Practice Test - 4 - Results

Question 1 Skipped

Azure Pay As you Go is an example of which cloud expenditure model?

Correct answer

◯ **Operational (OpEx)**

Explanation

Azure Pay As You Go is an example of an Operational Expenditure (OpEx) model in cloud computing. In this model, users pay for the services they use on a pay-as-you-go basis, similar to utility bills. This allows for flexibility and scalability as users can adjust their usage and costs based on their needs without upfront capital investment.

◯ **Capital (CapEx)**

Explanation

Capital Expenditure (CapEx) models involve upfront investments in infrastructure or resources that are depreciated over time. Azure Pay As You Go does not require any upfront capital investment, making it more aligned with an Operational Expenditure (OpEx) model where costs are incurred as services are consumed.

Overall explanation

One of the major changes that you will face when you move from on-premises cloud to the public cloud is the switch from capital expenditure (buying hardware) to operating expenditure (paying for service as you use it). However, this switch also requires more careful management of your costs.

Meet your reliability needs

Operate your mission-critical systems with speed and confidence – across high availability, disaster recovery and back-up scenarios.

Control your costs

Scale and adapt to changing business needs while managing your cloud spending with budget alerts and optimisation best practices.

Simplify your move

As you modernise your applications, take advantage of familiar operational protocols and integrations that reduce the learning curve.

Reference: https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/appendix/azure-scaffold

Domain

Describe cloud concepts (25–30%)

Question 2 Skipped

Which of the following is an offline tier optimized for storing data that is rarely accessed, and that has flexible latency requirements?

○ Hot Tier

Explanation

The Hot Tier is optimized for storing data that is frequently accessed and requires low latency. It is not suitable for data that is rarely accessed.

○ Cool Tier

Explanation

The Cool Tier is optimized for storing data that is accessed less frequently than data in the Hot Tier but more frequently than data in the Archive Tier. It does not have flexible latency requirements and is not specifically designed for rarely accessed data.

Correct answer

○ **Archive Tier**

Explanation

The Archive Tier is an offline tier optimized for storing data that is rarely accessed. It is cost-effective and has flexible latency requirements, making it suitable for long-term storage of infrequently accessed data.

◯ **Infrequent Tier**

Explanation

The Infrequent Tier is not a storage tier option in Azure. It is not specifically designed for storing rarely accessed data with flexible latency requirements.

Overall explanation

From the Official Azure Documentation:

Data stored in the cloud grows at an exponential pace. To manage costs for your expanding storage needs, it can be helpful to organize your data based on how frequently it will be accessed and how long it will be retained. Azure storage offers different access tiers so that you can store your blob data in the most cost-effective manner based on how it's being used. Azure Storage access tiers include:

- **Hot tier** - An online tier optimized for storing data that is accessed or modified frequently. The Hot tier has the highest storage costs, but the lowest access costs.
- **Cool tier** - An online tier optimized for storing data that is infrequently accessed or modified. Data in the Cool tier should be stored for a minimum of 30 days. The Cool tier has lower storage costs and higher access costs compared to the Hot tier.
- **Archive tier** - An offline tier optimized for storing data that is rarely accessed, and that has flexible latency requirements, on the order of hours. Data in the Archive tier should be stored for a minimum of 180 days.

Reference: https://docs.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview

Domain

Describe Azure architecture and services (35–40%)

Question 3 Skipped

_____ is a domain-specific language (DSL) that uses declarative syntax to deploy Azure resources

Correct answer

- ◯ **Bicep**
- ◯ **HTML**
- ◯ **Tricep**
- ◯ **PHP**

Overall explanation

From the official Azure documentation:

Bicep is a domain-specific language (DSL) that uses declarative syntax to deploy Azure resources. In Bicep files, you define the infrastructure you intend to deploy and its properties. Compared to ARM templates, Bicep files are easier to read and write for a non-developer audience because they use a concise syntax.

Reference: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/infrastructure-as-code

Domain

Describe Azure management and governance (30–35%)

Question 4 Skipped

Which type of resource lock allows you to modify the resource, but not delete it?

○ **Read-only lock**

Explanation

Read-only lock restricts all operations, including modification, on a resource. It does not allow any changes to be made, including modifications.

Correct answer

○ **CanNotDelete lock**

Explanation

CanNotDelete lock allows you to modify the resource but prevents you from deleting it. This type of lock ensures that the resource remains intact while still allowing updates and changes to be made.

○ **Restrict lock**

Explanation

Restrict lock does not exist as a type of resource lock in Azure. It is not a valid option for allowing modification but preventing deletion of a resource.

○ **CanNotModify lock**

Explanation

CanNotModify lock does not exist as a type of resource lock in Azure. It is not a valid option for allowing modification while preventing deletion of a resource.

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.

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

Domain

Describe Azure management and governance (30–35%)

Question 5 Skipped

A developer deploys event-driven code in Azure that runs without the need for server management and is billed solely based on execution time. Which Azure concept does this represent?

Correct answer

◯ **Serverless with consumption pricing**

Explanation

Serverless computing allows developers to run code without managing servers, automatically scaling based on demand, and being billed only for the actual execution time of the code. This

aligns with the scenario of deploying event-driven code in Azure without server management and being billed solely based on execution time, making it the correct choice.

○ **IaaS with fixed pricing**

Explanation

IaaS (Infrastructure as a Service) typically involves managing virtual machines, storage, and networking resources, which requires server management. It usually comes with fixed pricing based on the resources provisioned, regardless of actual usage. This choice does not align with the scenario of deploying event-driven code in Azure without server management and billing based on execution time.

○ **PaaS with subscription pricing**

Explanation

PaaS (Platform as a Service) provides a platform for developers to build, deploy, and manage applications without the complexity of infrastructure management. It often involves subscription pricing based on the resources allocated, rather than direct execution time. While PaaS can offer scalability and flexibility, it does not match the scenario described in the question.

○ **SaaS with per-user pricing**

Explanation

SaaS (Software as a Service) delivers software applications over the internet on a subscription basis, typically with pricing based on the number of users or features used. This choice does not relate to the scenario of deploying event-driven code in Azure without server management and being billed based on execution time.

Overall explanation

Serverless with consumption pricing: This is the correct answer. In a **serverless** model, the developer writes event-driven code (like Azure Functions), and Azure automatically handles the infrastructure. The code runs only when needed and is billed based on the actual execution

time, which is characteristic of **consumption pricing**. There is no need to manage or provision servers in a serverless environment.

Why the other options are incorrect:

- **IaaS with fixed pricing**: **IaaS (Infrastructure-as-a-Service)** involves managing virtual machines or infrastructure. It does not eliminate server management in the same way as serverless. Moreover, **fixed pricing** is not a feature of IaaS as pricing is often based on resource usage, not just fixed amounts.

- **PaaS with subscription pricing**: **PaaS (Platform-as-a-Service)** offers a managed platform for applications, but it typically involves paying for the platform or resources over a subscription, not based on execution time like in a serverless scenario. While PaaS simplifies infrastructure management, the billing model described is more aligned with **serverless**.

- **SaaS with per-user pricing**: **SaaS (Software-as-a-Service)** typically involves using ready-made applications hosted in the cloud. This doesn't align with the description of event-driven code and execution-time billing, as SaaS is a fully managed service typically billed on a **per-user** or **subscription** basis, not based on how the code executes.

Thus, **Serverless with consumption pricing** is the best fit for the scenario described.

Domain

Describe cloud concepts (25–30%)

Question 6 Skipped

Which of the following is **NOT** a feature of **Azure Service Health**?

- ○ **Provides real-time notifications of service outages in Azure**

Explanation

Azure Service Health does provide real-time notifications of service outages in Azure, allowing users to stay informed about any disruptions in their services.

◯ **Informs about planned maintenance that may affect services**

Explanation

Azure Service Health does inform users about planned maintenance that may affect their services, giving them the opportunity to prepare for any potential downtime or disruptions.

◯ **Provides health alerts about the status of Azure resources**

Explanation

Azure Service Health does provide health alerts about the status of Azure resources, helping users monitor the health and availability of their resources in the Azure environment.

Correct answer

◯ **Tracks and resolves performance issues for applications**

Explanation

Azure Service Health does not track and resolve performance issues for applications. It primarily focuses on providing information about service outages, planned maintenance, and health alerts for Azure resources.

Overall explanation

Azure Service Health provides updates on Azure-wide service issues, planned maintenance, and health advisories but doesn't focus on tracking or resolving application performance issues. For application-level monitoring, **Application Insights** is the correct service.

Domain

Describe Azure management and governance (30–35%)

Question 7 Skipped

An IT team deploys a solution in Azure requiring auto-scaling web servers, fault-tolerant database VMs, and remote desktop access for employees. Which services align with these needs? (Select all that apply.)

Correct selection

☐ **Availability Sets**

Explanation

Availability Sets in Azure ensure high availability of applications by distributing VMs across multiple physical servers. This aligns with the need for fault-tolerant database VMs in the solution deployed by the IT team.

Correct selection

☐ **Azure Virtual Desktop**

Explanation

Azure Virtual Desktop provides remote desktop access for employees, allowing them to access their desktops and applications from anywhere. This aligns with the requirement for remote desktop access for employees in the solution deployed by the IT team.

☐ **Azure File Sync**

Explanation

Azure File Sync is a service that synchronizes files between on-premises servers and Azure storage. While it can be useful for file synchronization, it does not directly align with the needs of auto-scaling web servers, fault-tolerant database VMs, or remote desktop access in the solution deployed by the IT team.

