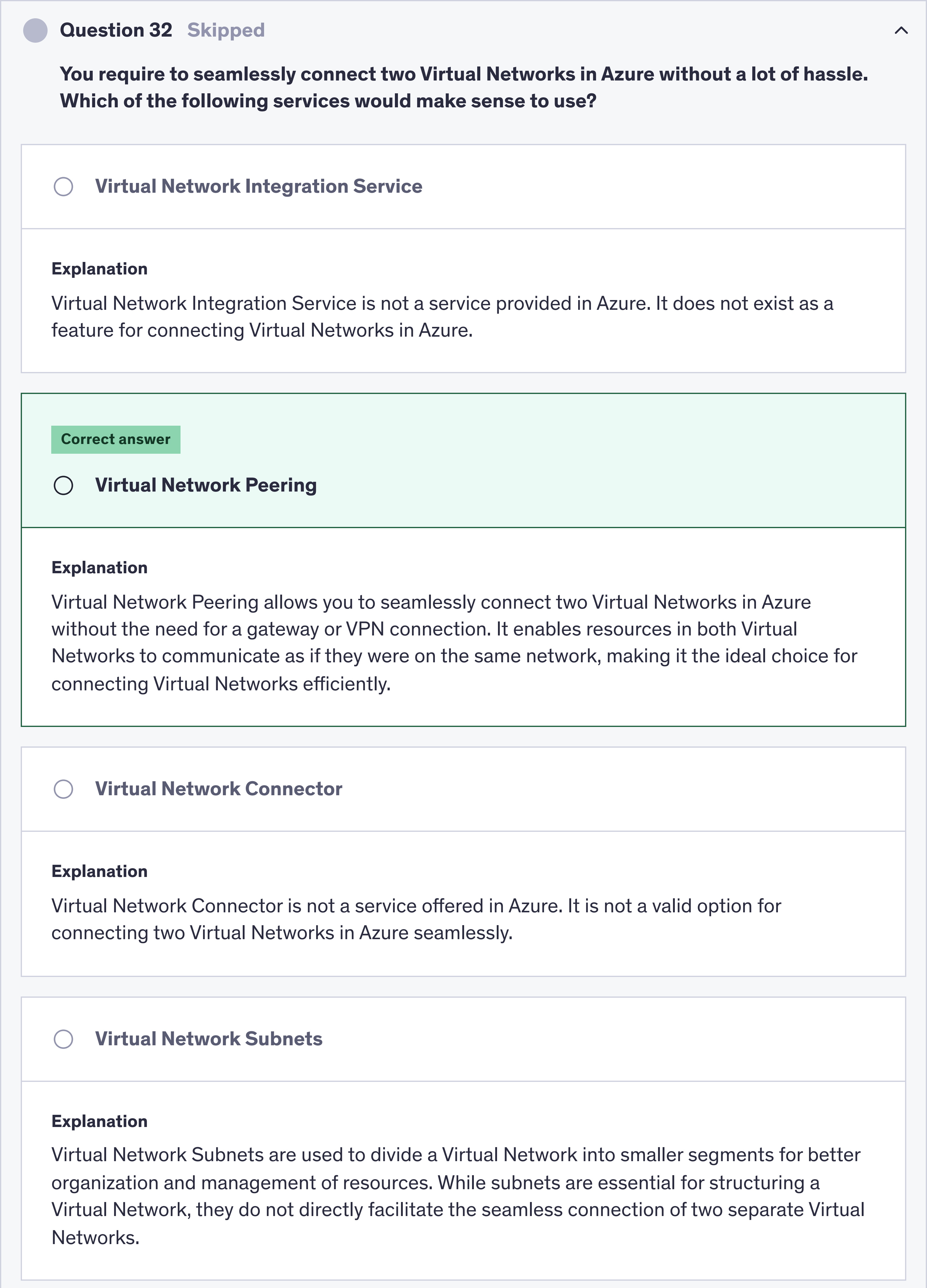
- **Zone-redundant storage (ZRS)** copies your data synchronously across three Azure availability zones in the primary region. For applications requiring high availability, Microsoft recommends using ZRS in the primary region, and also replicating to a secondary region.

- **Geo-zone-redundant storage (GZRS)** combines the high availability provided by redundancy across availability zones with protection from regional outages provided by geo-replication. Data in a GZRS storage account is copied across three Azure availability zones in the primary region and is also replicated to a secondary geographic region for protection from regional disasters.

Reference: https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#geo-redundant-storage

Domain

Describe Azure architecture and services (35–40%)



Question 32 Skipped

You require to seamlessly connect two Virtual Networks in Azure without a lot of hassle. Which of the following services would make sense to use?

○ **Virtual Network Integration Service**

Explanation

Virtual Network Integration Service is not a service provided in Azure. It does not exist as a feature for connecting Virtual Networks in Azure.

Correct answer

○ **Virtual Network Peering**

Explanation

Virtual Network Peering allows you to seamlessly connect two Virtual Networks in Azure without the need for a gateway or VPN connection. It enables resources in both Virtual Networks to communicate as if they were on the same network, making it the ideal choice for connecting Virtual Networks efficiently.

○ **Virtual Network Connector**

Explanation

Virtual Network Connector is not a service offered in Azure. It is not a valid option for connecting two Virtual Networks in Azure seamlessly.

○ **Virtual Network Subnets**

Explanation

Virtual Network Subnets are used to divide a Virtual Network into smaller segments for better organization and management of resources. While subnets are essential for structuring a Virtual Network, they do not directly facilitate the seamless connection of two separate Virtual Networks.

Overall explanation

From the Official Azure Documentation:

Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's *private* network only.

Azure supports the following types of peering:

- **Virtual network peering**: Connecting virtual networks within the same Azure region.
- **Global virtual network peering**: Connecting virtual networks across Azure regions.

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

Domain

Describe Azure architecture and services (35–40%)

● **Question 33** Skipped

A retailer uses Microsoft Entra ID to manage staff access to Azure apps. The following security measures are in place:

- Staff can access apps using **a single login**.
- **A text code** is required for access to sensitive data.
- A **biometric app** is being piloted for sign-ins.

Which of the following best describes the authentication methods being used in this scenario?

○ **Password-Based Authentication, Single Sign-On (SSO), and Conditional Access**

Explanation

Password-Based Authentication is not mentioned in the scenario, as staff are using a single login and a text code for access. Single Sign-On (SSO) is correctly identified as a security measure in place, but Conditional Access is not mentioned. Conditional Access allows organizations to set policies for accessing apps based on specific conditions.

○ **Passwordless Authentication, Single Sign-On (SSO), and Encryption**

Explanation

While Passwordless Authentication is correctly identified as a security measure being piloted with the biometric app, Single Sign-On (SSO) and Encryption are not mentioned in the scenario. SSO allows staff to access multiple apps with a single login, while Encryption is used to protect data at rest and in transit, not specifically mentioned in the scenario.

○ **Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and Conditional Access**

Explanation

While Multi-Factor Authentication (MFA) is correctly identified as a security measure in place, Role-Based Access Control (RBAC) and Conditional Access are not mentioned in the scenario. RBAC is used to manage user access to Azure resources based on their roles, while Conditional Access enforces access controls based on specific conditions.

Correct answer

○ **Single Sign-On (SSO), Multi-Factor Authentication (MFA), and Passwordless Authentication**

Explanation

Single Sign-On (SSO) allows staff to access multiple Azure apps with a single login, improving user experience and security. Multi-Factor Authentication (MFA) adds an extra layer of security by requiring a text code in addition to the password for access to sensitive data. Passwordless Authentication, such as the biometric app being piloted, eliminates the need for passwords and enhances security.

Overall explanation

Correct Answer: Single Sign-On (SSO), Multi-Factor Authentication (MFA), and Passwordless Authentication

- **Single Sign-On (SSO)**: Staff can access multiple Azure apps with **one login**, which is a classic example of SSO.

- **Multi-Factor Authentication (MFA)**: The **text code** required for accessing sensitive data is a form of MFA, as it involves using more than one method of verification (e.g., something you know, like a password, and something you have, like a text code).

- **Passwordless Authentication**: The **biometric app** being piloted for sign-ins is a form of passwordless authentication, as it involves verifying identity without using a traditional password.

Domain

Describe Azure architecture and services (35–40%)

Question 34 Skipped

How does the "compute" layer contribute to the defense-in-depth strategy?

○ **It ensures that services are secure and free of vulnerabilities.**

○ **It prevents unauthorized physical access to hardware.**

○ **It secures access to physical data centers.**

Correct answer

○ **It focuses on securing virtual machines and access to them.**

Overall explanation

From the official docs: The focus in this layer is on making sure that your compute resources are secure and that you have the proper controls in place to minimize security issues.

At this layer, it's important to:

- Secure access to virtual machines.
- Implement endpoint protection on devices and keep systems patched and current.

Therefore, the "compute" layer in the defense-in-depth model concentrates on securing access to virtual machines and ensuring they are properly protected. It involves implementing security controls and measures within the virtual machine environment. This is the best option out of the ones given.

Reference: https://learn.microsoft.com/en-us/training/modules/describe-azure-identity-access-security/8-describe-defense-depth

Domain

Describe Azure architecture and services (35–40%)

Question 35 Skipped

Yes or No:

You can use Azure DNS to buy a domain name.

Correct answer

○ **No**

Explanation

The correct answer is No because Azure DNS does not offer the functionality to buy domain names. Azure DNS is specifically designed for hosting DNS domains and managing DNS records, not for purchasing domain names. Users need to acquire domain names from domain registrars or providers before configuring them in Azure DNS for DNS hosting.

○ Yes

Explanation

Azure DNS is a service provided by Microsoft Azure that allows users to host their DNS domain in Azure. While Azure DNS enables users to manage DNS records for their domain, it does not provide the capability to purchase domain names. Users need to purchase domain names from domain registrars or providers separately and then configure them in Azure DNS for DNS hosting.

Overall explanation

From the Official Azure Documentation:

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records by using the same credentials, APIs, tools, and billing as your other Azure services.

You can't use Azure DNS to buy a domain name. For an annual fee, you can buy a domain name by using App Service domains or a third-party domain name registrar. Your domains then can be hosted in Azure DNS for record management. For more information, see Delegate a domain to Azure DNS.

Reference: https://azure.microsoft.com/en-ca/services/advisor/#features

Domain

Describe Azure architecture and services (35–40%)

● **Question 36** Skipped

In the middle of a critical outage, a distressed intern, unable to access her laptop, logs into a browser, launches a shell, and runs the commands `az vm stop` and `Stop-AzVM` to stop a rogue VM—without needing to install any local tools. Does this scenario demonstrate Azure Cloud Shell's capabilities?

Which of the following best describes the Azure Cloud Shell capabilities demonstrated in this situation?

○ **Cloud Shell's restriction to GUI-based management only**

Explanation

Cloud Shell is not restricted to GUI-based management only. It offers a command-line interface for managing Azure resources, allowing users to run Azure CLI and PowerShell commands directly from the browser-based shell environment.

Correct answer

○ **Cloud Shell's full support for both Azure CLI and PowerShell commands**

Explanation

Cloud Shell provides a browser-based shell experience that supports both Azure CLI and PowerShell commands. In this scenario, the intern was able to run the az vm stop command (Azure CLI) and Stop-AzVM command (PowerShell) to stop the rogue VM without needing to install any local tools, showcasing Cloud Shell's full support for both types of commands.

○ **Cloud Shell's reliance on local tools to run commands**

Explanation

Cloud Shell does not rely on local tools to run commands. It provides a cloud-based shell environment that can be accessed through a browser, eliminating the need to install any tools locally to manage Azure resources.

○ **Cloud Shell's ability to execute scripts only on virtual machines**

Explanation

Cloud Shell's capabilities are not limited to executing scripts only on virtual machines. It allows users to manage Azure resources, run commands, and automate tasks across a wide range of Azure services, not just virtual machines.

Overall explanation

- **Cloud Shell's full support for both Azure CLI and PowerShell commands**: This is the correct answer because Azure Cloud Shell allows users to run both Azure CLI and PowerShell commands directly in the browser, with no need for local tools or installation. The intern is using both the Azure CLI (`az vm stop`) and PowerShell (`Stop-AzVM`) commands, which demonstrates Cloud Shell's full capabilities.

- **Cloud Shell's ability to execute scripts only on virtual machines**: This is incorrect because Azure Cloud Shell is capable of executing a wide range of commands across all Azure resources, not just virtual machines.

- **Cloud Shell's reliance on local tools to run commands**: This is incorrect because Azure Cloud Shell eliminates the need for local tools. It provides a browser-based environment that does not require any software installation on the user's machine.

- **Cloud Shell's restriction to GUI-based management only**: This is incorrect because Azure Cloud Shell is a command-line interface (CLI) and PowerShell environment, not a GUI-based management tool.

Domain

Describe Azure architecture and services (35–40%)

● **Question 37** Skipped

It's possible to deploy an Azure VM from a MacOS based system by using which of the following options?

Correct selection

☐ **Azure Cloudshell**

Correct selection

☐ **Azure Portal**

Correct selection

□ **Azure Powershell**

Correct selection

□ **Azure CLI**

Overall explanation

All of the above can be used to manage Azure resources on a MacOS based system!

Azure Portal - Available for all Operating Systems

Azure CLI - Available for MacOS, Windows and Linux

Azure Powershell - Available to install on MacOS, Windows, Linux, Docker, and Arm (Subset of Azure Cloudshell)

Azure Cloudshell - Azure Cloud Shell is an interactive, authenticated, browser-accessible shell for managing Azure resources. It provides the flexibility of choosing the shell experience that best suits the way you work, either **Bash or PowerShell.**

Reference : https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell-core-on-macos?view=powershell-7

https://docs.microsoft.com/en-us/azure/cloud-shell/overview

https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-macos

Domain

Describe Azure management and governance (30–35%)

● **Question 38** Skipped

Yes or No:

A Resource can only access other resources in the same resource group.