Correct selection

☐ **Virtual Machine Scale Sets**

Explanation

Virtual Machine Scale Sets in Azure allow for the automatic scaling of identical virtual machines to meet demand. This aligns with the requirement for auto-scaling web servers in the solution deployed by the IT team.

Overall explanation

To meet the requirements of **auto-scaling web servers**, **fault-tolerant database VMs**, and **remote desktop access for employees**, the appropriate Azure services would be:

Virtual Machine Scale Sets

- **Virtual Machine Scale Sets (VMSS)** allow you to deploy and manage a set of identical VMs that automatically scale in or out based on demand. This aligns with the need for **auto-scaling web servers**.
- VMSS ensures that the web servers can automatically adjust the number of instances to handle changing traffic loads.

Availability Sets

- **Availability Sets** are used to ensure that VMs are distributed across different fault domains and update domains within a data center. This ensures **fault tolerance** for the database VMs and other VMs in the application, minimizing downtime during maintenance or hardware failures.
- By placing VMs in an Availability Set, you can make sure that they are fault-tolerant and highly available.

Azure Virtual Desktop

- **Azure Virtual Desktop (AVD)** is a fully managed desktop and app virtualization service in Azure that allows employees to securely access remote desktops and applications.
- This aligns with the requirement for **remote desktop access for employees**. It provides virtual desktops that employees can access from anywhere, which is

perfect for remote work.

Incorrect -

Azure File Sync

- **Azure File Sync** is a service that syncs on-premises file servers with Azure File Shares, enabling centralization of file services in Azure.
- While this is a useful service for file storage and syncing, it does not directly address the requirements for auto-scaling web servers, fault-tolerant database VMs, or remote desktop access.

Domain

Describe Azure architecture and services (35–40%)

Question 8 Skipped

An IT administrator needs to stay informed about a planned maintenance event that is impacting Azure virtual machines in the East US region. To receive real-time notifications and updates about this event, which Azure service should the admin use?

○ **Azure Monitor**

Explanation

Azure Monitor is a service that provides monitoring and analytics for applications and infrastructure in Azure. While it can be used to monitor the performance and availability of virtual machines, it is not specifically designed to provide real-time notifications and updates about planned maintenance events impacting specific regions.

○ **Azure Advisor**

Explanation

Azure Advisor is a service that provides personalized recommendations to optimize Azure resources for high availability, security, performance, and cost. While it can offer guidance on

best practices and recommendations, it does not provide real-time notifications about planned maintenance events impacting specific regions.

Correct answer

◯ **Azure Service Health**

Explanation

Azure Service Health is the correct choice for the IT administrator to stay informed about planned maintenance events impacting Azure resources, including virtual machines. It provides real-time notifications, updates, and guidance during service incidents and maintenance events, helping users to stay informed and take necessary actions.

◯ **Azure Log Analytics**

Explanation

Azure Log Analytics is a service that collects and analyzes log and performance data from various sources in Azure. While it can be used to monitor and troubleshoot virtual machine issues, it is not specifically designed to provide real-time notifications and updates about planned maintenance events impacting specific regions.

Overall explanation

Correct Answer: **Azure Service Health**

Azure Service Health provides personalized alerts and guidance for service issues that affect your Azure resources. It helps admins track planned maintenance, service incidents, and health advisories specific to their resources. By using **Azure Service Health**, IT administrators can receive **real-time notifications** about maintenance events or service issues that might impact their workloads, such as virtual machines in the East US region.

Key features of Azure Service Health:

- **Planned maintenance notifications**: Stay informed about upcoming maintenance events that may affect your resources.

- **Service incidents**: Get alerts when there are unplanned service disruptions or incidents.
- **Health advisories**: Receive important advisories that may impact resource performance or compliance.

Why the other options are incorrect:

- **Azure Monitor**: While **Azure Monitor** helps collect, analyze, and act on telemetry data from Azure resources, it's more focused on performance metrics, logs, and monitoring system health, rather than providing notifications about planned maintenance or service incidents.
- **Azure Advisor**: **Azure Advisor** provides personalized best practices for optimizing Azure resources in terms of cost, security, performance, and availability. It doesn't handle real-time notifications about service health or planned maintenance.
- **Azure Log Analytics**: **Log Analytics** is part of **Azure Monitor** and allows for querying and analyzing log data, but it doesn't provide real-time notifications about planned maintenance events or incidents. It's more for gathering insights from operational logs.

Domain

Describe Azure management and governance (30–35%)

Question 9 Skipped

_____ service is available to transfer on-premises data to Blob storage when large datasets or network constraints make uploading data over the wire unrealistic.

○ **Azure Data Factory**

Explanation

Azure Data Factory is a cloud-based data integration service that allows you to create data-driven workflows for orchestrating and automating data movement and data transformation. While it can be used to transfer data between different data stores, it is not specifically designed for transferring on-premises data to Blob storage in scenarios where large datasets or network constraints make uploading data over the wire unrealistic.

◯ **Azure FileSync**

Explanation

Azure FileSync is a service in Microsoft Azure that enables you to synchronize files between on-premises servers and Azure File storage. While it helps in syncing files, it is not specifically designed for transferring large datasets to Blob storage when network constraints or large datasets make uploading data over the wire unrealistic.

◯ **Azure Blob Storage**

Explanation

Azure Blob Storage is a cloud storage service provided by Microsoft Azure that allows you to store large amounts of unstructured data, such as text or binary data. While it is used for storing data, it is not specifically designed for transferring on-premises data to Blob storage in scenarios where large datasets or network constraints make uploading data over the wire unrealistic.

Correct answer

◯ **Azure Data Box**

Explanation

Azure Data Box is a physical device provided by Microsoft Azure that allows you to transfer large amounts of data to Azure Blob storage when network constraints or large datasets make uploading data over the wire impractical. It provides a secure and efficient way to transfer data from on-premises environments to Azure storage.

Overall explanation

From the Official Azure Documentation:

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:

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

A number of solutions exist for migrating existing data to Blob storage:

- ***Azure Data Box*** service is available to transfer on-premises data to Blob storage when large datasets or network constraints make uploading data over the wire unrealistic. Depending on your data size, you can request Azure Data Box Disk, Azure Data Box, or Azure Data Box Heavy devices from Microsoft. You can then copy your data to those devices and ship them back to Microsoft to be uploaded into Blob storage.

- **AzCopy** is an easy-to-use command-line tool for Windows and Linux that copies data to and from Blob storage, across containers, or across storage accounts. For more information about AzCopy, see Transfer data with the AzCopy v10.

and more..

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

Domain

Describe Azure architecture and services (35–40%)

Question 10 Skipped

Which of the following scenarios is a suitable use case for applying a resource lock?

Correct answer

◯ **Ensuring a critical storage account is not accidentally deleted.**

Explanation

Applying a resource lock to a critical storage account can help ensure that it is not accidentally deleted. Resource locks prevent users from deleting or modifying a resource, providing an additional layer of protection for important resources.

◯ **Restricting network access to an Azure SQL database.**

Explanation

Restricting network access to an Azure SQL database is more appropriately managed through network security groups, firewall rules, and Entra ID authentication. Resource locks are not designed for this specific use case.

◯ **Preventing read access to a development virtual machine.**

Explanation

Resource locks are not typically used to prevent read access to a virtual machine. Instead, access control and permissions should be managed through Azure RBAC (Role-Based Access Control) to control who can read, write, and manage Azure resources.

◯ **Automating the deployment of resources using templates.**

Explanation

Automating the deployment of resources using templates is not a suitable use case for applying a resource lock. Resource locks are intended for protecting individual resources from accidental deletion or modification, rather than for automating deployment processes.

Overall explanation

Using a lock, READ access is never affected. Read below 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.

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

Domain

Describe Azure management and governance (30–35%)

Question 11 Skipped

In the context of Infrastructure as Code (IaC), _____ are independent files, typically containing set of resources meant to be deployed together.

- ○ Functions
- ○ Units
- ○ Methods

Correct answer

- ◯ Modules

Explanation

Modules in the context of Infrastructure as Code (IaC) are independent files that contain a set of related resources meant to be deployed together. They help in organizing and managing infrastructure configurations efficiently.

Overall explanation

From the official Azure documentation:

One of the goals of using code to deploy infrastructure is to avoid duplicating work or creating multiple templates for the same or similar purposes. Infrastructure modules should be reusable and flexible and should have a clear purpose.

Modules are independent files, typically containing set of resources meant to be deployed together. Modules allow you to break complex templates into smaller, more manageable sets of code. You can ensure that each module focuses on a specific task and that all modules are reusable for multiple deployments and workloads.

Reference: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/infrastructure-as-code

Domain

Describe Azure management and governance (30–35%)

Question 12 Skipped

A company is tracking performance and reliability of its Azure-hosted application by analyzing logs for errors, setting up notifications for high memory usage, and diagnosing web app performance issues. Which Azure Monitor components are being used? (Select all that apply.)

Correct selection

☐ **Application Insights**

Explanation

Application Insights is used to diagnose web app performance issues by providing real-time insights into the application's performance, usage, and availability. In this situation, Application

Insights is being used to track the performance and reliability of the Azure-hosted application.

☐ **Azure Service Health**

Explanation

Azure Service Health provides personalized guidance and support when Azure services are affected by outages or incidents. While Azure Service Health is an important component for monitoring the overall health of Azure services, it is not directly related to tracking the performance and reliability of a specific application through log analysis and performance diagnostics.

Correct selection

☐ **Azure Monitor Alerts**

Explanation

Azure Monitor Alerts allow users to set up notifications and alerts based on metrics, logs, and activity logs. In this case, Azure Monitor Alerts are being used to notify the company of high memory usage, helping them monitor the application's performance and reliability.

Correct selection

☐ **Log Analytics**

Explanation

Log Analytics is used for analyzing logs and collecting data from various sources, including Azure resources, applications, and operating systems. In this scenario, Log Analytics is being used to track performance and reliability by analyzing logs for errors.

Overall explanation

Correct Answers:

Log Analytics
Azure Monitor Alerts
Application Insights

- **Log Analytics**:

  Log Analytics is used to collect, query, and analyze data from various sources in Azure, such as VMs. Since the company is querying VM logs for errors, **Log Analytics** is being used to analyze and troubleshoot issues based on log data.

- **Azure Monitor Alerts**:

  Azure Monitor Alerts enables the company to set up custom alerts for certain performance thresholds, like high memory usage. Alerts can be triggered based on specific metrics or log data, and the company is using it to stay informed of critical issues.

- **Application Insights**:

  Application Insights is used to monitor the performance of applications, especially for tracking metrics like response times, dependencies, and exceptions. Since the company is analyzing web app performance issues, **Application Insights** is actively being used to track application-specific telemetry.

Why **Azure Service Health** is incorrect:

- **Azure Service Health** is designed to inform users about service issues, planned maintenance, or health advisories affecting Azure services. It does not provide log analytics or performance tracking for virtual machines or web applications. Since the scenario focuses on monitoring and alerting for application and VM performance, **Azure Service Health** is not relevant here.

Domain

Describe Azure management and governance (30–35%)

Question 13 Skipped

Which of the following is a key benefit of using Role-Based Access Control (RBAC) over traditional access control methods?

Correct answer

◯ **RBAC allows you to assign permissions to specific roles rather than individual users.**

Explanation

This is a key benefit of using RBAC over traditional access control methods. By assigning permissions to specific roles, rather than individual users, RBAC simplifies access management and reduces the complexity of managing permissions for multiple users.

◯ **RBAC provides stronger encryption for sensitive data.**

Explanation

RBAC does not directly provide stronger encryption for sensitive data. Encryption is a separate security measure that can be implemented in addition to RBAC to protect sensitive data.

◯ **RBAC provides centralized management of user identities and access.**

Explanation

RBAC does provide centralized management of user identities and access, but this is not a key benefit unique to RBAC over traditional access control methods. Centralized management is a common feature in both RBAC and traditional methods.

◯ **RBAC supports a wider range of authentication protocols than traditional methods.**

Explanation

RBAC does not necessarily support a wider range of authentication protocols than traditional methods. The focus of RBAC is on assigning permissions based on roles, rather than the authentication protocols used.

Overall explanation

The correct answer is : RBAC allows you to assign permissions to specific roles rather than individual users.

Role-Based Access Control (RBAC) is an approach to access control that allows you to manage user access based on the roles they perform within an organization. With RBAC, you can define a set of roles, each with a specific set of permissions, and then assign users to those roles.

One of the key benefits of RBAC over traditional access control methods is that it allows you to assign permissions to specific **roles** rather than individual users. This means that when a user's role changes, their permissions can be automatically adjusted without the need for manual updates. This can help to streamline the process of managing access control and reduce the risk of errors or oversights.

RBAC provides centralized management of user identities and access: This is incorrect because RBAC does not provide centralized management of user identities and access. Instead, RBAC is a way to manage access control for specific resources within an organization.

RBAC supports a wider range of authentication protocols than traditional methods: This is incorrect because RBAC does not necessarily support a wider range of authentication protocols than traditional methods. RBAC is a method of access control, whereas authentication protocols are used to verify the identity of users.

RBAC provides stronger encryption for sensitive data: This is incorrect because RBAC does not provide stronger encryption for sensitive data. Encryption is a method of protecting data from unauthorized access, whereas RBAC is a way to manage access control for specific resources within an organization.

Therefore, the correct answer is 'RBAC allows you to assign permissions to specific roles rather than individual users', as RBAC allows you to assign permissions to specific roles rather than individual users, making it easier to manage access control and reduce the risk of errors or oversights.

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

https://docs.microsoft.com/en-us/azure/role-based-access-control/best-practices

Domain

Describe Azure architecture and services (35–40%)

Question 14 Skipped

You are the lead architect of your organization. One of the teams has a requirement to copy hundreds of TBs of data to Azure storage in a secure and efficient manner. The data can be ingested one time or an ongoing basis for archival scenarios.

Which of the following would be a good solution for this use case?

Correct answer

◯ **Azure Data Box**

Explanation

Azure Data Box is a physical device provided by Microsoft for secure and efficient data transfer to Azure storage. It is designed for scenarios where large amounts of data need to be ingested quickly and securely, making it an ideal solution for copying hundreds of TBs of data to Azure storage in a secure and efficient manner.

◯ **Azure Data Lake Storage**

Explanation

Azure Data Lake Storage is a scalable and secure data lake service for big data analytics. While it can handle large volumes of data, it may not be the most efficient solution for copying hundreds of TBs of data to Azure storage in a secure and efficient manner compared to Azure Data Box, which is specifically designed for such scenarios.

◯ **Azure Cosmos DB**

Explanation

Azure Cosmos DB is a globally distributed, multi-model database service for scalable applications. It is not specifically designed for large-scale data ingestion or archival scenarios, making it less suitable for the use case of copying hundreds of TBs of data to Azure storage.

○ **Azure File Sync**

Explanation

Azure File Sync is a service that enables synchronization of on-premises file servers with Azure Files. While it can be used for syncing files between on-premises and Azure storage, it may not be the most efficient solution for copying hundreds of TBs of data to Azure storage in a secure and efficient manner.

Overall explanation

From the Official Azure Documentation:

Azure Data Box Gateway is a storage solution that enables you to seamlessly send data to Azure. This article provides you an overview of the Azure Data Box Gateway solution, benefits, key capabilities, and the scenarios where you can deploy this device.

Data Box Gateway is a virtual device based on a virtual machine provisioned in your virtualized environment or hypervisor. The virtual device resides in your premises and you write data to it using the NFS and SMB protocols. The device then transfers your data to Azure block blob, page blob, or Azure Files.

Use cases -

Data Box Gateway can be leveraged for transferring data to the cloud such as cloud archival, disaster recovery, or if there is a need to process your data at cloud scale. Here are the various scenarios where Data Box Gateway can be used for data transfer.

- **Cloud archival** - Copy hundreds of TBs of data to Azure storage using Data Box Gateway in a secure and efficient manner. The data can be ingested one time or an ongoing basis for archival scenarios.

- **Continuous data ingestion** - Continuously ingest data into the device to copy to the cloud, regardless of the data size. As the data is written to the gateway device, the device uploads the data to Azure Storage.

- **Initial bulk transfer followed by incremental transfer** - Use Data Box for the bulk transfer in an offline mode (initial seed) and Data Box Gateway for

incremental transfers (ongoing feed) over the network.

Reference: https://docs.microsoft.com/en-us/azure/databox-gateway/data-box-gateway-overview

Domain

Describe Azure architecture and services (35–40%)

Question 15 Skipped

What is the default action for a Network Security Rule (NSG) rule if no other action is specified?

○ **Block**

Explanation

Setting the default action for a Network Security Rule (NSG) rule to block means that all traffic will be blocked unless there is a specific rule allowing it. This is not the correct default action for NSG rules, as the default action is to deny traffic.

○ **Allow**

Explanation

If no other action is specified in a Network Security Group (NSG) rule, the default action is not to allow traffic. This means that the traffic will be denied by default unless there is a specific rule allowing it.

Correct answer

○ **Deny**

Explanation

The correct default action for a Network Security Rule (NSG) rule when no other action is specified is to deny traffic. This ensures that any traffic not explicitly allowed by a rule will be

blocked by default.

Overall explanation

The default action for an NSG rule if no other action is specified is **DENY**.

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

Domain

Describe Azure architecture and services (35–40%)

Question 16 Skipped

True or False:

Each zone is made up of one or more datacentres equipped with common power, cooling, and networking.

○ True

Correct answer

○ False

Overall explanation

From the Official Azure Documentation:

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

Reference: https://azure.microsoft.com/en-ca/global-infrastructure/

Domain

Describe Azure architecture and services (35–40%)

Question 17 Skipped

As the owner of a streaming platform deployed on Azure, you notice a huge spike in traffic whenever a new web-series in released but moderate traffic otherwise. Which of the following is a clear benefit of this type of workload?

○ **High latency**

Explanation

High latency refers to delays in data transmission or processing, which can negatively impact user experience on a streaming platform. The benefit described in the question is related to the workload's ability to handle sudden increases in traffic, not the latency experienced by users.

○ **Load balancing**

Explanation

Load balancing is the process of distributing incoming network traffic across multiple servers to optimize resource utilization, maximize throughput, and minimize response time. While load balancing is important for distributing traffic efficiently, the benefit described in the question is more specifically related to the workload's ability to scale resources dynamically based on demand.

○ **High availability**

Explanation

High availability ensures that your streaming platform is always accessible and operational, regardless of traffic spikes or fluctuations. However, the benefit described in the question is

related to the workload's behavior during traffic spikes, not the platform's availability during normal operations.

Correct answer

◯ **Elasticity**

Explanation

Elasticity allows the streaming platform to automatically scale resources up or down based on demand. This means that during traffic spikes, additional resources can be provisioned to handle the increased load, ensuring smooth performance without over-provisioning during periods of moderate traffic.

Overall explanation

Elasticity in this case is the ability to provide additional compute resource when needed (spikes) and reduce the compute resource when not needed to reduce costs. Load Balancing and High Availability are also great advantages the streaming platform would enjoy, but Elasticity is the option that best describes the workload in the question.