○ Yes

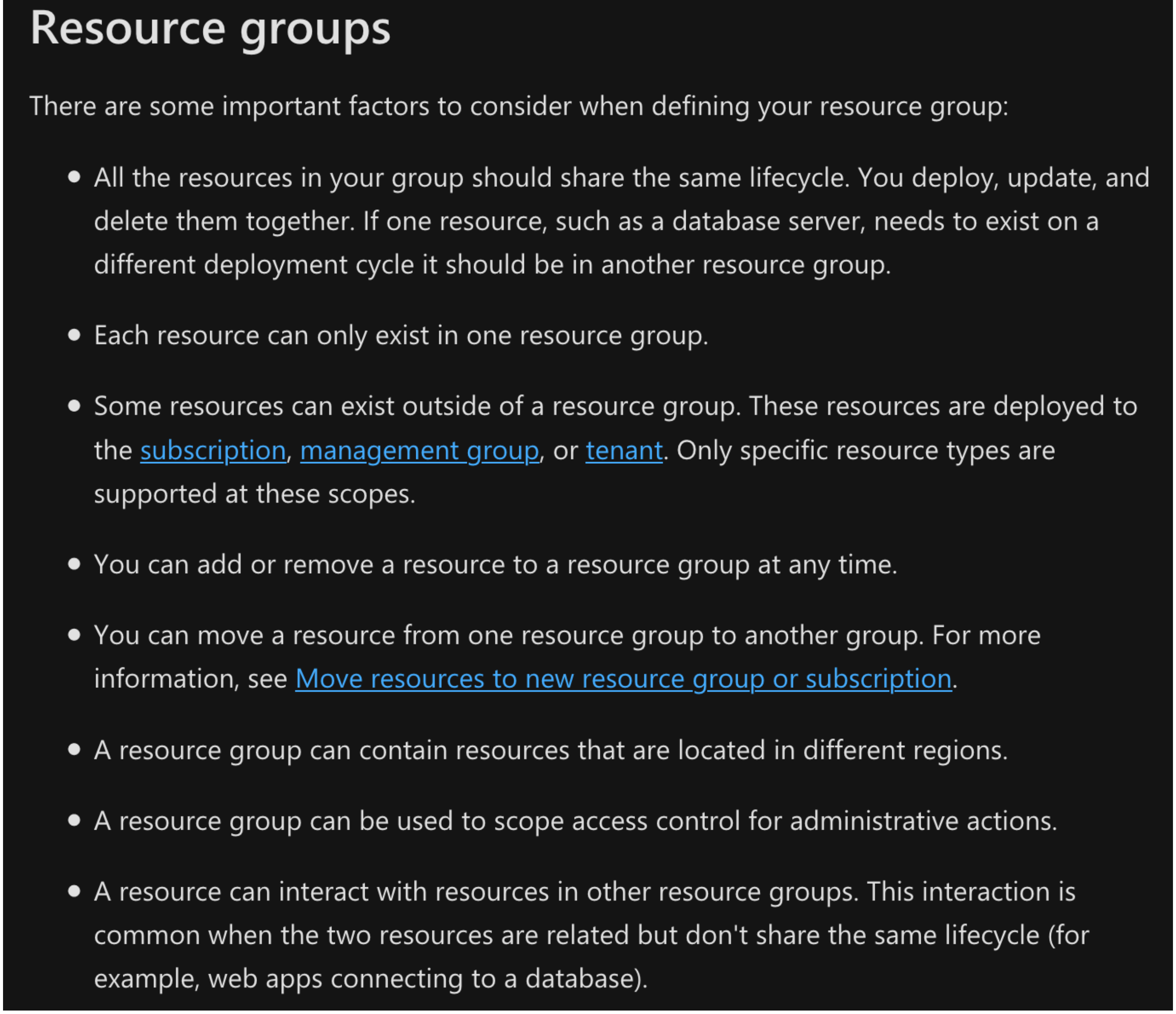
Correct answer

○ No

Overall explanation

From the official Azure documentation:

A resource can connect to resources in other resource groups. This scenario is common when the two resources are related but don't share the same lifecycle. For example, you can have a web app that connects to a database in a different resource group.



Resource groups

There are some important factors to consider when defining your resource group:

- All the resources in your group should share the same lifecycle. You deploy, update, and delete them together. If one resource, such as a database server, needs to exist on a different deployment cycle it should be in another resource group.
- Each resource can only exist in one resource group.
- Some resources can exist outside of a resource group. These resources are deployed to the subscription, management group, or tenant. Only specific resource types are supported at these scopes.
- You can add or remove a resource to a resource group at any time.
- You can move a resource from one resource group to another group. For more information, see Move resources to new resource group or subscription.
- A resource group can contain resources that are located in different regions.
- A resource group can be used to scope access control for administrative actions.
- A resource can interact with resources in other resource groups. This interaction is common when the two resources are related but don't share the same lifecycle (for example, web apps connecting to a database).

Reference : https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview#resource-groups

Domain

Describe Azure management and governance (30–35%)

Question 39 Skipped

A startup has deployed a set of Virtual Machines which are critical for their day-to-day operations. They need to ensure their availability even if a single data center goes down.

One of their interns has suggested that deploying these VMs using a Scale Set would solve the problem. Do you agree?

Correct answer

○ **No**

Explanation

The correct answer is No because deploying Virtual Machines using a Scale Set does not guarantee availability in the event of a data center failure. To ensure high availability across data centers, the startup should consider using Azure Availability Zones or Azure Site Recovery for disaster recovery solutions.

○ **Yes**

Explanation

Deploying Virtual Machines using a Scale Set does not inherently solve the problem of ensuring availability in the event of a data center failure. While Scale Sets can automatically scale the number of VM instances based on demand, they do not provide built-in redundancy across data centers to ensure high availability in case of a data center outage.

Overall explanation

This answer does not specify that the scale set will be configured across multiple data centers so this solution does not meet the goal.

Azure virtual machine scale sets let you create and manage a group of load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update many VMs.

Virtual machines in a scale set can be deployed across multiple update domains and fault domains to maximize availability and resilience to outages due to data center outages, and planned or unplanned maintenance events.

Reference: https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/availability

Domain

Describe cloud concepts (25–30%)

Question 40 Skipped

A healthcare provider secures its Azure environment, classifying sensitive data across storage accounts, monitoring VM performance with alerts, and assessing cloud-wide security posture. Which tools support these tasks? (Select all that apply.)

Correct selection

□ **Azure Monitor**

Explanation

Azure Monitor is a monitoring and alerting service that helps track the performance of virtual machines (VMs) and other resources in the Azure environment. It allows users to set up alerts based on performance metrics to proactively address issues.

Correct selection

□ **Microsoft Defender for Cloud**

Explanation

Microsoft Defender for Cloud is a cloud-native security solution that provides continuous monitoring and assessment of the security posture of the Azure environment. It helps identify and remediate security vulnerabilities and threats across the cloud infrastructure.

□ **Storage Tiers**

Explanation

Storage Tiers are not directly related to the tasks of classifying sensitive data, monitoring VM performance, or assessing cloud-wide security posture. Storage Tiers are used to manage the cost and performance of Azure Storage accounts by storing data in different tiers based on access frequency.

Correct selection

□ **Microsoft Purview**

Explanation

Microsoft Purview is a data governance service that helps organizations discover and classify sensitive data across their Azure environment. It provides insights into data usage and helps maintain compliance with data protection regulations.

Overall explanation

The correct answers are:

Microsoft Purview, for data classification

Azure Monitor, for VM performance and alerts

Microsoft Defender for Cloud, for security assessments

1. **Microsoft Purview**: This tool helps classify and govern sensitive data across various data sources, such as storage accounts. It supports data classification by identifying and tagging sensitive information, which is essential for regulatory compliance in the healthcare industry.
2. **Azure Monitor**: Azure Monitor is used for monitoring the performance of Azure resources like VMs. It enables setting up performance metrics, logging, and alerting, which aligns with the task of monitoring VM performance and setting up alerts based on specific thresholds or conditions.
3. **Microsoft Defender for Cloud**: Microsoft Defender for Cloud is a comprehensive security management tool that assesses and strengthens the security posture of Azure environments. It provides security assessments, identifies vulnerabilities, and offers threat protection across resources, making it an essential tool for security posture management.

Why the other option is incorrect:

- **Storage Tiers, for data cost optimization**: While storage tiers can be useful for optimizing costs by classifying data into different levels (e.g., hot, cool, and archive), this does not directly address the security, monitoring, or classification of sensitive data. Therefore, it's not directly aligned with the tasks mentioned in the question.

Domain

Describe Azure architecture and services (35–40%)

Question 41 Skipped

What is the primary objective of the "Secure" aspect of Defender for Cloud?

○ **To focus on Azure Security Benchmark compliance.**

○ **To deploy Log Analytics agents on all virtual machines.**

○ **To provide protection against physical attacks on datacenters.**

Correct answer

○ **To ensure secure configurations of workloads and resources.**

Overall explanation

The "Secure" aspect of Defender for Cloud aims to ensure that workloads and resources are securely configured. It provides policies and guidelines to help achieve Azure Security Benchmark compliance and secure configurations.

Reference: https://learn.microsoft.com/en-us/training/modules/describe-azure-identity-access-security/9-describe-microsoft-defender-for-cloud

Domain

Describe Azure architecture and services (35–40%)

Question 42 Skipped

Which of the following can be included as artifacts in an Azure Blueprint? (Select all that apply)

Correct selection

□ **Policy assignments**

Correct selection

□ **Resource groups**

Correct selection

□ **Azure Resource Manager templates**

Correct selection

□ **Role assignments**

Overall explanation

All the options are correct. From the official docs: Azure Blueprints deploy a new environment based on all of the requirements, settings, and configurations of the associated artifacts. Artifacts can include things such as:

- Role assignments
- Policy assignments
- Azure Resource Manager templates
- Resource groups

Reference: https://learn.microsoft.com/en-us/training/modules/describe-features-tools-azure-for-governance-compliance/2-describe-purpose-of-azure-blueprints

Domain

Describe Azure management and governance (30–35%)

● **Question 43** Skipped

How do resource locks affect Azure resources?

Correct answer

○ **Resource locks prevent modifications but allow read access.**

Explanation

Resource locks prevent modifications to Azure resources, such as deleting or updating them, but they do allow read access to view the resource properties and configuration settings.

○ **Resource locks restrict any access to the resources.**

Explanation

Resource locks do not restrict any access to the resources. They only prevent modifications to the resources while allowing read access to view the resource properties.

○ **Resource locks completely hide the resources from the Azure portal.**

Explanation

Resource locks do not completely hide resources from the Azure portal. They simply prevent modifications to the resources, but the resources are still visible and accessible in the portal.

○ **Resource locks enforce automatic scaling of resources.**

Explanation

Resource locks do not enforce automatic scaling of resources. They are used to prevent accidental deletion or modification of resources, not to control the scaling behavior of resources.

Overall explanation

From the Azure docs:

As an administrator, you can lock an Azure subscription, resource group, or resource to protect them from accidental user deletions and modifications. The lock overrides any user permissions.

You can set locks that prevent either deletions or modifications. In the portal, these locks are called **Delete** and **Read-only**. In the command line, these locks are called **CanNotDelete** and **ReadOnly**.

- **CanNotDelete** means authorized users can read and modify a resource, but they can't delete it.
- **ReadOnly** means authorized users can read a resource, but they can't delete or update it. Applying this lock is similar to restricting all authorized users to the permissions that the **Reader** role provides.

Based on these definitions, we can still **READ** but not modify/delete the resources. This allows you to view resource configurations without accidentally altering them.

Reference: https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

Domain

Describe Azure management and governance (30–35%)

Question 44 Skipped

An organization has multiple business units, each requiring separate access to Azure resources while maintaining a unified governance model at the top level. The organization wants to ensure that policies and cost management can be applied to each business unit while allowing flexibility in resource management. Which of the following Azure features should be used to accomplish this?

○ **Management Groups for centralized policy management, with Resource Groups grouped by geographic location**

Explanation

Using Management Groups for centralized policy management and organizing Resource Groups by geographic location may not align with the organization's goal of maintaining separate access for each business unit. This approach may not provide the necessary flexibility in resource management for each business unit.

Correct answer

○ **Azure Management Groups, with Resource Groups organized by business unit**

Explanation

Azure Management Groups allow for centralized policy management and cost control across multiple subscriptions. By organizing Resource Groups by business unit under Management Groups, the organization can maintain a unified governance model while providing flexibility in resource management within each business unit.

○ **Resource Groups and Subscriptions for each business unit, with policies applied at the subscription level**

Explanation

Using Resource Groups and Subscriptions for each business unit with policies applied at the subscription level can provide isolation and governance at the business unit level. However, it may not offer the flexibility needed for resource management within each business unit.

○ **Resource Groups within a single subscription, and policies applied to the resources directly**

Explanation

While organizing Resource Groups within a single subscription and applying policies directly to the resources can provide some level of governance, it may not be the most efficient approach for managing multiple business units with separate access requirements.

Overall explanation

Azure Management Groups allow for centralized policy enforcement across multiple subscriptions. By organizing business units under different Management Groups and applying governance and policies at the management group level, the organization can ensure consistent access control, policy enforcement, and cost management across its Azure environment.

Domain

Describe Azure architecture and services (35–40%)

● **Question 45** Skipped

Azure strives to ensure a minimum distance of _______________ miles between datacenters in enabled regions, although it isn't possible across all geographies.

○ **200**

○ **400**

Correct answer

○ **300**

Explanation

Azure strives to maintain a minimum distance of 300 miles between datacenters in enabled regions to enhance data redundancy, availability, and disaster recovery capabilities. This distance helps ensure that data is stored in geographically dispersed locations to minimize the risk of data loss.