Autoscaling is an example of elasticity.

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

Domain

Describe cloud concepts (25–30%)

Question 18 Skipped

A company frequently experiences variable workloads with unpredictable demand spikes for its Azure-hosted application. It wants to optimize costs while ensuring that resources are available during peak usage periods without incurring charges during low-demand periods. Which combination of pricing models would be most suitable to achieve this?

○ **Spot Instances for scalability and Reserved Instances for baseline capacity**

Explanation

While Reserved instances are great for ensuring baseline capacity, spot instances are not guaranteed and aren't meant for scalability.

Correct answer

○ **Consumption-based model for unpredictable demand and Reserved Instances for long-term predictable usage**

Explanation

A consumption-based model is ideal for unpredictable demand as it allows for flexible usage and payment based on actual resource consumption. Reserved Instances are beneficial for long-term predictable usage, offering cost savings and resource availability during peak periods without incurring charges during low-demand periods.

○ **Consumption-based model with Spot Instances for cost reduction during low demand periods**

Explanation

While a consumption-based model is suitable for unpredictable demand, using Spot Instances for cost reduction during low-demand periods may not guarantee resource availability during peak usage periods. Reserved Instances would be more appropriate for ensuring resources are available during peak periods without incurring charges during low-demand periods.

○ **Pay-as-you-go pricing for both unpredictable and predictable workloads**

Explanation

Pay-as-you-go pricing may not be the most cost-effective option for a company with variable workloads and unpredictable demand spikes, as it could result in higher costs during peak periods. Utilizing Reserved Instances for both unpredictable and predictable workloads may not optimize costs effectively.

Overall explanation

In this scenario, the company can use the **consumption-based model** to handle unpredictable demand and **Reserved Instances** to ensure cost optimization for baseline, predictable usage. **Reserved Instances** offer discounted pricing in exchange for a one- or three-year commitment, making it ideal for stable, predictable workloads. Meanwhile, the consumption-based model ensures the flexibility to scale during variable demand periods without overpaying when resources are not needed.

Domain

Describe cloud concepts (25–30%)

Question 19 Skipped

_____ **Infrastructure as Code** involves writing a definition that defines how you want your environment to look. In this definition, you specify a desired outcome rather than how you want it to be accomplished.

- ○ **Imperative**

Correct answer

- ◯ **Declarative**

- ○ **Defined**

- ○ **Ad-Hoc**

Overall explanation

From the official Azure documentation:

Declarative Infrastructure as Code involves writing a definition that defines how you want your environment to look. In this definition, you specify a desired outcome rather than how you want it to be accomplished. The tooling figures out how to make the outcome happen by inspecting your current state, comparing it to your target state, and then applying the differences.

Reference: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/infrastructure-as-code

Domain

Describe Azure management and governance (30–35%)

Question 20 Skipped

Which of the following two storage solutions are built to handle NoSQL data?

Correct selection

☐ **Azure Cosmos DB**

Explanation

Azure Cosmos DB is a globally distributed, multi-model database service designed to handle NoSQL data. It supports key-value, graph, column-family, and document data models, making it a suitable choice for handling various types of NoSQL data.

Correct selection

☐ **Azure Table Storage**

Explanation

Azure Table Storage is a NoSQL data store that is designed to store semi-structured data such as key-value pairs. It is a good choice for applications that require fast and scalable storage of non-relational data, making it a suitable solution for handling NoSQL data.

☐ **Azure NoSQL Database**

Explanation

Azure NoSQL Database is not a specific service offered by Microsoft Azure. NoSQL databases are a category of databases that do not use the traditional tabular structure of relational databases, and Azure offers specific services like Azure Cosmos DB and Azure Table Storage to handle NoSQL data.

☐ **Azure SQL Database**

Explanation

Azure SQL Database is a fully managed relational database service that is based on the SQL Server engine. It is designed to handle structured data in a relational format, making it more suitable for traditional SQL data rather than NoSQL data.

Overall explanation

From the Official Azure Documentation:

Azure Table storage is a service that stores non-relational structured data (also known as structured NoSQL data) in the cloud, providing a key/attribute store with a schemaless design. Because Table storage is schemaless, it's easy to adapt your data as the needs of your application evolve.

Azure Cosmos DB is a fully managed NoSQL database for modern app development. Single-digit millisecond response times, and automatic and instant scalability, guarantee speed at any scale.

Reference: https://docs.microsoft.com/en-us/azure/cosmos-db/introduction

https://docs.microsoft.com/en-us/azure/storage/tables/table-storage-overview

Domain

Describe Azure architecture and services (35–40%)

Question 21 Skipped

Which cloud deployment model is best suited for organizations with extremely strict data security and compliance requirements?

○ **Public cloud**

Explanation

Public cloud deployment models are not typically the best choice for organizations with extremely strict data security and compliance requirements. Public clouds involve sharing resources and infrastructure with other organizations, which may raise concerns about data security and compliance.

○ **Hybrid cloud**

Explanation

Hybrid cloud deployment models combine public and private cloud resources, which may not be ideal for organizations with extremely strict data security and compliance requirements. While hybrid clouds offer flexibility, they also introduce additional complexities in managing security and compliance across different environments.

Correct answer

○ **Private cloud**

Explanation

Private cloud deployment models are best suited for organizations with extremely strict data security and compliance requirements. Private clouds offer dedicated resources and infrastructure, allowing organizations to have more control over their data and security measures.

○ **Community cloud**

Explanation

Community cloud deployment models involve sharing resources and infrastructure with a specific community of users, which may not provide the level of control and security required by organizations with extremely strict data security and compliance requirements. Community clouds may not offer the same level of customization and security measures as private clouds.

Overall explanation

The correct answer is **Private Cloud.** Private clouds are cloud deployments that are dedicated to a single organization and are hosted either on-premises or in a third-party data center. Private clouds offer greater control over data security and compliance, as the organization has direct control over the infrastructure and can implement security measures tailored to their specific requirements. Private clouds can also be used to address regulatory compliance requirements that may restrict the use of public clouds for certain types of data.

In contrast, public clouds and community clouds are shared by multiple organizations, which can raise concerns about data security and compliance. Hybrid clouds, which combine elements of public and private clouds, can also be used to address data security and compliance requirements, but they can be more complex to manage.

Reference: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-private-cloud

Domain

Describe cloud concepts (25–30%)

Question 22 Skipped

True or False:

Azure DNS can manage DNS records for your Azure services, but cannot provide DNS for your external resources.

Correct answer

○ **False**

○ **True**

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.

Azure DNS can manage DNS records for your Azure services **and provide DNS for your external resources as well.** Azure DNS is integrated in the Azure portal and uses the same credentials, support contract, and billing as your other Azure services.

DNS billing is based on the number of DNS zones hosted in Azure and on the number of DNS queries received. To learn more about pricing, see Azure DNS pricing.

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

Domain

Describe Azure architecture and services (35–40%)

Question 23 Skipped

In the context of Azure networking, what is the purpose of a Network Security Group (NSG) associated with a private endpoint?

○ **To manage IP address assignments for the private endpoint.**

Explanation

Managing IP address assignments for a private endpoint is typically handled through the Azure networking configuration, such as Virtual Network (VNet) settings and subnet configurations. Network Security Groups (NSGs) are focused on enforcing access control rules rather than managing IP address assignments.

Correct answer

○ **To enforce access control rules on inbound and outbound traffic to the private endpoint.**

Explanation

Network Security Groups (NSGs) are used to enforce access control rules on inbound and outbound traffic to resources in Azure, including private endpoints. By associating an NSG with a private endpoint, you can define rules to allow or deny specific types of traffic to and from the private endpoint, enhancing security and controlling network access.

○ **To ensure the availability and uptime of the private endpoint.**

Explanation

Ensuring the availability and uptime of a private endpoint is more related to network monitoring, redundancy, and fault tolerance mechanisms rather than the role of a Network Security Group (NSG). NSGs are primarily used for access control and security enforcement on network traffic to and from resources, including private endpoints.

○ **To encrypt data traffic between the private endpoint and the Azure service.**

Explanation

Encrypting data traffic between a private endpoint and an Azure service is typically achieved through other means such as Transport Layer Security (TLS) or Virtual Network Service Endpoints. While encryption is important for data security, it is not the primary purpose of a Network Security Group (NSG) associated with a private endpoint.

Overall explanation

A Network Security Group (NSG) associated with a private endpoint is used to enforce access control rules on the inbound and outbound traffic to the private endpoint. This helps in controlling and restricting the network traffic flow to and from the private endpoint, enhancing security and compliance.

Reference: https://learn.microsoft.com/en-us/azure/private-link/private-link-overview

Domain

Describe Azure architecture and services (35–40%)

Question 24 Skipped

You have managed a Web App that you developed and deployed On-Prem for a long time, but would now like to move it to Azure and relieved of all the manual administration and maintenance. Which of the following buckets would be most suitable for your use case?

○ **Infrastructure as a Service (IaaS)**

Explanation

Infrastructure as a Service (IaaS) provides virtualized computing resources over the internet and requires manual administration and maintenance of the infrastructure. While it offers more control than SaaS, it does not provide the level of automation and relief from manual tasks that you are looking for in moving your Web App to Azure.

○ **Software as a Service (SaaS)**

Explanation

Software as a Service (SaaS) would not be the most suitable option for your use case as it involves using software applications over the internet that are managed by a third-party provider. This option does not provide the level of control and customization needed for moving your Web App to Azure.