○ **500**

Overall explanation

From the official Azure Docs:

Azure strives to ensure a minimum distance of 300 miles (483 kilometers) between datacenters in enabled regions, although it isn't possible across all geographies. Datacenter separation reduces the likelihood that natural disaster, civil unrest, power outages, or physical network outages can affect multiple regions. Isolation is subject to the constraints within a geography, such as geography size, power or network infrastructure availability, and regulations.

Reference : https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions

Domain

Describe Azure architecture and services (35–40%)

● **Question 46** Skipped

A gaming company tracks its Azure app, querying VM logs for errors, setting CPU usage alerts, and diagnosing crashes. Which Azure Monitor components are in use?

Correct selection

□ **Log Analytics**

Explanation

Log Analytics is used by the gaming company to query VM logs for errors and diagnose crashes. It provides advanced analytics and insights into the performance and health of the virtual machines, helping the company troubleshoot issues effectively.

Correct selection

□ **Application Insights**

Explanation

Application Insights is used by the gaming company to monitor the performance and usage of their Azure app. It helps track user interactions, diagnose issues, and improve overall user experience by providing detailed insights into application behavior.

Correct selection

□ **Azure Monitor Alerts**

Explanation

Azure Monitor Alerts are used by the gaming company to set CPU usage alerts and receive notifications when certain thresholds are exceeded. This component helps the company proactively monitor and manage the performance of their Azure resources.

□ **Azure Service Health**

Explanation

Azure Service Health is not directly related to the specific monitoring activities mentioned by the gaming company. It provides information about the health of Azure services and regions, helping users stay informed about any service disruptions or planned maintenance events.

Overall explanation

The correct answer is:

Log Analytics
Azure Monitor Alerts
Application Insights

Log Analytics:

- **Log Analytics** is part of **Azure Monitor** that allows you to query logs from your Azure resources. In the case of the gaming company, **querying VM logs for errors** falls under **Log Analytics**, which helps to analyze and search through logs generated by resources in Azure.

Azure Monitor Alerts:

- **Azure Monitor Alerts** are used to create **notifications** or actions based on certain metrics or events. In the case of setting **CPU usage alerts**, this falls under **Azure Monitor Alerts**, which helps detect threshold breaches or anomalies and notifies administrators or takes automated actions.

Application Insights:

- **Application Insights** is part of **Azure Monitor** and is specifically designed for monitoring and diagnosing application performance. It is used to diagnose issues like **app crashes** and **performance bottlenecks** in real time. The gaming company would use this to track errors, crashes, and overall application health.

Azure Service Health:

- **Azure Service Health** provides alerts and guidance when Azure services are experiencing issues or undergoing maintenance. However, it is **not** typically used to track individual application or VM logs and crashes, so it does not apply in this scenario.

Domain

Describe Azure management and governance (30–35%)

Question 47 Skipped

____________ is a bridge that extends the Azure platform to help you build applications and services with the flexibility to run across datacenters, at the edge, and in multicloud

environments. It also simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.

○ **Azure Bridge**

Explanation

Azure Bridge is not a recognized service or feature within the Microsoft Azure platform. It does not exist as a tool or service that extends the Azure platform to enable building applications and services with the flexibility to run across datacenters, at the edge, and in multicloud environments.

○ **Azure DNS**

Explanation

Azure DNS is a domain name system (DNS) hosting service provided by Microsoft Azure for managing domain names and mapping them to IP addresses. While DNS is essential for resolving domain names to IP addresses, it does not serve as a bridge to extend the Azure platform for building applications and services across different environments as described in the question.

Correct answer

○ **Azure Arc**

Explanation

Azure Arc is the correct choice as it is a service provided by Microsoft Azure that extends the Azure platform to enable the development of applications and services that can run across different environments such as datacenters, edge locations, and multicloud setups. It also offers a consistent management platform for both on-premises and multi-cloud environments, simplifying governance and management tasks.

○ **Azure Sentinel**

Explanation

Azure Sentinel is a cloud-native security information and event management (SIEM) service provided by Microsoft Azure. While it focuses on security monitoring and threat detection, it does not specifically address the requirements mentioned in the question related to building applications and services that can run across different environments.

Overall explanation

From the Official Azure Documentation:

Azure Arc is a bridge that extends the Azure platform to help you build applications and services with the flexibility to run across datacenters, at the edge, and in multicloud environments. Develop cloud-native applications with a consistent development, operations, and security model. Azure Arc runs on both new and existing hardware, virtualization and Kubernetes platforms, IoT devices, and integrated systems.

Today, companies struggle to control and govern increasingly complex environments that extend across data centers, multiple clouds, and edge. Each environment and cloud possesses its own set of management tools, and new DevOps and ITOps operational models can be hard to implement across resources.

Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.

Reference: https://docs.microsoft.com/en-us/azure/azure-arc/overview

Domain

Describe Azure architecture and services (35–40%)

● **Question 48** Skipped

A healthcare provider classifies sensitive patient data in Azure Blob Storage and on-premises SQL servers, ensuring compliance with privacy laws. Which Azure tool supports this data governance?

○ **Azure Cost Management**

Explanation

Azure Cost Management is a tool that helps organizations monitor and optimize their Azure spending. While it is essential for cost management and optimization, it is not designed for data governance and classification tasks like Microsoft Purview.

○ **Azure Policy**

Explanation

Azure Policy is a tool that allows organizations to enforce governance policies for their Azure resources. While it can help with overall governance and compliance, it is not specifically designed for data classification and protection like Microsoft Purview.

Correct answer

○ **Microsoft Purview**

Explanation

Microsoft Purview is a data governance tool in Azure that helps organizations discover, classify, and protect sensitive data across hybrid environments. It provides insights into data usage, helps maintain compliance with privacy laws, and enables organizations to track data lineage and governance policies.

○ **Microsoft Defender for Cloud**

Explanation

Microsoft Defender for Cloud is a security tool that helps organizations protect their cloud resources from threats and vulnerabilities. While it plays a crucial role in overall security, it is not focused on data governance and classification like Microsoft Purview.

Overall explanation

The correct answer is: **Microsoft Purview**

- **Microsoft Purview** is an Azure data governance tool that helps with the classification, labeling, and management of sensitive data across both cloud and on-premises environments. It ensures compliance with data privacy laws by enabling organizations to discover, classify, and protect sensitive data. In the scenario described, it would classify sensitive patient data in **Azure Blob Storage** and on-premises **SQL servers** to ensure compliance with privacy regulations.

Why the other options aren't the best fit:

- **Azure Policy**: This is primarily used for enforcing organizational standards and compliance across Azure resources (such as ensuring that certain resource configurations are compliant with rules) but is not specifically focused on data classification or governance.

- **Microsoft Defender for Cloud**: While it focuses on security and threat detection, it is not specifically designed for data classification or governance. It helps protect resources against potential threats but does not classify or manage data for compliance purposes.

- **Azure Cost Management**: This tool is focused on managing and optimizing cloud costs, not data governance or compliance.

Domain

Describe Azure management and governance (30–35%)

Question 49 Skipped

Yes or No:

______________ notifies you about Azure service incidents and planned maintenance so you can take action to mitigate downtime.

Correct answer

○ **Azure Service Health**

Explanation

Azure Service Health is the correct choice as it is specifically designed to notify users about Azure service incidents and planned maintenance. It provides real-time status updates, incident details, and proactive notifications to help users take necessary actions to mitigate downtime.

○ **Azure Health Bot**

Explanation

Azure Health Bot is not the correct choice for this scenario. While it may provide health-related information and support, it is not specifically focused on notifying users about Azure service incidents and planned maintenance.

○ **Azure Percept**

Explanation

Azure Percept is not the correct choice for this scenario. Azure Percept is a platform for creating edge AI solutions, and it is not designed to notify users about Azure service incidents and planned maintenance.

○ **Azure Chaos Studio**

Explanation

Azure Chaos Studio is not the correct choice for this scenario. Azure Chaos Studio is a tool for chaos engineering experiments to test the resilience of cloud applications, and it is not intended to notify users about Azure service incidents and planned maintenance.

Overall explanation

From the Official Azure Documentation:

Azure Service Health notifies you about Azure service incidents and planned maintenance so you can take action to mitigate downtime. Configure customisable cloud alerts and use your personalised dashboard to analyse health issues, monitor the impact to your cloud resources, get guidance and support, and share details and updates.

Reference: https://azure.microsoft.com/en-ca/features/service-health/#overview

Domain

Describe Azure management and governance (30–35%)

● **Question 50** Skipped

How does Azure Blueprints help in monitoring deployments?

Correct answer

○ **By preserving the relationship between blueprint definition and blueprint assignment**

Explanation

Azure Blueprints help in monitoring deployments by preserving the relationship between blueprint definition and blueprint assignment. This ensures that the deployed resources adhere to the defined blueprint, making it easier to track and manage deployments.

○ **By providing real-time monitoring of resource usage**

Explanation

Azure Blueprints do not directly provide real-time monitoring of resource usage. They are used for defining a repeatable set of Azure resources that can be deployed consistently and securely.

○ **By sending email notifications when a deployment reaches a certain milestone**

Explanation

Azure Blueprints do not have the functionality to send email notifications when a deployment reaches a certain milestone. Notifications and alerts for deployments can be set up using Azure Monitor or other monitoring tools within Azure.

○ **By automatically suspending resources when they reach a certain cost threshold**

Explanation

Azure Blueprints do not have the capability to automatically suspend resources when they reach a certain cost threshold. This functionality is typically managed through Azure Cost Management and Azure Policy.

Overall explanation

Azure Blueprints helps in monitoring deployments by preserving the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed). This connection allows you to track and audit your deployments effectively.

Other options:

- Azure Blueprints doesn't provide real-time monitoring of resource usage. It focuses on standardizing and automating environment deployments based on predefined configurations.
- **Automatically suspending resources when they reach a certain cost threshold** is not a function of Azure Blueprints. It is more related to cost management features like budgets and cost alerts.
- **Sending email notifications when a deployment reaches a certain milestone** is not a feature specific to Azure Blueprints. This could be achieved through other Azure services or custom monitoring solutions.

Reference: https://learn.microsoft.com/en-us/training/modules/describe-features-tools-azure-for-governance-compliance/2-describe-purpose-of-azure-blueprints

Domain

Describe Azure management and governance (30–35%)

● **Question 51** Skipped

How can JSON strings be used to assign more than the maximum number of allowed tags to an Azure resource?

○ By creating additional subscriptions

Correct answer

○ **By including multiple values for a single tag name**

○ By creating additional tag names

○ By creating additional resource groups

Overall explanation

The correct answer is **'By including multiple values for a single tag name'.**

When you need to assign more than the maximum number of allowed tags to an Azure resource, you can use JSON strings to include multiple values for a single tag name. This approach allows you to apply more tag values than the limit allows while maintaining compliance with Azure's tag limit. The JSON string should be added as the tag value, and it should contain a comma-separated list of values that you want to apply to the tag.

Reference: https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json#limitations

Domain

Describe Azure management and governance (30–35%)

● **Question 52** Skipped

A university manages its Azure resources, grouping VMs and storage for a research project, billing them under a single entity, and applying compliance policies across multiple such entities campus-wide. Which components form this hierarchy? (Select all that apply.)

□ Public Endpoints

Explanation

Public Endpoints are not part of the hierarchy for managing Azure resources, grouping VMs and storage, billing, and applying compliance policies. Public Endpoints are used to expose services or resources to the public internet, and they are not directly related to resource management and compliance across multiple entities.

Correct selection

□ Resource Groups

Explanation

Resource Groups in Azure allow organizations to group Azure resources together, such as VMs and storage accounts, for easier management, billing, and compliance. They provide a way to manage and apply policies to a collection of resources as a single entity.

Correct selection

□ Management Groups

Explanation

Management Groups in Azure provide a way to manage access, policies, and compliance across multiple subscriptions. They allow organizations to apply policies and controls at scale across different subscriptions, providing a way to manage resources campus-wide under a single entity.

Correct selection

□ Subscriptions

Explanation

Subscriptions in Azure are used to group and manage billing for Azure resources. They allow organizations to manage access, limits, and compliance across multiple resources within the subscription. Subscriptions are used to organize and manage resources at a higher level.

Overall explanation

The correct answers are:

Resource Groups, for project resource organization

- **Resource Groups** are used to organize resources like VMs and storage accounts. They allow the university to group related resources for a specific project, like a research project, and manage them collectively. Resource Groups provide a logical container for Azure resources and help in managing them easily.

Subscriptions, for billing and access boundaries

- **Subscriptions** define billing boundaries and provide access management boundaries in Azure. By assigning resources to different subscriptions, the university can manage and track costs effectively for different projects or departments. Each subscription is linked to a specific billing account and can contain multiple resource groups.

Management Groups, for campus-wide policy enforcement

- **Management Groups** are used to organize and manage multiple Azure subscriptions at a higher level. In this case, the university can use management groups to enforce policies, governance, and compliance across its entire campus, including the different research projects. Management Groups allow for policy enforcement across multiple subscriptions and resource groups.

Why **Public Endpoints** is incorrect:

- **Public Endpoints** refer to the IP addresses and network settings used to allow external access to Azure resources like VMs, databases, etc. They are not related to the hierarchy or organization of resources for billing, access management, or policy enforcement.

Domain

Describe Azure management and governance (30–35%)

● **Question 53** Skipped

Which of the following are appropriate use cases for these cloud models? (Select all that apply.)

Correct selection

□ **Private cloud for a financial institution requiring strict data isolation**

Explanation

Private cloud is ideal for a financial institution that requires strict data isolation and security. Financial institutions deal with sensitive customer data and regulatory requirements, making a private cloud environment the best option to ensure data privacy and compliance.

Correct selection

□ **Hybrid cloud for a retailer combining on-premises inventory systems with cloud-based analytics**

Explanation

Hybrid cloud is a good fit for a retailer that wants to combine on-premises inventory systems with cloud-based analytics. Retailers often have existing infrastructure in place and can benefit from the flexibility and scalability of the cloud for data analysis and insights while maintaining control over critical inventory systems.

Correct selection

□ **Public cloud for a startup needing cost-effective, scalable web hosting**

Explanation

Public cloud is suitable for a startup as it provides cost-effective and scalable web hosting services. Startups often have limited resources and need flexibility to scale their operations as they grow, making public cloud an ideal choice for meeting their hosting needs.

☐ **Public cloud for a hospital needing full control over patient data security**

Explanation

Public cloud may not be the best choice for a hospital needing full control over patient data security. Hospitals deal with highly sensitive patient information that requires strict security and compliance measures. A private cloud or on-premises solution may be more suitable for ensuring full control and security over patient data.

Overall explanation

Public cloud for a startup needing cost-effective, scalable web hosting:

- **Correct**. The **Public Cloud** is a great fit for a startup that needs to scale quickly and cost-effectively. It allows them to access computing resources without the need to invest in physical infrastructure, making it ideal for web hosting, especially for small and growing businesses.

Private cloud for a financial institution requiring strict data isolation

- **Correct**. A **Private Cloud** is suitable for businesses like a financial institution that requires tight control over security and data isolation. This model provides dedicated resources that are not shared with other tenants, which is important for compliance with regulations and handling sensitive financial data.

Hybrid cloud for a retailer combining on-premises inventory systems with cloud-based analytics

- **Correct**. A **Hybrid Cloud** is appropriate when a retailer needs to integrate on-premises legacy systems (such as inventory management) with cloud-based services (such as analytics). This model allows the company to keep some systems on-premises while using the cloud for other functionalities, offering flexibility and scalability.

Public cloud for a hospital needing full control over patient data security

- **Incorrect**. For a hospital dealing with sensitive patient data, full control over data security is essential due to compliance with regulations like HIPAA (Health Insurance Portability and Accountability Act). A **Private Cloud** or a **Hybrid Cloud** would be more appropriate because it allows for better control over security and data privacy. The **Public Cloud**, while cost-effective and scalable, typically doesn't offer the level of control and isolation required for highly sensitive data like patient health records.

Domain

Describe cloud concepts (25–30%)

● **Question 54** Skipped

A company wants to deploy a high-availability solution for their virtual desktop infrastructure (VDI) using Azure. They aim to provide scaling capabilities based on user demand, with automatic load balancing and distribution across multiple instances of virtual machines (VMs). Which of the following Azure services would be best suited for this requirement?

Correct answer

○ **Azure Virtual Desktop (AVD) with Azure Scale Sets**

Explanation

Azure Virtual Desktop (AVD) with Azure Scale Sets is the best choice for this requirement. Azure Scale Sets allow for automatic scaling of VM instances based on demand, ensuring high availability and load balancing across multiple instances. This combination provides the necessary scalability and distribution for a high-availability VDI solution.

○ **Azure Virtual Machine Scale Sets (VMSS) with Azure Load Balancer**

Explanation

Azure Virtual Machine Scale Sets (VMSS) with Azure Load Balancer is not the ideal solution for this requirement. While VMSS allows for automatic scaling of VM instances, it does not specifically cater to virtual desktop infrastructure needs like AVD. Azure Load Balancer alone may not provide the necessary capabilities for load balancing and distribution in a VDI environment.

○ **Azure Virtual Machines (VMs) deployed with Availability Zones**

Explanation

Azure Virtual Machines (VMs) deployed with Availability Zones is not the most suitable option for this requirement. While Availability Zones provide high availability by distributing VMs across different data centers within a region, they do not offer automatic scaling capabilities based on user demand, which is essential for a VDI solution with scaling requirements.

○ **Azure Virtual Desktop (AVD) combined with Azure Availability Sets**

Explanation

Azure Virtual Desktop (AVD) combined with Azure Availability Sets is not the best option for this requirement. While Azure Availability Sets provide high availability by distributing VMs across multiple fault domains, they do not offer automatic scaling capabilities based on user demand.

Overall explanation

Azure Virtual Desktop (AVD) is specifically designed for managing and scaling VDI environments. Azure Scale Sets allow for the automatic scaling of VM instances based on demand, and when used with AVD, they help manage the load of virtual desktops effectively across multiple instances.

Domain

Describe Azure architecture and services (35–40%)

● **Question 55** Skipped

A(n) _______________ lets you run legacy applications in the cloud that can't use modern authentication methods, or where you don't want directory lookups to always go back to an on-premises AD DS environment

○ **Azure Migrate deployment**

Explanation

Azure Migrate deployment is a service that helps you assess and migrate your on-premises workloads to Azure. It is not related to running legacy applications in the cloud or addressing authentication methods for those applications.

Correct answer

○ **Microsoft Entra Domain Services**

Explanation

Microsoft Entra Domain Services allows you to run legacy applications in the cloud that cannot use modern authentication methods. It provides a managed domain service that is compatible with traditional Active Directory environments, allowing you to avoid directory lookups going back to an on-premises AD DS environment.

○ **Azure Active Directory External Identities**

Explanation

Azure Active Directory External Identities is a service that allows you to provide secure access to your applications for external users. It is not specifically designed for running legacy applications in the cloud or addressing the need for traditional authentication methods.

○ **Azure Single Sign On (SSO)**

Explanation

Azure Single Sign On (SSO) is a service that allows users to access multiple applications with a single set of credentials. While it simplifies the authentication process, it is not specifically designed for running legacy applications in the cloud or addressing the need for traditional authentication methods.

Overall explanation

From the Official Azure Documentation:

Microsoft Entra Domain Services provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. You use these domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.

An Azure AD DS managed domain lets you run **legacy** applications in the cloud that can't use modern authentication methods, or where you don't want directory lookups to always go back to an on-premises AD DS environment. You can lift and shift those legacy applications from your on-premises environment into a managed domain, without needing to manage the AD DS environment in the cloud.

Azure AD DS integrates with your existing Azure AD tenant. This integration lets users sign in to services and applications connected to the managed domain using their existing credentials. You can also use existing groups and user accounts to secure access to resources. These features provide a smoother lift-and-shift of on-premises resources to Azure.

Reference: https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview

Domain

Describe Azure architecture and services (35–40%)

Question 56 Skipped

______________ is a command-line utility that you can use to copy blobs or files to or from a storage account.

Correct answer

○ **AzCopy**

Explanation

AzCopy is a command-line utility provided by Microsoft that allows users to copy blobs or files to and from Azure storage accounts. It is a versatile tool that supports various transfer options, including parallel transfer, resume functionality, and more, making it a popular choice for managing data in Azure storage.

○ **AzMigrate**

Explanation

AzMigrate is not a valid command-line utility provided by Microsoft for copying blobs or files to or from Azure storage accounts. To effectively manage data transfer operations in Azure storage, it is crucial to utilize the correct tool, such as AzCopy, which is specifically designed for this purpose.

○ **AzReplicate**

Explanation

AzReplicate is not a valid command-line utility provided by Microsoft for copying blobs or files to and from Azure storage accounts. When working with Azure storage, it is essential to use the appropriate tools like AzCopy to ensure seamless data transfer operations and avoid any potential issues.

○ **AzMove**

Explanation

AzMove is not a valid command-line utility provided by Microsoft for copying blobs or files to and from Azure storage accounts. It is important to use the correct tool, which in this case is AzCopy, to ensure efficient and reliable data transfer operations.

Overall explanation

From the Official Azure Documentation:

AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

Example of a command -

```
azcopy make 'https://mystorageaccount.file.core.windows.net/myfileshare?
sv=2018-03-28&ss=bjqt&srs=sco&sp=rjklhjup&se=2019-05-10T04:37:48Z&st=2019-05-
09T20:37:48Z&spr=https&sig=%2FSOVEFfsKDqRry4bk3qz1vAQFwY5DDzp2%2B%2F3Eykf%2FJLs%3D'
```

Reference: https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10

Domain

Describe Azure architecture and services (35–40%)

● **Question 57** Skipped

A company uses the ________ Calculator to estimate monthly Azure VM costs and the ________ Calculator to compare five-year savings against an on-premises datacenter.

○ **Pricing, Total Cost of Migration**

Explanation

No "Total Cost of Migration" Calculator exists.

○ **Total Cost of Ownership, Pricing**

Explanation

Opposite order, so wrong.

Correct answer

○ **Pricing, Total Cost of Ownership**

Explanation

The Pricing Calculator is specifically designed to provide detailed pricing information for Azure services, including VMs, storage, networking, and more. It helps users estimate the costs associated with using Azure services. The Total Cost of Ownership (TCO) Calculator, on the other hand, is used to compare the total cost of ownership over a specified period, typically five years, including factors such as hardware, software, maintenance, and operational costs.

○ **Estimation, Pricing**

Explanation

The Estimation Calculator is not a specific tool used in Azure for cost estimation. The Pricing Calculator, however, is used to estimate the costs associated with using Azure services. The Total Cost of Ownership (TCO) Calculator is used to compare the total cost of ownership over a specified period, typically five years, against an on-premises datacenter.

Overall explanation

The correct answer is: **Pricing Calculator** to estimate monthly Azure VM costs and **TCO Calculator** to compare five-year savings against an on-premises datacenter.

- **Pricing Calculator**: This tool is used to estimate the cost of using various Azure resources, including virtual machines (VMs). It helps users to calculate how much they will spend monthly based on their selected services, regions, and configurations. This tool allows you to estimate costs before deployment.

- **TCO (Total Cost of Ownership) Calculator**: This tool helps users compare the total cost of running workloads on Azure with the cost of maintaining an on-premises datacenter. It provides insights into potential savings over a period (like five years) and takes into account factors like energy, hardware, maintenance, and personnel costs associated with on-prem infrastructure.

Domain

Describe Azure management and governance (30–35%)

● **Question 58** Skipped

You are looking to link resources together in your on-premises environment and within your Azure subscription but don't want the connection to travel over the internet. Which of the following can you use?

○ **Azure Site-to-Site VPN**

Explanation

Azure Site-to-Site VPN allows you to securely connect your on-premises network to Azure over the public internet. While it provides a VPN connection, it does not offer a private connection that does not travel over the internet.

○ **Azure Bastion**

Explanation

Azure Bastion is a service that allows you to securely connect to your Azure virtual machines over the Internet using RDP or SSH without exposing them to the public internet. It does not provide a private connection between on-premises resources and Azure without traveling over the internet.

○ **Azure Point-to-Site VPN**

Explanation

Azure Point-to-Site VPN allows individual devices to securely connect to Azure resources over the public internet. It does not provide a private connection between on-premises resources and Azure without traveling over the internet.

○ **Azure Sentinel**

Explanation

Azure Sentinel is a cloud-native SIEM (Security Information and Event Management) service that uses AI and automation to help analyze security threats. It is not designed for creating private connections between on-premises resources and Azure without using the internet.

Correct answer

○ **Azure ExpressRoute**

Explanation

Azure ExpressRoute provides a private, dedicated connection between your on-premises datacenter or network and Azure. It does not rely on the public internet, offering a more secure and reliable connection for transferring data between on-premises and Azure resources.

Overall explanation

From the Official Azure Documentation:

Azure virtual networks enable you to link resources together in your on-premises environment and within your Azure subscription. In effect, you can create a network that spans both your local and cloud environments. There are three mechanisms for you to achieve this connectivity:

- **Point-to-site virtual private networks** The typical approach to a virtual private network (VPN) connection is from a computer outside your organization, back into your corporate network. In this case, the client computer initiates an encrypted VPN connection to connect that computer to the Azure virtual network.

- **Site-to-site virtual private networks** A site-to-site VPN links your on-premises VPN device or gateway to the Azure VPN gateway in a virtual network. In effect, the devices in Azure can appear as being on the local network. The connection is encrypted and works over the internet.

- **Azure ExpressRoute** For environments where you need greater bandwidth and even higher levels of security, Azure ExpressRoute is the best approach. ExpressRoute provides a dedicated private connectivity to Azure that doesn't travel over the internet.

Reference: https://docs.microsoft.com/en-ca/learn/modules/azure-networking-fundamentals/azure-virtual-network-fundamentals

Domain

Describe Azure architecture and services (35–40%)

Question 59 Skipped

What is the key difference between vertical scaling and horizontal scaling?

Correct answer

○ **Horizontal scaling adjusts the number of resources, while vertical scaling adjusts capabilities.**

Explanation

Horizontal scaling involves adding more resources, such as additional servers or instances, to distribute the workload across multiple machines. This allows for increased capacity and improved performance by handling more requests simultaneously. On the other hand, vertical scaling increases the capabilities of a single resource, such as adding more CPU, memory, or storage to a single server, to handle increased workloads efficiently.

○ **Vertical scaling is automatic, while horizontal scaling requires manual intervention.**

○ **Vertical scaling only applies to virtual machines, while horizontal scaling applies to containers.**

Explanation

Vertical scaling and horizontal scaling are both applicable to various types of resources, including virtual machines and containers. Vertical scaling involves increasing the capacity of a single resource, while horizontal scaling involves adding more resources to distribute the workload.

○ **Vertical scaling adds more processing power, while horizontal scaling increases storage capacity.**

Overall explanation

Vertical scaling involves adjusting the number of resources, such as CPUs or RAM. Horizontal scaling, on the other hand, involves adding or subtracting resources to adjust capabilities, such as adding more virtual machines.

Reference: https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json

Domain

Describe cloud concepts (25–30%)

● **Question 60** Skipped

Which of the following alert types are available in the Cost Management service? (Select all that apply)

□ **Resource usage alerts**

Correct selection

□ **Budget alerts**

Correct selection

□ **Department spending quota alerts**

Correct selection

□ Credit alerts

Overall explanation

- **Budget alerts:** Correct. Budget alerts notify you when spending, based on usage or cost, reaches or exceeds the amount defined in the alert condition of the budget.

- **Credit alerts:** Correct. Credit alerts notify you when your Azure credit monetary commitments are consumed. Monetary commitments are for organizations with Enterprise Agreements (EAs).