Correct answer

◯ **Platform as a Service (PaaS)**

Explanation

Platform as a Service (PaaS) would be the most suitable option for your use case. PaaS provides a platform for developers to build, deploy, and manage applications without the complexity of infrastructure management. It allows you to focus on developing and deploying your Web App without worrying about manual administration and maintenance tasks.

◯ **Database as a Service (DaaS)**

Explanation

Database as a Service (DaaS) is a cloud computing service model that provides database management and hosting. While it can be beneficial for managing databases in the cloud, it is not the most suitable option for moving your entire Web App to Azure and relieving manual administration and maintenance tasks.

Overall explanation

From the Official Azure Documentation:

Azure App Service is a platform-as-a-service (PaaS) offering that lets you create web and mobile apps for any platform or device and connect to data anywhere, in the cloud or on-premises. App Service includes the web and mobile capabilities that were previously delivered separately as Azure Websites and Azure Mobile Services.

References: https://docs.microsoft.com/en-us/azure/security/fundamentals/paas-applications-using-app-services

Domain

Describe cloud concepts (25–30%)

Question 25 Skipped

If your organization has many Azure subscriptions, which of the following is useful to efficiently manage access, policies, and compliance for those subscriptions?

○ **Azure Blueprints**

Explanation

Azure Blueprints are a service that allows organizations to define a repeatable set of resources that adhere to standards, patterns, and requirements. While Azure Blueprints are useful for creating standardized environments, they are not specifically focused on managing access, policies, and compliance across multiple subscriptions within an organization.

○ **Azure Subscriptions**

Explanation

Azure Subscriptions are used to group resources and manage billing for Azure services. While they are essential for organizing resources and managing costs, they do not provide the necessary tools to efficiently manage access, policies, and compliance across multiple subscriptions within an organization.

Correct answer

○ **Azure Management Groups**

Explanation

Azure Management Groups are a way to efficiently manage access, policies, and compliance for multiple Azure subscriptions. By organizing subscriptions into management groups, administrators can apply policies and access controls at the management group level, ensuring consistency and compliance across all subscriptions within the group.

○ **Azure Policy**

Explanation

Azure Policy is a service that allows organizations to create, assign, and manage policies to enforce compliance with corporate standards and service-level agreements. While Azure Policy

is essential for enforcing governance and compliance, it is not specifically designed to efficiently manage access, policies, and compliance for multiple subscriptions.

Overall explanation

From the Official Azure Documentation:

If your organization has many Azure subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. **Management groups** provide a governance scope above subscriptions. You organize subscriptions into management groups the governance conditions you apply cascade by inheritance to all associated subscriptions.

Management groups give you enterprise-grade management at scale no matter what type of subscriptions you might have. However, all subscriptions within a single management group must trust the same Azure Active Directory (Azure AD) tenant.

For example, you can apply policies to a management group that limits the regions available for virtual machine (VM) creation. This policy would be applied to all nested management groups, subscriptions, and resources, and allow VM creation only in authorized regions.

Reference: https://docs.microsoft.com/en-us/azure/governance/management-groups/overview

Domain

Describe Azure management and governance (30–35%)

Question 26 Skipped

_____ is a security framework that uses the principles of explicit verification, least privileged access, and assuming breach to keep users and data secure while allowing for common scenarios like access to applications from outside the network perimeter.

- ○ No Trust

Explanation

No Trust is not a commonly used security framework in the context of Azure or general security practices. It does not align with the principles of explicit verification, least privileged access, and assuming breach mentioned in the question.

Correct answer

◯ **Zero Trust**

Explanation

Zero Trust is a security framework that aligns with the principles of explicit verification, least privileged access, and assuming breach. It focuses on verifying every user and device trying to access resources, regardless of their location, to ensure security while allowing necessary access.

◯ **Less Trust**

Explanation

Less Trust is not a recognized security framework in the context of Azure or general security practices. It does not align with the principles of explicit verification, least privileged access, and assuming breach mentioned in the question.

◯ **Least Trust**

Explanation

Least Trust is not a recognized security framework in the context of Azure or general security practices. It does not align with the principles of explicit verification, least privileged access, and assuming breach mentioned in the question.

Overall explanation

From the Official Azure Documentation:

Zero Trust is a security framework that does not rely on the implicit trust afforded to interactions behind a secure network perimeter. Instead, it uses the principles of explicit

verification, least privileged access, and assuming breach to keep users and data secure while allowing for common scenarios like access to applications from outside the network perimeter.

App developers can improve app security, minimize the impact of breaches, and ensure that their applications meet their customers' security requirements by adopting Zero Trust principles.

Reference: https://docs.microsoft.com/en-us/security/zero-trust/develop/identity

Domain

Describe Azure architecture and services (35–40%)

Question 27 Skipped

When a blob is in the archive access tier, what must you do first before accessing it?

- ○ **Move it to File Storage**

Explanation

Moving the blob to File Storage is not the correct action to take when a blob is in the archive access tier. The first step should be to rehydrate the blob to make it accessible before considering any other actions.

- ○ **Add it to a new resource group**

Explanation

Adding the blob to a new resource group is not necessary before accessing a blob in the archive access tier. The first step should be to rehydrate the blob to make it accessible for use.

Correct answer

- ○ **Rehydrate it**

Explanation

When a blob is in the archive access tier, it needs to be rehydrated before it can be accessed. Rehydration is the process of moving the blob back to a hot or cool access tier where it can be readily accessed and used.

○ **Modify its policy**

Explanation

Modifying the policy of the blob is not the immediate step to take when a blob is in the archive access tier. The priority should be to rehydrate the blob to bring it back to a more accessible tier.

Overall explanation

From the Official Azure Documentation:

Rehydrate blob data from the archive tier

04/08/2020 • 6 minutes to read •

While a blob is in the archive access tier, it's considered offline and can't be read or modified. The blob metadata remains online and available, allowing you to list the blob and its properties. Reading and modifying blob data is only available with online tiers such as hot or cool. There are two options to retrieve and access data stored in the archive access tier.

1. Rehydrate an archived blob to an online tier - Rehydrate an archive blob to hot or cool by changing its tier using the Set Blob Tier operation.
2. Copy an archived blob to an online tier - Create a new copy of an archive blob by using the Copy Blob operation. Specify a different blob name and a destination tier of hot or cool.

Reference : https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-rehydration?tabs=azure-portal

Domain

Describe Azure architecture and services (35–40%)

Question 28 Skipped

Yes or No:

Subscriptions can be moved to another Management Group as well as merged into one Single subscription.

○ **Yes**

Explanation

Subscriptions can indeed be moved to another Management Group within the same directory, but they cannot be merged into a single subscription. Each subscription remains a separate entity with its own billing and resource management.

Correct answer

○ **No**

Explanation

The correct answer is No because while subscriptions can be moved to another Management Group, they cannot be merged into a single subscription. Each subscription maintains its individual identity and cannot be combined with others.

Overall explanation

Even though Subscriptions can be moved to another management group, they cannot be merged into 1 single subscription.

From the Official Azure Documentation:

Azure management groups

Azure management groups help you efficiently manage access, policies, and compliance for your subscriptions. Each management group is a container for one or more subscriptions.

Management groups are arranged in a single hierarchy. You define this hierarchy in your Azure Active Directory (Azure AD) tenant to align with your organization's structure and needs. The top level is called the *root management group*. You can define up to six levels of management groups in your hierarchy. Each subscription is contained by only one management group.

Azure provides four levels of management scope:

- Management groups
- Subscriptions
- Resource groups
- Resources

Any access or policy applied at one level in the hierarchy is inherited by the levels below it. A resource owner or subscription owner can't alter an inherited policy. This limitation helps improve governance.

> **Note**
>
> Tag inheritance is not yet supported but will be available soon.

This inheritance model lets you arrange the subscriptions in your hierarchy so that each subscription follows appropriate policies and security controls.