- **Department spending quota alerts:** Correct. Department spending quota alerts notify you when department spending reaches a fixed threshold of the quota. Spending quotas are configured in the EA portal.

Other options -

- **Resource usage alerts:** Incorrect. Resource usage alerts are not part of the Cost Management service. Cost Management focuses on costs, budgets, and spending alerts.

Reference: https://learn.microsoft.com/en-us/training/modules/describe-cost-management-azure/6-describe-azure-tool

Domain

Describe Azure management and governance (30–35%)

● **Question 61** Skipped

A _______________ can enable branch offices to share sensitive information between locations.

○ DNS

Explanation

DNS (Domain Name System) is responsible for translating domain names into IP addresses, and it is not directly related to enabling branch offices to share sensitive information securely between locations. While DNS is essential for internet communication, it does not provide the necessary security features for sensitive data sharing.

○ **Bastion**

Explanation

A Bastion host is a special-purpose computer on a network specifically designed and configured to withstand attacks. While it can enhance security by providing a controlled access point for administrators, it is not primarily used to enable branch offices to share sensitive information securely between locations.

○ **Bridge**

Explanation

A Bridge is a network device that connects multiple network segments together, but it does not provide the necessary security features to enable branch offices to securely share sensitive information between locations. Bridges are used for network connectivity and segmentation, not for secure data transmission.

Correct answer

○ **VPN**

Explanation

A VPN (Virtual Private Network) creates a secure, encrypted connection over the internet, allowing branch offices to securely share sensitive information between locations. It provides a private network that ensures data confidentiality and integrity during transmission.

Overall explanation

From the Official Azure Documentation:

VPNs use an encrypted tunnel within another network. They're typically deployed to connect two or more trusted private networks to one another over an untrusted network (typically the public internet). Traffic is encrypted while traveling over the untrusted network to prevent eavesdropping or other attacks.

VPNs can enable branch offices to share sensitive information between locations. For example, let's say that your offices on the East coast region of North America need to access your company's private customer data, which is stored on servers that are physically located in a West coast region. A VPN can connect your East coast offices to your West coast servers allowing your company to securely access your private customer data.

Reference: https://docs.microsoft.com/en-ca/learn/modules/azure-networking-fundamentals/azure-vpn-gateway-fundamentals

Domain

Describe Azure architecture and services (35–40%)

Question 62 Skipped

_____________ devices can easily move data to Azure when busy networks aren’t an option.

○ **Azure Storage Explorer**

Explanation

Azure Storage Explorer is a tool that allows users to interact with Azure storage services through a graphical interface. While it facilitates managing and accessing Azure storage resources, it is not specifically designed for offline data transfer when network conditions are challenging.

Correct answer

○ **Azure Data Box**

Explanation

Azure Data Box is a physical device provided by Microsoft that allows for offline data transfer to Azure. It is designed for scenarios where network bandwidth is limited or unreliable, enabling large amounts of data to be easily moved to Azure without relying on busy networks.

○ **Azure File Sync**

Explanation

Azure File Sync is a service that enables synchronization of on-premises file servers with Azure Files. It is focused on file synchronization and collaboration, rather than offline data transfer in scenarios where busy networks are not an option.

○ **Azure Migrate**

Explanation

Azure Migrate is a service that helps organizations assess and migrate their on-premises workloads to Azure. While it facilitates the migration process, it is not specifically designed for offline data transfer when network conditions are not optimal.

Overall explanation

From the Official Azure Documentation:

Azure Data Box devices easily move data to Azure when busy networks aren’t an option. Move large amounts of data to Azure when you're limited by time, network availability, or costs, using common copy tools such as Robocopy. All data is AES-encrypted, and the devices are wiped clean after upload, in accordance with NIST Special Publication 800-88 revision 1 standards.

Reference: https://azure.microsoft.com/en-us/services/databox/

Domain

Describe Azure architecture and services (35–40%)

Question 63 Skipped

Yes or No:

Azure Service Health has the ability to configure cloud alerts to notify you about active and upcoming service issues

○ No

Correct answer

○ Yes

Explanation

Yes, Azure Service Health allows users to configure cloud alerts to receive notifications about active and upcoming service issues. This feature helps users stay informed about the status of Azure services and take necessary actions to mitigate any potential impact on their resources.

Overall explanation

From the Official Azure Documentation:

Azure Service Health notifies you about Azure service incidents and planned maintenance so you can take action to mitigate downtime. Configure customisable cloud alerts and use your personalised dashboard to analyse health issues, monitor the impact to your cloud resources, get guidance and support, and share details and updates.

Personalised dashboard shows the service issues that affect you

Configurable cloud alerts notify you about active and upcoming service issues

Shareable details and updates, including incident root cause analyses

Guidance and support during service incidents

Reference: https://docs.microsoft.com/en-us/learn/modules/intro-to-governance/7-monitoring

Domain

Describe Azure management and governance (30–35%)

Question 64 Skipped

Which of the following is an example of a security layer in the defense-in-depth model?

○ **The physical locks on server room doors.**

○ **A strong password policy for user accounts.**

○ **A single firewall at the network perimeter.**

Correct answer

○ **A dedicated intrusion detection system (IDS).**

Overall explanation

From the official documentation: "At Microsoft Azure, our security approach focuses on defense in depth, with layers of protection built throughout all phases of design, development, and deployment of our platforms and technologies. We also focus on transparency, making sure customers are aware of how we're constantly working to learn and improve our offerings to help mitigate the cyberthreats of today and prepare for the cyberthreats of tomorrow."

The defence in depth model is all about multiple layers - so always choose the option that best matches this.

A dedicated intrusion detection system (IDS) is an example of a security layer in the defense-in-depth model. It monitors network traffic for suspicious activity and helps detect and respond to potential breaches.

Reference: https://azure.microsoft.com/en-us/blog/microsoft-azures-defense-in-depth-approach-to-cloud-vulnerabilities/

Domain

Describe Azure architecture and services (35–40%)

● **Question 65** Skipped

Which of the following Azure resource types does NOT support tagging?

○ **Virtual Machines**

○ **Azure App Service**

○ **Azure Cosmos DB**

Correct answer

○ **Azure Container Registry**

Overall explanation

Azure provides the ability to apply metadata tags to resources to help organize and manage resources. These tags consist of name-value pairs that can be used to categorize resources based on common attributes. Azure supports tagging for most of its resource types, but some do not support tagging. **Azure Container Registry** is correct as Azure Container Registry does not support tagging. Container Registry is a private registry for storing and managing container images and does not currently support metadata tags.

- **Virtual Machines -** This is incorrect as Virtual Machines support tagging. Tags can be used to help identify and manage VMs.

- **Azure App Service -** This is incorrect as Azure App Service supports tagging. Tags can be used to help organize and manage App Service resources.

- **Azure Cosmos DB -** This is incorrect as Azure Cosmos DB supports tagging. Tags can be used to help identify and manage Cosmos DB resources.

Reference: https://learn.microsoft.com/en-us/azure/container-registry/container-registry-intro

Domain

Describe Azure architecture and services (35–40%)

● **Question 66** Skipped

Yes or No:

Azure Service Health allows us to define the critical resources that should never be impacted due to outages and downtimes.

Correct answer

○ **No**

Explanation

The correct answer is No because Azure Service Health does not provide the capability to define critical resources that should never be impacted by outages or downtimes. It primarily focuses on providing information and updates on the health of Azure services and regions to help users stay informed about any potential issues.

○ **Yes**

Overall explanation

From the Official Azure Documentation:

Azure Service Health notifies you about Azure service incidents and planned maintenance so you can take action to mitigate downtime. Configure customisable cloud alerts and use your personalised dashboard to analyse health issues, monitor the impact to your cloud resources, get guidance and support, and share details and updates.

Although you can see when a maintenance is planned and act accordingly to migrate a VM if needed, **you can't prevent service failures.**

Reference: https://azure.microsoft.com/en-ca/features/service-health/#features

Domain

Describe Azure management and governance (30–35%)

● **Question 67** Skipped

A developer deploys an Azure VM in Japan East, uses premium SSD storage, and forgets to deallocate it after testing, leading to a high bill. Which factor most directly impacts this cost overrun?

○ **Data egress**

Explanation

Data egress costs are related to the transfer of data out of Azure services, such as VMs, and can contribute to the overall bill. However, in this specific scenario, where the cost overrun is due to forgetting to deallocate the VM after testing, data egress is not the most direct factor impacting the high bill.

○ **Storage tier**

Explanation

While the storage tier (premium SSD in this case) does contribute to the overall cost of the Azure VM, it is not the most direct factor impacting the cost overrun in this scenario. The primary issue leading to the high bill is the continuous resource usage due to the VM not being deallocated after testing.

Correct answer

○ **Resource usage**

Explanation

Resource usage directly impacts the cost of running an Azure VM, as the longer the VM is running and actively consuming resources, the higher the cost will be. Forgetting to deallocate the VM after testing results in continuous resource usage and leads to a high bill.

○ **Region selection**

Explanation

Region selection can indirectly impact the cost of running an Azure VM, as different regions may have varying pricing structures. However, in this scenario, the developer deploying the VM in Japan East is not the primary factor contributing to the high bill; it is the failure to deallocate the VM after testing.

Overall explanation

The most direct factor impacting the cost overrun in this scenario is **resource usage**. When the developer deploys the Azure VM and forgets to deallocate it after testing, the VM continues to incur charges, even if it's not in active use. In Azure, you are billed based on the **time** the resources are running, which includes compute resources like VMs and associated services (e.g., storage). If the VM is running, even though it's not being used for active testing, it still incurs compute charges.

Why the other options are less relevant:

- **Region selection**: While choosing a region can impact pricing due to regional pricing differences (e.g., costs may vary between Japan East and other regions), the cost overrun in this case is more directly related to the fact that the VM was left running, not necessarily the region choice itself.

- **Storage tier**: The developer is using premium SSD storage, which is generally more expensive than standard storage, but the issue here is that the VM was not deallocated. Premium SSD storage is a factor in the cost, but the **primary cause** of the cost overrun is the **running VM** that wasn't deallocated.

- **Data egress**: Data egress charges occur when data is transferred **out of** Azure to external systems or other regions. However, in this case, the overrun is related to the VM being active, not the transfer of data out of Azure.

Domain

Describe Azure management and governance (30–35%)

Question 68 Skipped

A team uses Azure Cloud Shell to deploy VMs in West US and East US, noticing higher costs in one region. Does region selection affect Azure costs in this scenario?

○ No

Correct answer

○ Yes

Explanation

Yes, region selection does affect Azure costs in this scenario. Azure pricing varies by region, with some regions being more expensive than others due to factors such as demand, availability of resources, and data center location. Deploying resources in a region with higher costs will result in higher overall expenses for the team.

Overall explanation

The correct answer is: **Yes**

Region selection **does** affect Azure costs. The price for Azure services, including virtual machines (VMs), can vary depending on the region where the services are deployed. This is due to factors such as data center location, regional demand, and local operational costs. For example, some regions may have higher infrastructure costs or taxes, which could contribute to the higher cost of services deployed there.

So, if a team notices higher costs in one region, it's likely because of the pricing differences between the **West US** and **East US** regions.

Domain

Describe Azure management and governance (30–35%)

Question 69 Skipped

What types of threats does Defender for Cloud help detect across Azure PaaS services?

○ **Threats related to physical hardware vulnerabilities.**

Explanation

Defender for Cloud is not designed to detect threats related to physical hardware vulnerabilities. Physical hardware vulnerabilities are typically addressed through hardware security measures, firmware updates, and patch management, rather than through a cloud security service like Defender for Cloud.

○ **Denial of service (DoS) attacks against network resources.**

Explanation

Denial of service (DoS) attacks against network resources are not the primary focus of Defender for Cloud, which is more geared towards detecting threats targeting Azure PaaS services. DoS attacks are typically mitigated through network security measures and monitoring.

Correct answer

○ **Threats targeting Azure services like Azure App Service, Azure SQL, and Azure Storage Account.**

Explanation

Defender for Cloud helps detect threats targeting Azure services like Azure App Service, Azure SQL, and Azure Storage Account. These threats may include unauthorized access attempts, data breaches, malware infections, and other security vulnerabilities specific to Azure PaaS services.

○ **Physical security breaches within datacenters.**

Explanation

Defender for Cloud focuses on detecting threats within Azure PaaS services and does not specifically address physical security breaches within datacenters. Physical security breaches are typically addressed by other security measures such as access controls, surveillance systems, and security personnel.

Overall explanation

Defender for Cloud helps detect threats targeting various Azure services, such as Azure App Service, Azure SQL, and Azure Storage Account - these are PaaS services anyway. It provides monitoring and protection for these services to enhance their security.

Reference: https://learn.microsoft.com/en-us/training/modules/describe-azure-identity-access-security/9-describe-microsoft-defender-for-cloud

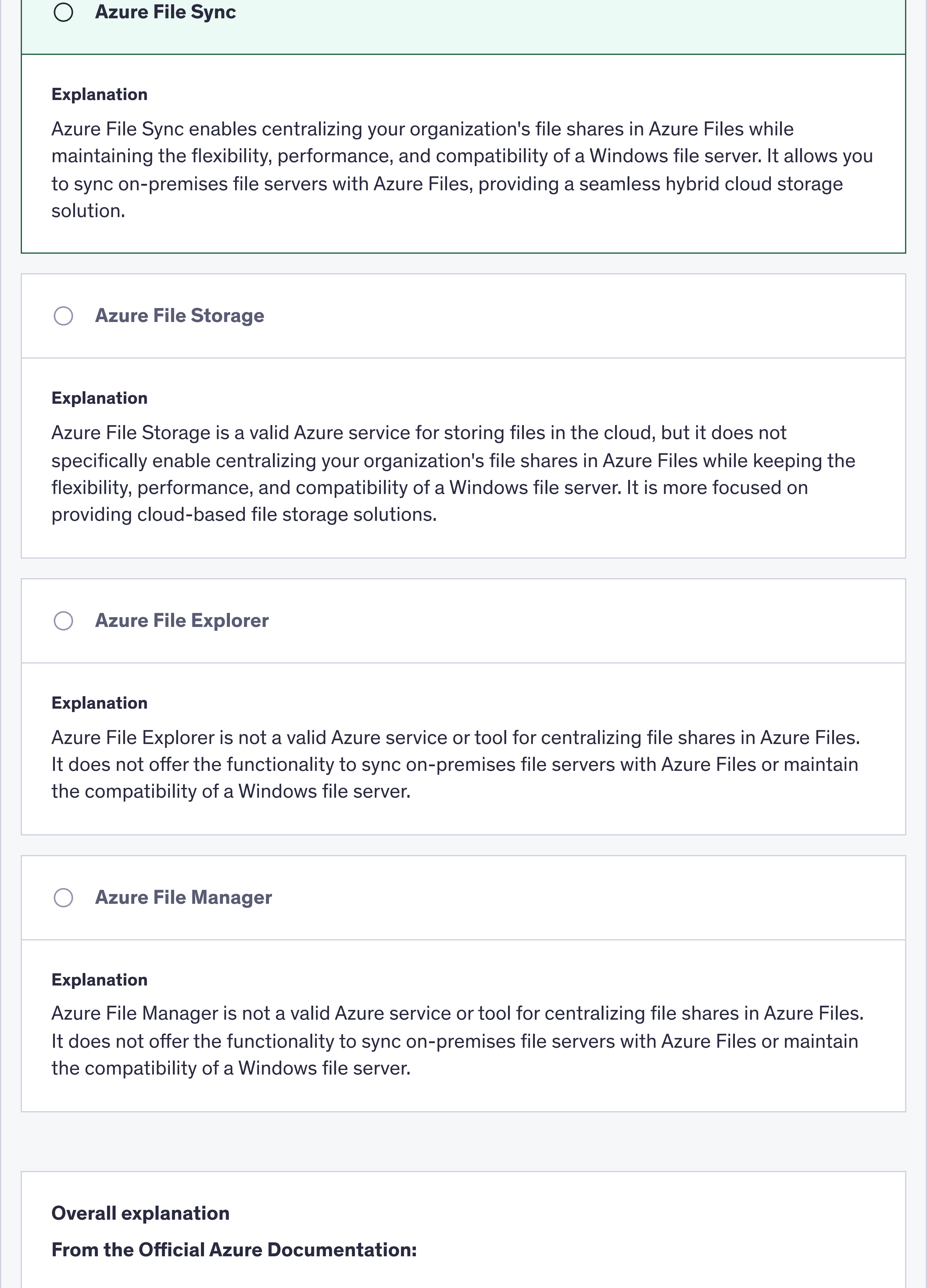
Domain

Describe Azure architecture and services (35–40%)

Question 70 Skipped

Which of the following enables centralizing your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of a Windows file server?

Correct answer



○ **Azure File Sync**

Explanation

Azure File Sync enables centralizing your organization's file shares in Azure Files while maintaining the flexibility, performance, and compatibility of a Windows file server. It allows you to sync on-premises file servers with Azure Files, providing a seamless hybrid cloud storage solution.

○ **Azure File Storage**

Explanation

Azure File Storage is a valid Azure service for storing files in the cloud, but it does not specifically enable centralizing your organization's file shares in Azure Files while keeping the flexibility, performance, and compatibility of a Windows file server. It is more focused on providing cloud-based file storage solutions.

○ **Azure File Explorer**

Explanation

Azure File Explorer is not a valid Azure service or tool for centralizing file shares in Azure Files. It does not offer the functionality to sync on-premises file servers with Azure Files or maintain the compatibility of a Windows file server.

○ **Azure File Manager**

Explanation

Azure File Manager is not a valid Azure service or tool for centralizing file shares in Azure Files. It does not offer the functionality to sync on-premises file servers with Azure Files or maintain the compatibility of a Windows file server.

Overall explanation

From the Official Azure Documentation:

Azure File Sync enables centralizing your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of a Windows file server. While some users may opt to keep a full copy of their data locally, Azure File Sync additionally has the ability to transform Windows Server into a quick cache of your Azure file share. You can use any protocol that's available on Windows Server to access your data locally, including SMB, NFS, and FTPS. You can have as many caches as you need across the world.

Reference: https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-introduction

Domain

Describe Azure architecture and services (35–40%)

Question 71 Skipped

Azure provides native support for IaC via the ________________ model.

Correct answer

○ **Azure Resource Manager**

Explanation

Azure Resource Manager is the correct choice as it is the service that provides the infrastructure as code (IaC) capabilities in Azure. It allows you to define your infrastructure in a declarative template format, enabling you to manage and deploy Azure resources consistently and efficiently.

○ **Azure Templates**

Explanation

Azure Templates are not the correct choice in this context. While Azure Templates are used in conjunction with Azure Resource Manager for defining and deploying Azure resources, they are not the primary model for infrastructure as code in Azure. Azure Resource Manager is the service that natively supports IaC.

○ **Azure Arc**

Explanation

Azure Arc is a service that extends Azure management and services to any infrastructure, including on-premises, multi-cloud, and edge environments. While Azure Arc provides centralized management and governance for these resources, it is not specifically designed for infrastructure as code like Azure Resource Manager.

○ **Azure Tags**

Explanation

Azure Tags are used for organizing and categorizing Azure resources, but they are not directly related to infrastructure as code. While tags can be helpful for resource management and organization, they do not provide the same level of automation and consistency as the infrastructure as code model supported by Azure Resource Manager.

Overall explanation

From the official documentation:

Azure provides native support for IaC via the Azure Resource Manager model. Teams can define declarative ARM templates that specify the infrastructure required to deploy solutions.

Third-party platforms like Terraform, Ansible, Chef, and Pulumi also support IaC to manage automated infrastructure.

Reference: https://learn.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code

Domain

Describe Azure management and governance (30–35%)

● **Question 72** Skipped

Microsoft Azure services operated by ____________ in China.

○ Xiaomi

○ Morgan Stanley

○ Alibaba

Correct answer

○ **21Vianet**

Overall explanation

Microsoft Azure operated by **21Vianet** is the first international public cloud service that has been commercialized in China in compliance with Chinese laws and regulations.

Reference : https://docs.azure.cn/en-us/articles/azure-china-purchasing-guidance/

Domain

Describe Azure architecture and services (35–40%)

Question 73 Skipped

Which of the following is a good usage of tags?

○ Using Tags to quickly locate resources associated with specific workloads, environments, ownership groups, or other important information.

○ **Making business groups aware of cloud resource consumption requires IT to understand the resources and workloads each team is using**

Correct answer

○ **All of these**

○ **To help identify the assets required to support a single workload.**

○ **Using tags for data classification**

Overall explanation

All of the above can help leverage the power of tags in one way or the other.

From the official Azure docs:

Organizing cloud-based resources is a crucial task for IT, unless you only have simple deployments. Use naming and tagging standards to organize your resources for the following reasons:

- **Resource management:** Your IT teams need to quickly locate resources associated with specific workloads, environments, ownership groups, or other important information. Organizing resources is critical to assigning organizational roles and access permissions for resource management.

- **Cost management and optimization:** Making business groups aware of cloud resource consumption requires IT to understand the resources and workloads each team is using.

- **Operations management:** Visibility for the operations management team about business commitments and SLAs is an important aspect of ongoing operations. For operations to be managed well, tagging for mission criticality is required.

- **Security:** Classification of data and security impact is a vital data point for the team, when breaches or other security issues arise. To operate securely, tagging for data classification is required.

- **Governance and regulatory compliance:** Maintaining consistency across resources helps identify changes from agreed-upon policies. Prescriptive guidance for resource tagging demonstrates how one of the following patterns can help when deploying governance practices. Similar patterns are available to evaluate regulatory compliance using tags.

- **Automation:** A proper organizational scheme allows you to take advantage of automation as part of resource creation, operational monitoring, and the creation of DevOps processes. It also makes resources easier for IT to manage.

- **Workload optimization:** Tagging can help identify patterns and resolve broad issues. Tag can also help identify the assets required to support a single workload. Tagging all assets associated with each workload enables deeper analysis of your mission-critical workloads to make sound architectural decisions.

To learn even more about this : https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/resource-tagging/?toc=%2Fazure%2Fazure-resource-manager%2Fmanagement%2Ftoc.json

Domain

Describe Azure management and governance (30–35%)

Question 74 Skipped

Which of the following is the mission-critical cloud deployment available only to US Federal, State, Local and Tribal Governments and their partners?

○ ISO

Explanation

ISO is a set of international standards that provide guidelines for quality management and security, but it is not specifically related to cloud deployments for US government entities.

○ **Azure Federal**

Explanation

Azure Federal is a cloud deployment option for US government agencies, but it is not limited to Federal, State, Local, and Tribal Governments and their partners. It is specifically designed for federal agencies.

Correct answer

○ **Azure Government**

Explanation

Azure Government is the correct choice as it is the mission-critical cloud deployment available exclusively to US Federal, State, Local, and Tribal Governments and their partners. It provides dedicated regions and services to meet the specific compliance and security requirements of these entities.

○ **Azure Nation**

Explanation

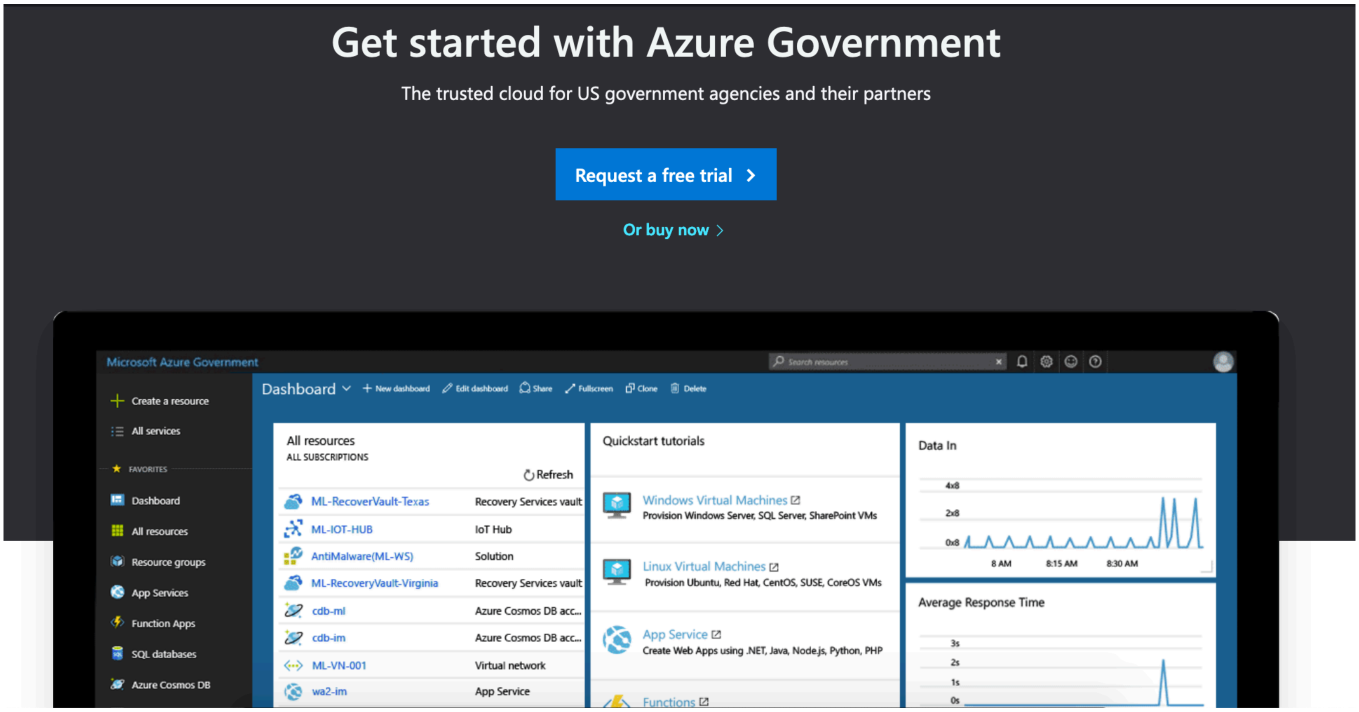
Azure Nation is not a recognized cloud deployment option in Microsoft Azure. It is not specifically designed for US government entities and their partners.

Overall explanation

From the Official Azure Documentation:

Azure Government is the mission-critical cloud, delivering breakthrough innovation to **US government customers and their partners.** Only US federal, state, local and tribal governments and their partners have access to this dedicated instance, operated by screened

US citizens. Azure Government offers the broadest level of certifications of any cloud provider to simplify even the most critical government compliance requirements.



Get started with Azure Government

The trusted cloud for US government agencies and their partners

All resources
ALL SUBSCRIPTIONS

ML-RecoverVault-Texas	Recovery Services vault
ML-IOT-HUB	IoT Hub
AntiMalware(ML-WS)	Solution
ML-RecoveryVault-Virginia	Recovery Services vault
cdb-ml	Azure Cosmos DB acc...
cdb-im	Azure Cosmos DB acc...
ML-VN-001	Virtual network
wa2-im	App Service

Quickstart tutorials

Windows Virtual Machines
Provision Windows Server, SQL Server, SharePoint VMs

Linux Virtual Machines
Provision Ubuntu, Red Hat, CentOS, SUSE, CoreOS VMs

App Service
Create Web Apps using .NET, Java, Node.js, Python, PHP

Functions

Reference: https://azure.microsoft.com/en-in/global-infrastructure/government/get-started/

Domain

Describe cloud concepts (25–30%)

Question 75 Skipped

Your streaming website experiences a burst of heavy traffic whenever you launch a new web-series, but relatively moderate traffic on other days. Which of the following would be a great benefit if you migrate your setup to Azure?