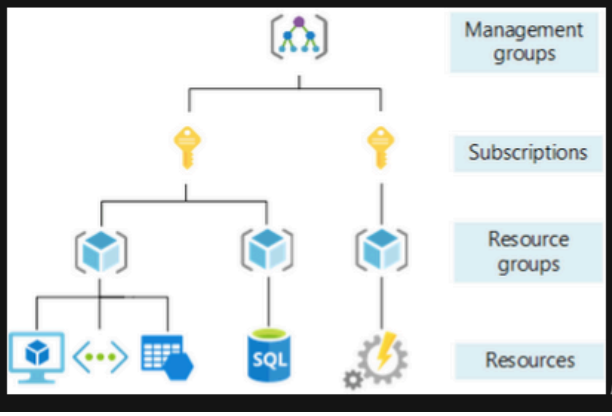


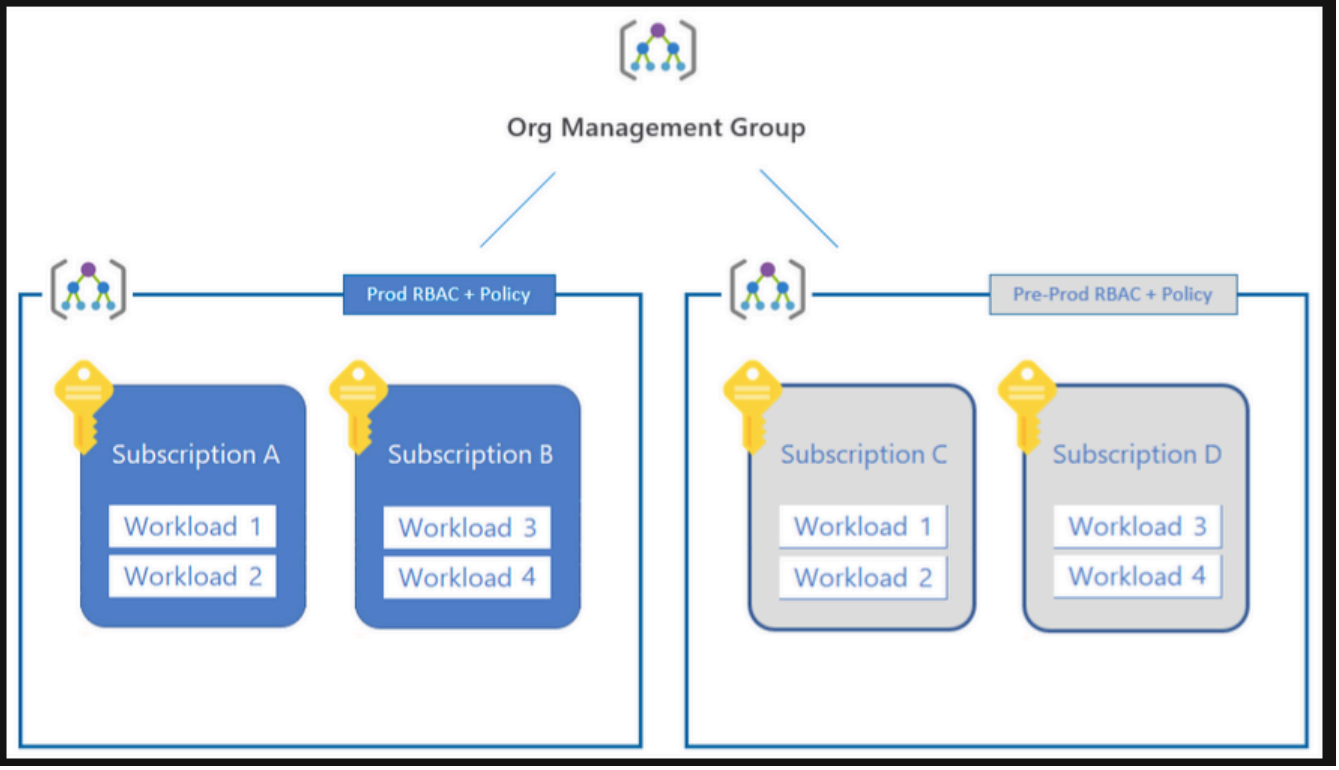
Figure 1: The four scope levels for organizing your Azure resources.

Create your management group hierarchy

When you define your management group hierarchy, first create the root management group. Then move all existing subscriptions in the directory into the root management group. New subscriptions are always created in the root management group. Later, you can move them to another management group.

When you move a subscription to an existing management group, it inherits the policies and role assignments from the management group hierarchy above it. Once you have established multiple subscriptions for your Azure workloads, you can create additional subscriptions to contain Azure services that other subscriptions share.

If you expect your Azure environment to grow, you should create management groups for production and nonproduction now, and apply appropriate policies and access controls at the management group level. New subscriptions will inherit the appropriate controls as they're added to each management group.



Reference: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/organize-subscriptions

Domain

Describe Azure management and governance (30–35%)

Question 29 Skipped

Which of the following is NOT a feature of Azure Monitor?

- ○ **Alerts**

Explanation

Alerts is a feature of Azure Monitor that enables you to set up notifications and automated responses based on predefined conditions. It helps you proactively monitor the health and performance of your Azure resources and take action when issues arise.

○ **Metrics**

Explanation

Metrics is a feature of Azure Monitor that provides visualizations and insights into the performance and health of your Azure resources. It allows you to monitor key metrics and track the performance of your applications and services.

Correct answer

○ **Database management**

Explanation

Database management is NOT a feature of Azure Monitor. Azure Monitor focuses on monitoring and analyzing the performance and health of your Azure resources, such as virtual machines, databases, and applications. Database management tasks are typically handled by other Azure services like Azure SQL Database or Azure Cosmos DB.

○ **Log Analytics**

Explanation

Log Analytics is a feature of Azure Monitor that allows you to collect, analyze, and visualize log data from your resources in Azure. It helps you gain insights into the performance and health of your applications and infrastructure.

Overall explanation

Azure Monitor is a service that provides full-stack monitoring capabilities for applications and infrastructure in Azure. It collects and analyzes telemetry data from a variety of sources,

including Azure resources, third-party resources, and custom applications. The key features of Azure Monitor include:

Log Analytics: This feature allows you to collect and analyze log data from various sources, including Azure resources, operating systems, and custom applications. It provides advanced querying and visualization capabilities to help you understand and troubleshoot issues.

Metrics: This feature provides a comprehensive view of the performance and health of your Azure resources, including virtual machines, databases, and web applications. It allows you to set up custom charts and alerts based on specific metrics.

Alerts: This feature enables you to set up notifications for specific conditions or events in your Azure environment, such as high CPU usage, application errors, or security threats. It supports various notification channels, including email, SMS, and webhooks.

Other option -

Database management: This is not a feature of Azure Monitor. There are other Azure services, such as Azure SQL Database and Azure Database for MySQL, that provide database management capabilities.

Reference: https://learn.microsoft.com/en-us/azure/azure-monitor/overview

Domain

Describe Azure management and governance (30–35%)

Question 30 Skipped

Which of the following services can host the following type of apps:

- **Web apps**
- **API apps**
- **WebJobs**
- **Mobile apps**

○ **Azure App Environment**

Explanation

Azure App Environment is not a valid service in Azure. There is no service called Azure App Environment that specifically hosts web apps, API apps, WebJobs, or mobile apps. This choice is incorrect in the context of hosting the mentioned types of applications.

◯ **Azure Bastion**

Explanation

Azure Bastion is a service that provides secure and seamless RDP and SSH access to virtual machines directly through the Azure portal. It is not designed for hosting web apps, API apps, WebJobs, or mobile apps. Therefore, this choice is incorrect for the given scenario.

◯ **Azure Arc**

Explanation

Azure Arc is not the correct choice for hosting web apps, API apps, WebJobs, or mobile apps. Azure Arc is a service that extends Azure management and services to any infrastructure, including on-premises, multi-cloud, and edge environments, but it is not designed for hosting application types like web apps or mobile apps.

Correct answer

◯ **Azure App Service**

Explanation

Azure App Service is the correct choice because it is a fully managed platform that enables you to build, deploy, and scale web apps, API apps, WebJobs, and mobile apps. It provides a flexible and scalable environment for hosting various types of applications.

Overall explanation

From the official Azure docs:

App Service enables you to build and host web apps, background jobs, mobile back-ends, and RESTful APIs in the programming language of your choice without managing infrastructure. It offers automatic scaling and high availability. App Service supports Windows and Linux. It enables automated deployments from GitHub, Azure DevOps, or any Git repo to support a continuous deployment model.

Types of app services

With App Service, you can host most common app service styles like:

- Web apps
- API apps
- WebJobs
- Mobile apps

Reference: https://learn.microsoft.com/en-us/training/modules/describe-azure-compute-networking-services/7-describe-application-hosting-options

Domain

Describe Azure architecture and services (35–40%)

Question 31 Skipped

How can you apply a resource lock to an Azure resource?

- ○ By creating a new resource group for the resource.

Correct answer

- ○ By using the Azure portal or Azure PowerShell

- ○ By using the Azure API for RBAC

- By configuring a network security group.
- By assigning a custom role to the resource.

Overall explanation

You can apply a resource lock to an Azure resource using the Azure portal or Azure PowerShell. This allows you to control access and modifications to the resource.

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

Domain

Describe Azure management and governance (30–35%)

Question 32 Skipped

Which of the following best describes the concept of "immutable infrastructure" in the context of IaC?

- Infrastructure that is managed through a graphical user interface.
- Infrastructure that cannot be changed once deployed.
- Infrastructure that is stored in a physical data center.

Correct answer

- Infrastructure that is recreated rather than modified in place.

Overall explanation

Immutable infrastructure refers to the practice of recreating infrastructure components whenever changes are needed rather than modifying them in place. This approach aligns with IaC principles, enhancing consistency and reducing configuration drift.

Reference: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/infrastructure-as-code

Domain

Describe Azure management and governance (30–35%)

Question 33 Skipped

A healthcare organization is tasked with ensuring that sensitive patient data across both Azure Blob Storage and an on-premises SQL server is properly classified and protected to meet strict regulatory compliance standards. Which Azure service or tool can assist in classifying and managing the sensitivity of this data across hybrid environments?

○ Azure Information Protection

Explanation

Azure Information Protection is a service that helps organizations classify and protect documents and emails by applying labels and encryption. While it is designed for data protection, it may not be the most suitable choice for the healthcare organization's requirement to classify and manage sensitive patient data across Azure Blob Storage and an on-premises SQL server in hybrid environments. Azure Purview is more tailored for data classification and management across hybrid environments.

Correct answer

○ **Azure Purview**

Explanation

Azure Purview is a data governance service that helps organizations discover, classify, and manage sensitive data across hybrid environments. It provides a unified view of data across

on-premises, multicloud, and SaaS sources, making it an ideal choice for classifying and managing sensitive patient data in Azure Blob Storage and on-premises SQL server to meet regulatory compliance standards.

◯ **Azure Security Center**

Explanation

Azure Security Center is a unified security management system that provides advanced threat protection across hybrid workloads. While it helps secure resources and detect threats, it does not offer specific capabilities for classifying and managing data sensitivity, making it less suitable for the healthcare organization's need to classify and protect patient data.

◯ **Microsoft Defender for Identity**

Explanation

Microsoft Defender for Identity is a tool that helps detect advanced threats, compromised identities, and malicious insider actions across hybrid environments. While it enhances security, it is not specifically designed for classifying and managing data sensitivity, making it less suitable for the healthcare organization's requirement to protect patient data.