○ **Low Latency**

Explanation

Low Latency in Azure refers to the minimal delay in data transmission between the server and the user's device. While low latency is crucial for a smooth streaming experience, it may not directly address the issue of handling sudden spikes in traffic during new web-series launches.

○ **Load Balancing**

Explanation

Load Balancing in Azure helps distribute incoming network traffic across multiple servers to ensure no single server is overwhelmed. While load balancing can improve overall performance and reliability, it may not directly address the specific challenge of managing bursts of heavy traffic during new web-series launches.

○ **High Availibility**

Explanation

High Availability in Azure ensures that your services are always up and running, minimizing downtime and ensuring that your streaming website is accessible to users at all times. While important, high availability may not directly address the specific issue of handling bursts of heavy traffic during new web-series launches.

Correct answer

○ **Elasticity**

Explanation

Elasticity in Azure allows you to automatically scale your resources up or down based on demand. This means that during the burst of heavy traffic when launching a new web-series, Azure can quickly allocate additional resources to handle the increased load, and then scale back down during periods of moderate traffic, helping you manage costs efficiently.

Overall explanation

From the official Azure docs:

Elastic computing is the ability to quickly expand or decrease computer processing, memory, and storage resources to meet changing demands without worrying about capacity planning and engineering for peak usage. Typically controlled by system monitoring tools, elastic computing matches the amount of resources allocated to the amount of resources actually needed without disrupting operations.

With cloud elasticity, a company avoids paying for unused capacity or idle resources and doesn't have to worry about investing in the purchase or maintenance of additional resources and equipment.

References : https://azure.microsoft.com/en-us/overview/what-is-elastic-computing/

Domain

Describe cloud concepts (25–30%)

● **Question 76** Skipped

How does the syntax of commands differ between Azure PowerShell and the Azure CLI?

○ **There is no difference in command syntax between Azure PowerShell and the Azure CLI.**

○ **Azure PowerShell uses Bash scripts, while the Azure CLI uses JSON configuration files.**

○ **Azure PowerShell uses Python scripts, while the Azure CLI uses Ruby scripts.**

Correct answer

○ **Azure PowerShell uses PowerShell commands, while the Azure CLI uses Bash commands.**

Overall explanation

From the official Azure docs:

The Azure CLI is functionally equivalent to Azure PowerShell, with the primary difference being the syntax of commands. While Azure PowerShell uses PowerShell commands, the Azure CLI uses Bash commands.

The Azure CLI provides the same benefits of handling discrete tasks or orchestrating complex operations through code. It's also installable on Windows, Linux, and Mac platforms, as well as through Azure Cloud Shell.

Due to the similarities in capabilities and access between Azure PowerShell and the Bash based Azure CLI, it mainly comes down to which language you're most familiar with.

Reference: https://learn.microsoft.com/en-us/training/modules/describe-features-tools-manage-deploy-azure-resources/2-describe-interacting-azure

Domain

Describe Azure management and governance (30–35%)

● **Question 77** Skipped

_______________ is a set of capabilities in Microsoft Entra ID that enables organizations to secure and manage any outside user, including customers and partners.

Correct answer

○ **External Identities**

Explanation

External Identities in Microsoft Azure is a set of capabilities that allow organizations to securely manage and authenticate external users, such as customers and partners. It provides features like Azure AD B2B and B2C to enable secure access for external users.

○ **External Profiles**

Explanation

External Profiles is not a recognized term or capability in Microsoft Azure for managing outside users. It does not provide the necessary tools for secure management and authentication of external identities.

○ **Sentinel**

Explanation

Sentinel is a Security Information and Event Management (SIEM) tool in Microsoft Azure, used for threat detection and response. It is not related to managing outside users such as customers and partners.

○ **External User Management**

Explanation

External User Management is not a specific capability in Microsoft Azure for managing outside users. It does not specifically address the secure management of external identities.

Overall explanation

From the Official Azure Documentation:

External Identities is a set of capabilities that enables organizations to secure and manage any external user, including customers and partners. Building on B2B collaboration, External Identities gives you more ways to interact and connect with users outside your organization.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/external-identities/

Domain

Describe Azure architecture and services (35–40%)

● **Question 78** Skipped

______________ **is the process of verifying a user's credentials.**

○ **Federation**

Explanation

Federation is the process of linking a user's identity and attributes across multiple identity management systems. While it is related to authentication, it is not the direct process of verifying a user's credentials.

○ **Authorization**

Explanation

Authorization is the process of determining what actions a user is allowed to perform after they have been authenticated. It is not directly related to verifying a user's credentials.

○ **Ticketing**

Explanation

Ticketing is a process used in IT service management to track and manage requests for support or services. It is not directly related to verifying a user's credentials.

Correct answer

○ **Authentication**

Explanation

Authentication is the process of verifying a user's credentials, such as username and password, to ensure that the user is who they claim to be. It is essential for providing secure access to resources and services.

Overall explanation

Authentication is the process of establishing the identity of a person or service looking to access a resource. It involves the act of challenging a party for legitimate credentials and provides the basis for creating a security principal for identity and access control use. It establishes if they are who they say they are.

Authorization is the process of establishing what level of access an authenticated person or service has. It specifies what data they're allowed to access and what they can do with it.

Domain

Describe Azure management and governance (30–35%)

Question 79 Skipped

Yes or No:

Upon applying a Tag to a Resource Group, all Resources inside it inherit that Tag.

Correct answer

○ **No**

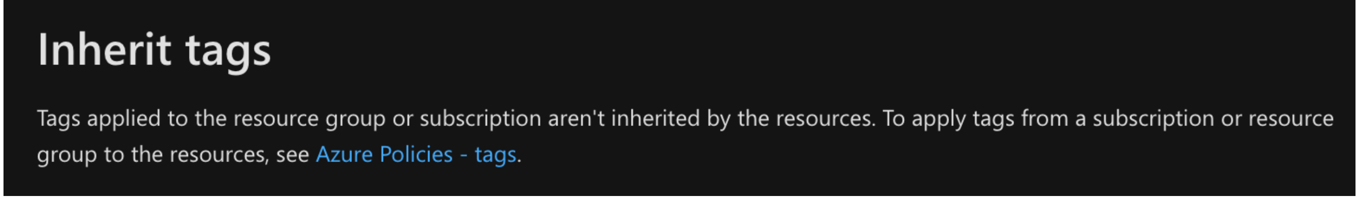
○ **Yes**

Overall explanation

Important question!

From the official documentation:

Tags applied to the resource group or subscription aren't inherited by the resources. To apply tags from a subscription or resource group to the resources, see Azure Policies - tags.



Inherit tags

Tags applied to the resource group or subscription aren't inherited by the resources. To apply tags from a subscription or resource group to the resources, see Azure Policies - tags.

Reference : https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources

Domain

Describe Azure management and governance (30–35%)

Question 80 Skipped

Which of the following is the strongest way to protect sensitive customer data?

Correct answer

○ **Encrypt the data both at rest and in transit.**

Explanation

Encrypting data both at rest and in transit provides a comprehensive security approach to protecting sensitive customer data. This ensures that the information is encrypted and secure both when it is stored on a server or storage device (at rest) and when it is being transmitted between systems or over a network (in transit).

○ **Encrypt the data in transit.**

Explanation

Encrypting data in transit ensures that the information is secure while it is being transferred between systems or over a network. This helps prevent interception and unauthorized access during the transmission process. However, it does not protect the data when it is stored on a server or storage device.

○ **Don't store sensitive data at all.**

Explanation

While not storing sensitive data at all is a valid approach to minimizing the risk of data breaches, it may not always be feasible or practical for businesses that need to store and process customer information. Encrypting data provides an additional layer of security to protect the data even if it is stored on servers or transmitted over networks.

○ **Encrypt the data at rest.**

Explanation

Encrypting data at rest is a good security practice to protect sensitive information from unauthorized access if the storage medium is compromised. However, it does not provide protection when the data is being transmitted between systems or over a network.

Overall explanation

From the official Azure docs:

To help protect data in the cloud, you need to account for the possible states in which your data can occur, and what controls are available for that state. Best practices for Azure data security and encryption relate to the following data states:

1) At rest: This includes all information storage objects, containers, and types that exist statically on physical media, whether magnetic or optical disk.

2) In transit: When data is being transferred between components, locations, or programs, it's in transit. Examples are transfer over the network, across a service bus (from on-premises to cloud and vice-versa, including hybrid connections such as ExpressRoute), or during an input/output process.

Reference : https://docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices

Domain

Describe Azure architecture and services (35–40%)

Question 81 Skipped

Please fill the blank field(s) in the statement with the right words.

An architect defines an Azure app’s VMs and networking in a JSON file for repeatable deployments, using __ as code to automate infrastructure setup.

Correct answer

infrastructure

Explanation

The correct answer is **"Infrastructure"** as code.

In this context, **"Infrastructure as Code" (IaC)** refers to the practice of defining and managing infrastructure (like VMs, networking, storage, etc.) using code and configuration files instead of manual processes. This is typically done using tools like **Azure Resource Manager (ARM) templates**, **Terraform**, or **Bicep**.

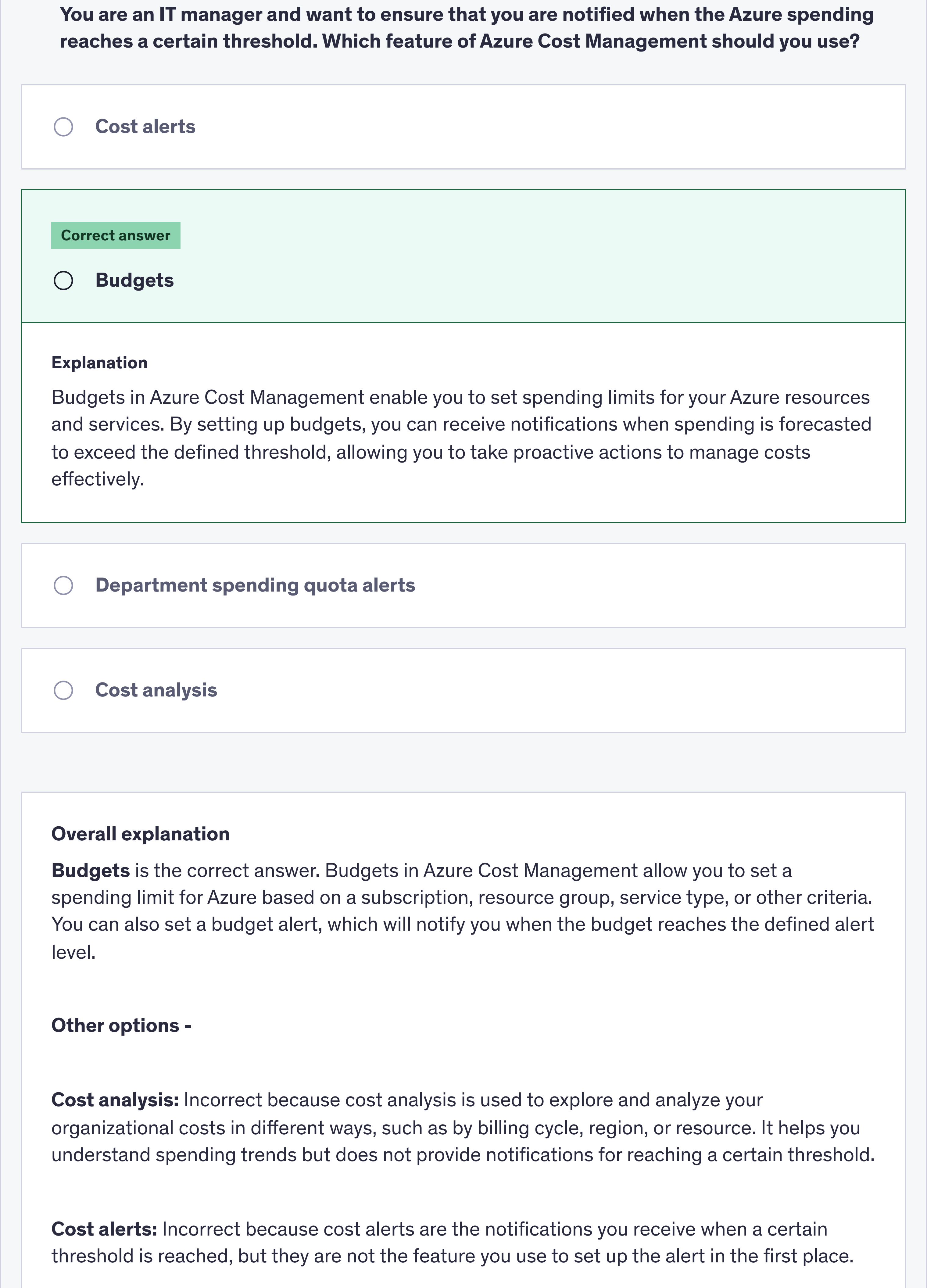
- The **JSON file** mentioned in your example is likely an **ARM template**, which allows for the declarative definition of Azure resources in code.

- This approach helps automate the deployment and management of infrastructure, ensuring consistency, repeatability, and scalability without the need for manual intervention.

Domain

Describe Azure management and governance (30–35%)

Question 82 Skipped



You are an IT manager and want to ensure that you are notified when the Azure spending reaches a certain threshold. Which feature of Azure Cost Management should you use?

○ **Cost alerts**

Correct answer

○ **Budgets**

Explanation

Budgets in Azure Cost Management enable you to set spending limits for your Azure resources and services. By setting up budgets, you can receive notifications when spending is forecasted to exceed the defined threshold, allowing you to take proactive actions to manage costs effectively.

○ **Department spending quota alerts**

○ **Cost analysis**

Overall explanation

Budgets is the correct answer. Budgets in Azure Cost Management allow you to set a spending limit for Azure based on a subscription, resource group, service type, or other criteria. You can also set a budget alert, which will notify you when the budget reaches the defined alert level.

Other options -

Cost analysis: Incorrect because cost analysis is used to explore and analyze your organizational costs in different ways, such as by billing cycle, region, or resource. It helps you understand spending trends but does not provide notifications for reaching a certain threshold.

Cost alerts: Incorrect because cost alerts are the notifications you receive when a certain threshold is reached, but they are not the feature you use to set up the alert in the first place.

You need to set a budget and configure a budget alert to receive cost alerts.

Department spending quota alerts: Incorrect because department spending quota alerts are specific to organizations with Enterprise Agreements (EAs) and are used to notify when department spending reaches a fixed threshold of the quota. This alert type is not related to general Azure spending thresholds.

Reference: https://learn.microsoft.com/en-us/training/modules/describe-cost-management-azure/6-describe-azure-tool

Domain

Describe Azure management and governance (30–35%)

● **Question 83** Skipped

Yes or No:

Having a hybrid cloud solution in place could be useful when regulations or policies do not permit moving specific data or workloads to the cloud.

Correct answer

○ **Yes**

Explanation

Yes, having a hybrid cloud solution allows organizations to keep sensitive data or workloads on-premises while still leveraging the benefits of the cloud for other operations. This can help organizations comply with regulations or policies that restrict certain data or workloads from being moved to the public cloud.

○ **No**

Overall explanation

From the official Azure documentation:

When organizations move workloads and data to the cloud, their on-premises datacenters often continue to play an important role. The term *hybrid cloud* refers to a combination of public cloud and on-premises datacenters, to create an integrated IT environment that spans both. Some organizations use hybrid cloud as a path to migrate their entire datacenter to the cloud over time. Other organizations use cloud services to extend their existing on-premises infrastructure.

When to use a hybrid solution

Consider using a hybrid solution in the following scenarios:

- As a transition strategy during a longer-term migration to a fully cloud-native solution.
- When regulations or policies do not permit moving specific data or workloads to the cloud.
- For disaster recovery and fault tolerance, by replicating data and services between on-premises and cloud environments.
- To reduce latency between your on-premises datacenter and remote locations, by hosting part of your architecture in Azure.

Reference : https://docs.microsoft.com/en-us/azure/architecture/data-guide/scenarios/hybrid-on-premises-and-cloud

Domain

Describe cloud concepts (25–30%)

Question 84 Skipped

A developer mistakenly uploads a JSON file to your Azure tenant, which results in the automatic deployment of multiple VMs, a virtual network, and a load balancer across two subscriptions, all without any manual intervention in the portal. This automated deployment is the result of a configuration using __________, which are commonly used for managing and provisioning resources at scale.

Which Azure feature is responsible for this automatic deployment?

○ **Azure CLI commands**

Explanation

Azure CLI commands are used for interacting with Azure resources through the command line interface, but they do not provide the capability to automatically deploy resources based on a predefined configuration like ARM templates. CLI commands are more focused on managing and configuring existing resources rather than provisioning new ones.

○ **Azure Automation scripts**

Explanation

Azure Automation scripts are used for automating repetitive tasks and processes in Azure, but they are not specifically designed for defining and deploying resources like VMs, virtual networks, and load balancers. While they can be used for automation, they are not the primary tool for resource provisioning at scale.

Correct answer

○ **Azure Resource Manager (ARM) templates**

Explanation

Azure Resource Manager (ARM) templates are JSON files that define the resources and their configurations needed for an application. When uploaded to Azure, ARM templates enable the automatic deployment of resources based on the defined configuration, making them ideal for managing and provisioning resources at scale without manual intervention.

○ **Azure Policy assignments**

Explanation

Azure Policy assignments are used to enforce rules and policies for resources in Azure, ensuring compliance and governance. While policies can control the deployment and configuration of resources, they do not directly enable the automatic deployment of resources like VMs, virtual networks, and load balancers across subscriptions without manual intervention.

Overall explanation

Azure Resource Manager (ARM) templates: This is the correct answer because ARM templates are used to define the infrastructure and configuration for Azure resources declaratively. The JSON format allows for automation of resource deployment across subscriptions, which fits the scenario described.

Azure Automation scripts: Azure Automation can be used for automating tasks but is more focused on process automation rather than infrastructure provisioning at scale like ARM templates.

Azure CLI commands: The Azure Command-Line Interface (CLI) can be used for scripting deployments, but it requires user interaction or manual script execution, which isn't the case here.

Azure Policy assignments: Azure Policy is primarily used to enforce governance rules and compliance across resources, but it doesn't handle resource provisioning like ARM templates.

Domain

Describe Azure architecture and services (35–40%)

● **Question 85** Skipped

__________________ is a hosting service for Domain Name System domains that provides name resolution by using Microsoft Azure infrastructure.

○ **Azure Virtual Subnets**

Explanation

Azure Virtual Subnets are used to segment and manage virtual networks in Azure. They help organize and isolate resources within a virtual network. While virtual subnets are essential for network management, they do not provide hosting services for DNS domains like Azure DNS does.

○ **Azure VPN Gateway**

Explanation

Azure VPN Gateway is a service that allows users to connect their on-premises networks to Azure securely over the internet. It provides encrypted communication between the on-premises network and Azure resources. While VPN Gateway is crucial for secure network connectivity, it is not specifically designed for hosting DNS domains.

Correct answer

○ **Azure DNS**

Explanation

Azure DNS is a hosting service for Domain Name System (DNS) domains that provides name resolution using Microsoft Azure infrastructure. It allows users to manage DNS records using the same credentials, billing, and support as other Azure services, making it a convenient and integrated solution for DNS management.

○ **Azure ExpressRoute**

Explanation

Azure ExpressRoute is a service that provides a private connection between an on-premises network and Microsoft Azure. It is used to establish a dedicated, high-throughput connection that does not involve the public internet. While it is essential for secure and reliable connectivity, it is not directly related to hosting DNS domains.

Overall explanation

From the Official Azure Documentation:

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records by using the same credentials, APIs, tools, and billing as your other Azure services.

You can't use Azure DNS to buy a domain name. For an annual fee, you can buy a domain name by using App Service domains or a third-party domain name registrar. Your domains then can be hosted in Azure DNS for record management. For more information, see Delegate a domain to Azure DNS.

Reference: https://docs.microsoft.com/en-us/azure/dns/dns-overview

Domain

Describe Azure architecture and services (35–40%)

● **Question 86** Skipped

Yes or No:

It's possible to deploy a new Azure VM from a Google Chromebook by using PowerAutomate.

○ **Yes**

Correct answer

○ **No**

Overall explanation

Tricky question! PowerAutomate is not the same as PowerShell.

PowerAutomate moreover isn't a part of Azure! It falls under the Microsoft umbrella of offerings, just like PowerApps.

Hence, this statement is definitely False. You can use the Azure portal to provision Virtual Machines, or even the CLI.

Reference: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal

● **Question 87** Skipped

What is the primary purpose of applying resource locks in Azure?

○ **To prevent any modifications to resources, including read access.**

Explanation

Resource locks in Azure are primarily used to prevent accidental deletion or modification of critical resources. They do not restrict read access to resources, but rather focus on preventing unwanted changes to important assets within the Azure environment.

Correct answer

○ **To prevent accidental deletion or modification of critical resources.**

Explanation

The primary purpose of applying resource locks in Azure is to prevent accidental deletion or modification of critical resources. By implementing resource locks, users can safeguard important assets from unintended changes that could impact the functionality or stability of the Azure environment.

○ **To restrict access to Azure resources to a specific user.**

Explanation

Resource locks are not designed to restrict access to Azure resources to a specific user. They are more focused on protecting critical resources from accidental modifications or deletions by any user with access to the resources.

○ **To ensure resources are automatically deleted after a specific time period.**

Explanation

Resource locks do not automatically delete resources after a specific time period. Their main purpose is to prevent unintended changes to critical resources, rather than managing the lifecycle or deletion of resources based on a time frame.

Overall explanation

From the official Azure docs:

As an administrator, you can lock an Azure subscription, resource group, or resource to protect them from accidental user deletions and modifications. The lock overrides any user permissions.

You can set locks that prevent either deletions or modifications. In the portal, these locks are called **Delete** and **Read-only**. In the command line, these locks are called **CanNotDelete** and **ReadOnly**.

- **CanNotDelete** means authorized users can read and modify a resource, but they can't delete it.
- **ReadOnly** means authorized users can read a resource, but they can't delete or update it. Applying this lock is similar to restricting all authorized users to the permissions that the **Reader** role provides.

Unlike role-based access control (RBAC), you use management locks to apply a restriction across all users and roles. To learn about setting permissions for users and roles, see Azure RBAC.

Therefore, Resource locks in Azure are used to prevent **accidental** deletion or modification of important resources. They help maintain the integrity of critical resources by preventing unwanted changes.

Reference: https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

Domain

Describe Azure management and governance (30–35%)

● **Question 88** Skipped

An organization splits its Azure virtual network into two subnets—one for web servers, one for databases—and connects it to another VNet in a different region for data sharing. Which feature enables this cross-VNet connectivity?

○ **Azure VPN Gateway**

Explanation

Azure VPN Gateway is used to establish secure connections between on-premises networks and Azure Virtual Networks, or between Azure Virtual Networks. While it provides secure connectivity, it is not specifically designed for enabling cross-VNet connectivity within Azure.

○ **Azure Virtual Subnets**

Explanation

Azure Virtual Subnets are used to divide a single Azure Virtual Network into multiple subnets for organizing and managing resources within the same network. They do not enable cross-VNet connectivity between different virtual networks.

Correct answer

○ **Virtual Network Peering**

Explanation

Virtual Network Peering allows connecting two Azure Virtual Networks in the same region or different regions to enable seamless communication and resource sharing between the networks. It is the correct feature that enables cross-VNet connectivity for data sharing between the web server and database subnets.

○ **Azure DNS**

Explanation

Azure DNS is a hosting service for DNS domains that provides name resolution using the Azure infrastructure. It does not directly enable cross-VNet connectivity between different virtual networks for data sharing purposes.

Overall explanation

The correct answer is: **Virtual Network Peering**

Virtual Network Peering enables connectivity between two virtual networks (VNets) in Azure, whether they are in the same region or across different regions (global VNet peering). In this scenario, the organization is connecting VNets across regions for data sharing, which is exactly what Virtual Network Peering is designed to do. It allows resources in each VNet to communicate with each other using private IP addresses as if they were part of the same network.

Here’s why the other options are incorrect:

- **Azure Virtual Subnets**: Subnets are divisions within a single VNet. While subnets organize network traffic within a VNet, they do not enable cross-VNet connectivity.

- **Azure VPN Gateway**: VPN Gateway is used to connect on-premises networks to Azure VNets or to connect Azure VNets to each other over a secure, encrypted VPN tunnel. However, it's not required if you are just using VNet peering within Azure.

- **Azure DNS**: Azure DNS is a service for hosting DNS domains and resolving DNS queries. It doesn't facilitate network connectivity between VNets.

Thus, **Virtual Network Peering** is the feature that enables the cross-VNet connectivity.

Domain

Describe Azure architecture and services (35–40%)

● **Question 89** Skipped

A CFO, skeptical of cloud savings, tasks you with proving Azure’s value. You use one tool to dazzle her with a detailed breakdown of VM and storage costs for a new app, tweaking regions and tiers on the fly, while another reveals how much her dusty on-premises servers are bleeding cash over three years—without touching Azure specifics. Which tool wins her over with the long-term savings pitch?

○ **Pricing Calculator, because it compares cloud vs. on-premises costs**

Explanation

The Pricing Calculator is a tool that helps estimate the cost of using Azure services based on specific configurations. While it allows for forecasting costs over time, it does not directly compare cloud vs. on-premises costs. Therefore, it may not be the best tool to win over the CFO with a long-term savings pitch.

○ **TCO Calculator, because it adjusts Azure costs by region**

Explanation

The TCO Calculator is the tool that estimates the total cost of using Azure services, including adjustments for factors like region. While region-specific cost adjustments are important, the primary focus of the TCO Calculator is to provide an overall estimate of Azure service pricing and compare it to on-premises costs, making it the ideal tool to win over the CFO with a long-term savings pitch.

○ **Pricing Calculator, because it forecasts multi-year ownership costs**

Explanation

While the Pricing Calculator does allow for forecasting multi-year ownership costs, it does not directly compare cloud vs. on-premises costs. Therefore, it may not be as effective in convincing the CFO of the long-term savings potential of Azure compared to on-premises solutions.

Correct answer

○ **TCO Calculator, because it estimates Azure service pricing**

Explanation

The TCO (Total Cost of Ownership) Calculator is designed to estimate the total cost of using Azure services over a specified period, taking into account factors such as region, service tiers, and usage. By providing a detailed breakdown of Azure service pricing and comparing it to on-premises costs, the TCO Calculator is the tool that can effectively demonstrate long-term savings to the CFO.

Domain

Describe Azure management and governance (30–35%)

Question 90 Skipped

In Azure, when you set a budget, what happens when the budget alert level is reached?

○ **An invoice is sent to the account owner**

○ **The resource usage is suspended**

○ **The budget is automatically increased by 10%**

Correct answer

○ **A budget alert is triggered**

Overall explanation

A budget alert is triggered is the correct option!

Other options -

The budget is automatically increased.by 10%: This is incorrect because reaching the budget alert level does not cause the budget to automatically increase. The purpose of the alert is to notify you when the spending reaches a certain threshold.

The resource usage is suspended: This is incorrect because a budget alert by itself does not suspend resource usage. It simply provides a notification that the alert threshold has been reached. However, you can configure advanced automation to suspend or modify resources based on budget conditions, but this is not the default behavior.

An invoice is sent to the account owner: This is incorrect because reaching the budget alert level does not trigger an invoice to be sent to the account owner. The budget alert is intended to inform you about the spending level, not to generate an invoice.

Reference: https://learn.microsoft.com/en-us/training/modules/describe-cost-management-azure/6-describe-azure-tool

Domain

Describe Azure management and governance (30–35%)