Overall explanation

Azure Purview is an enterprise data governance service that helps organizations manage, classify, and secure their data across both cloud and on-premises environments. It provides features such as:

- **Data discovery**: It helps discover and classify sensitive data across various data stores, including Azure Blob Storage and on-premises systems like SQL Server.
- **Data cataloging**: It can create a unified catalog of data across hybrid environments, allowing for better visibility and control over sensitive information.
- **Compliance and regulatory needs**: Azure Purview supports compliance frameworks by classifying sensitive data based on built-in or custom classification rules, ensuring adherence to regulatory standards such as HIPAA, which is critical in healthcare.

Why the other options are incorrect:

- **Microsoft Defender for Identity**: This tool primarily focuses on protecting identities and detecting threats related to user activity. It is not specifically designed for classifying or managing data sensitivity across storage systems like Azure Blob Storage or on-premises databases.

- **Azure Security Center**: While Azure Security Center offers security management and threat protection for Azure resources, it doesn't specifically focus on classifying or managing sensitive data across hybrid environments like Azure Blob Storage and SQL servers. It is more about managing security posture and vulnerabilities.

- **Azure Information Protection**: This service helps classify and label data within documents and emails, but it is more focused on file-level protection rather than managing and classifying data across broader environments (like both Azure Blob Storage and on-premises SQL Server).

Domain

Describe Azure management and governance (30–35%)

Question 34 Skipped

A developer needs an Azure storage account to store unstructured data with high-performance access, supporting blobs and file shares in a single region. Which storage account and redundancy option best fits?

Correct answer

◯ **General-purpose v2 with LRS**

Explanation

General-purpose v2 storage accounts are recommended for most Azure Storage scenarios, including storing unstructured data like blobs and file shares. Locally redundant storage (LRS) ensures that data is replicated within the same region to provide high availability and durability for blobs and file shares.

◯ **Block Blob with GRS**

Explanation

Block Blob storage accounts are optimized for storing large amounts of unstructured data, typically used for media files, backups, and logs. However, geo-redundant storage (GRS) replicates data to a secondary region for disaster recovery, which may not be necessary for high-performance access within a single region.

◯ **General-purpose v1 with RA-GRS**

Explanation

General-purpose v1 storage accounts are an older version and may not offer the same features and performance optimizations as v2 accounts. Read-access geo-redundant storage (RA-GRS) replicates data to a secondary region for read access, which may not be necessary for storing unstructured data with high-performance access in a single region.

◯ **File Storage with ZRS**

Explanation

File Storage accounts are specifically designed for Azure File shares, providing fully managed file shares in the cloud. Zone-redundant storage (ZRS) replicates data across multiple availability zones within the same region for high availability, but it may not be the best fit for storing unstructured data with high-performance access.

Overall explanation

The best fit for storing unstructured data with high-performance access, supporting both blobs and file shares in a single region, is: **General-purpose v2 with LRS**

- **General-purpose v2 (GPv2)** storage accounts are the most flexible and cost-efficient option for storing unstructured data in Azure. They support both **Blob Storage** (for object storage) and **File Storage** (for SMB-based file shares), making them suitable for a variety of use cases, including the scenario described.

- **LRS (Locally Redundant Storage)** replicates the data within a single data center to protect against local hardware failures. Since the scenario specifies a single region (no cross-region replication needed), **LRS** is an ideal redundancy option for high-performance, cost-effective storage.

Why the other options are incorrect:

- **Block Blob with GRS**: While **Block Blob** is optimized for storing large amounts of unstructured data, this storage type is part of the **General-purpose v2** account type. **GRS (Geo-Redundant Storage)** replicates data across regions, which is more expensive and unnecessary in this case, as the requirement specifies a single region.

- **File Storage with ZRS**: **File Storage** is a specialized storage account type optimized for file shares (SMB protocol). While **ZRS (Zone-Redundant Storage)** provides resilience by replicating data across availability zones, this option does not support both blobs and file shares in a single account, which is required in the scenario.

- **General-purpose v1 with RA-GRS**: **General-purpose v1** accounts do not support the latest performance features available in **v2 accounts**, and **RA-GRS (Read-Access Geo-Redundant Storage)** replicates data across regions, which is not necessary for this single-region use case.

Domain

Describe Azure architecture and services (35–40%)

Question 35 Skipped

A(n) _____ in Azure Monitor monitors your telemetry and captures a signal to see if the signal meets the criteria of a preset condition. If the conditions are met, an alert is triggered, which initiates the associated action group.

- ○ **preset condition**

- preset rule
- alert condition

Correct answer

- alert rule

Overall explanation

From the Official Azure Documentation:

Alerts help you detect and address issues before users notice them by proactively notifying you when Azure Monitor data indicates that there may be a problem with your infrastructure or application.

You can alert on any metric or log data source in the Azure Monitor data platform.

An **alert rule** monitors your telemetry and captures a signal that indicates that something is happening on a specified target. The alert rule captures the signal and checks to see if the signal meets the criteria of the condition. If the conditions are met, an alert is triggered, which initiates the associated action group and updates the state of the alert.

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

Domain

Describe Azure management and governance (30–35%)

Question 36 Skipped

Which of the following is the **best use case** for **Platform-as-a-Service (PaaS)**?

○ **Deploying a pre-built CRM application to manage customer data**

Explanation

Deploying a pre-built CRM application to manage customer data is more aligned with Software-as-a-Service (SaaS) rather than Platform-as-a-Service (PaaS). In PaaS, the emphasis is on providing a platform for developers to build and deploy their own applications, rather than using pre-built applications.

Correct answer

○ **Deploying a web app where the developer focuses only on coding and not on managing servers**

Explanation

Deploying a web app where the developer focuses only on coding and not on managing servers is a perfect use case for Platform-as-a-Service (PaaS). PaaS allows developers to focus on writing code and building applications without the need to manage servers, infrastructure, or operating systems.

○ **Hosting a database where the admin manages the hardware and OS**

Explanation

Hosting a database where the admin manages the hardware and OS is closer to Infrastructure-as-a-Service (IaaS) rather than Platform-as-a-Service (PaaS). In PaaS, the focus is on providing a platform for developers to build and deploy applications, not on managing the underlying hardware and operating system.

○ **Hosting a virtual machine that runs a custom web application**

Explanation

Hosting a virtual machine that runs a custom web application falls more under the category of Infrastructure-as-a-Service (IaaS) rather than Platform-as-a-Service (PaaS). In PaaS, the focus is on providing a platform for developers to build, deploy, and manage applications without worrying about the underlying infrastructure.

Overall explanation

PaaS provides a platform for developers to build, deploy, and manage applications without worrying about the underlying infrastructure. It abstracts away hardware and OS management, making it ideal for applications where developers focus only on writing code.

Domain

Describe cloud concepts (25–30%)

Question 37 Skipped

Which of the following is NOT a benefit of using Azure Arc?

○ **Consistent management of resources across hybrid environments**

Explanation

Azure Arc provides consistent management of resources across hybrid environments by extending Azure management capabilities to on-premises, multi-cloud, and edge environments. It allows organizations to manage resources in a unified way regardless of their location.

Correct answer

○ **Centralized billing and cost management for all resources**

Explanation

Centralized billing and cost management for all resources is not a benefit of using Azure Arc. Azure Arc focuses on resource management and governance rather than billing and cost management. Organizations would still need to use Azure Cost Management or other tools for centralized billing and cost management.

○ **Increased visibility and control over resources**

Explanation

Azure Arc provides increased visibility and control over resources by allowing organizations to centrally manage and govern resources across different environments. It enables consistent monitoring, policy enforcement, and configuration management for resources, improving overall visibility and control.

◯ **Improved security and compliance for resources**

Explanation

Azure Arc helps improve security and compliance for resources by enabling organizations to apply Azure security policies, role-based access control, and compliance standards to resources outside of Azure. This ensures that all resources meet the necessary security and compliance requirements.

Overall explanation

Azure Arc is a hybrid management service that allows you to manage your servers, Kubernetes clusters, and applications across on-premises, multi-cloud, and edge environments. Some of the benefits of using Azure Arc include consistent management of resources across hybrid environments, improved security and compliance for resources, and increased visibility and control over resources.

Centralized billing and cost management for all resources: Thus is not a benefit of using Azure Arc. While Azure provides centralized billing and cost management for resources in the cloud, Azure Arc is focused on managing resources across hybrid environments and does not provide billing or cost management features.

Other options -

- **Consistent management of resources across hybrid environments**: This is a key benefit of using Azure Arc. With Azure Arc, you can apply policies, monitor and manage resources, and automate tasks across all of your environments, including on-premises, multi-cloud, and edge environments.

- **Improved security and compliance for resources:** This is another benefit of using Azure Arc. Azure Arc allows you to apply security and compliance policies to resources across all of your environments, providing consistent protection against threats and helping you maintain regulatory compliance.

- **Increased visibility and control over resources:** This is also a benefit of using Azure Arc. With Azure Arc, you can gain a unified view of all your resources across hybrid environments, and apply policies, automate tasks, and monitor resources from a single location. This provides greater control and visibility over your entire IT estate.

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

Domain

Describe Azure management and governance (30–35%)

Question 38 Skipped

Yes or No:

Each virtual network can have only one VPN gateway.

Correct answer

- ◯ **Yes**

- ◯ **No**

Overall explanation

From the Official Azure Documentation:

VPN Gateway sends encrypted traffic between an Azure virtual network and an on-premises location over the public Internet. You can also use VPN Gateway to send encrypted traffic between Azure virtual networks over the Microsoft network. A VPN gateway is a specific type of virtual network gateway. Each virtual network can have only one VPN gateway. However, you can create multiple connections to the same VPN gateway. When you create multiple connections to the same VPN gateway, all VPN tunnels share the available gateway bandwidth.

What is a VPN gateway?

When you configure a virtual network gateway, you configure a setting that specifies the gateway type. The gateway type determines how the virtual network gateway will be used and the actions that the gateway takes. The gateway type 'Vpn' specifies that the type of virtual network gateway created is a 'VPN gateway'. This distinguishes it from an ExpressRoute gateway, which uses a different gateway type. A virtual network can have two virtual network gateways; one VPN gateway and one ExpressRoute gateway. For more information, see Gateway types.

Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

Domain

Describe Azure architecture and services (35–40%)

Question 39 Skipped

Which of the following can help you automate deployments and use the practice of infrastructure as code?

○ **Mangement Groups**

Explanation

Management Groups in Azure are used to organize and manage access, policies, and compliance across multiple Azure subscriptions. While they are useful for governance and management purposes, they are not directly related to automating deployments or implementing infrastructure as code.

Correct answer

○ **ARM Templates**

Explanation

ARM Templates are used in Azure to define the infrastructure and configuration of Azure resources in a declarative format. They allow you to automate deployments by specifying the

desired state of the Azure resources, making them a key tool for implementing infrastructure as code practices.

○ **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 it provides centralized management capabilities, it is not specifically designed for automating deployments or implementing infrastructure as code.

○ **Azure IaaC**

Explanation

Azure IaaC (Infrastructure as Code) is not a specific tool or service in Azure. It seems to be a typo or a misinterpretation of the concept of infrastructure as code. The correct term for automating deployments using infrastructure as code in Azure is ARM Templates.

Overall explanation

From the Official Azure Documentation:

With the move to the cloud, many teams have adopted agile development methods. These teams iterate quickly. They need to repeatedly deploy their solutions to the cloud, and know their infrastructure is in a reliable state. As infrastructure has become part of the iterative process, the division between operations and development has disappeared. Teams need to manage infrastructure and application code through a unified process.

To meet these challenges, you can automate deployments and use the practice of infrastructure as code. In code, you define the infrastructure that needs to be deployed. The infrastructure code becomes part of your project. Just like application code, you store the infrastructure code in a source repository and version it. Any one on your team can run the code and deploy similar environments.

To implement infrastructure as code for your Azure solutions, use **Azure Resource Manager templates (ARM templates).** The template is a JavaScript Object Notation (JSON) file that

defines the infrastructure and configuration for your project. The template uses declarative syntax, which lets you state what you intend to deploy without having to write the sequence of programming commands to create it. In the template, you specify the resources to deploy and the properties for those resources.

Reference: https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/overview

Domain

Describe Azure management and governance (30–35%)

Question 40 Skipped

Which of the following resources can be managed using Azure Arc?

- Kubernetes clusters
- Only Kubernetes Clusters and Virtual Machines

Correct answer

- **All of these**

- Only Windows and Linux Servers & Virtual Machines
- Virtual machines
- Windows Server and Linux servers

Overall explanation

The answer is All of the these. Azure Arc enables you to manage resources both on-premises and across multiple clouds using a single control plane. This includes managing Windows Server and Linux servers, Kubernetes clusters, and virtual machines. By extending Azure services to hybrid environments, Azure Arc provides consistent management, security, and compliance across all resources.

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

Domain

Describe Azure management and governance (30–35%)

Question 41 Skipped

A government agency requires Azure services in a dedicated region operated by screened personnel to meet strict compliance needs, separate from standard public regions. Which type of Azure region supports this?

○ Region Pair

Explanation

Region Pair refers to a pair of Azure regions within the same geography, designed for data residency and business continuity. It does not specifically cater to the needs of a government agency requiring a dedicated region for compliance purposes operated by screened personnel.

Correct answer

○ Sovereign Region

Explanation

Sovereign Region is a type of Azure region specifically designed to meet the strict compliance needs of government agencies, separate from standard public regions. It is operated by screened personnel to ensure data sovereignty and compliance with regulations.

◯ **Availability Zone**

Explanation

Availability Zone is a physically separate data center within an Azure region, designed to provide high availability and resiliency for applications and services. While important for redundancy and fault tolerance, it does not address the specific compliance needs of a government agency requiring a dedicated region.

◯ **Standard Region**

Explanation

Standard Region refers to a regular Azure region available to all customers, including government agencies. It does not offer the level of compliance and data sovereignty required by a government agency with strict compliance needs.

Overall explanation

A **Sovereign Region** in Azure is designed specifically for organizations with stringent regulatory, compliance, and data residency requirements, such as government agencies or organizations in highly regulated industries. These regions are operated by screened personnel and offer isolation from standard public Azure regions.

- **Sovereign Regions** are typically operated in a manner that meets strict compliance standards and provide the ability to store data in a specific country or jurisdiction.
- Examples of Azure Sovereign Regions include **Azure Government** in the United States, **Azure China** (operated by 21Vianet), and **Azure Germany** (operated by a trusted partner under data control agreements).

Why the other options are incorrect:

- **Region Pair**: This refers to a set of two Azure regions within the same geography that are paired together for disaster recovery purposes. It doesn't meet the requirement for dedicated, isolated regions with strict compliance needs.

- **Availability Zone**: Availability Zones are physical data centers within an Azure region designed to provide high availability and fault tolerance. It doesn't offer the isolation and compliance required by a government agency.

- **Standard Region**: This is a typical Azure region available for general use, and it does not offer the dedicated compliance and security features needed for government agencies or highly regulated environments.

Domain

Describe Azure architecture and services (35–40%)

Question 42 Skipped

A _____ endpoint is a network interface that uses a private IP address from your virtual network.

- ○ Internal
- ○ Hybrid

Correct answer

- ◯ **Private**

Explanation

A Private endpoint is a network interface that uses a private IP address from your virtual network. It allows you to connect privately to Azure services without using public IP addresses.

- ○ Public

Explanation

Public endpoints use public IP addresses to communicate with services over the internet. They are not associated with private IP addresses from your virtual network.

Overall explanation

From the Official Azure Documentation:

A private endpoint is a network interface that uses a private IP address from your virtual network. This network interface connects you privately and securely to a service that's powered by Azure Private Link. By enabling a private endpoint, you're bringing the service into your virtual network.

The service could be an Azure service such as:

- Azure Storage
- Azure Cosmos DB
- Azure SQL Database
- Your own service, using Private Link service.

Reference: https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-overview

Domain

Describe Azure architecture and services (35–40%)

Question 43 Skipped

What is the primary purpose of external identities in Microsoft Entra ID?

Correct answer

- ○ **To allow external partners and customers to access resources in your Azure environment.**
- ○ **To enable single sign-on between Azure subscriptions.**

- ○ **To manage user identities exclusively for on-premises applications.**
- ○ **To provide secure access to Azure resources for employees within the organization.**

Overall explanation

External identities in Entra ID enable organizations to extend their identity management beyond their own employees. This allows external partners, vendors, and customers to access specific resources within the organization's Azure environment without requiring them to have internal accounts.

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

Domain

Describe Azure architecture and services (35–40%)

Question 44 Skipped

Which of the following best describes Azure Arc?

- ○ **A service for analyzing and visualizing large datasets in the cloud**

Explanation

Azure Arc is not a service for analyzing and visualizing large datasets in the cloud. It focuses on extending Azure management capabilities to hybrid and multi-cloud environments, rather than data analysis and visualization.

Correct answer

- ○ **A bridge that extends the Azure platform to help you build apps with the flexibility to run across datacenters**

Explanation

This is the correct choice. Azure Arc is a bridge that extends the Azure platform to help you build apps with the flexibility to run across datacenters. It allows you to manage and govern resources such as virtual machines, Kubernetes clusters, and databases wherever they are located.

○ **A platform for building microservices-based applications that run across multiple nodes**

Explanation

Azure Arc is not a platform for building microservices-based applications that run across multiple nodes. It is a management solution that enables organizations to manage resources and applications across different environments.

○ **A cloud-based identity and access management service**

Explanation

Azure Arc is not a cloud-based identity and access management service. It is a solution that extends Azure services and management to any infrastructure, including on-premises, multi-cloud, and edge environments.

Overall explanation

Azure Arc is a service from Microsoft that allows organizations to manage and govern their on-premises servers, Kubernetes clusters, and applications using Azure management tools and services. With Azure Arc, customers can use Azure services such as Azure Policy, Azure Security Center, and Azure Monitor to manage their resources across on-premises, multi-cloud, and edge environments. Azure Arc also enables customers to deploy and manage Azure services on-premises or on other clouds using the same tools and APIs as they use in Azure.

From the official 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.

Other Options -

- **A cloud-based identity and access management service** is incorrect because Azure Arc is not an identity and access management service. Azure Active Directory is a service from Microsoft that provides identity and access management capabilities for cloud applications and resources.

- **A platform for building microservices-based applications that run across multiple nodes** is incorrect because Azure Arc is not a platform for building microservices-based applications. Azure Kubernetes Service (AKS) is a service from Microsoft that provides managed Kubernetes clusters for deploying and managing containerized applications.

- **A service for analyzing and visualizing large datasets in the cloud** is incorrect because Azure Arc is not a service for analyzing and visualizing large datasets in the cloud. Azure Synapse Analytics is a service from Microsoft that provides analytics and data warehousing capabilities for big data and data integration scenarios.

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

Domain

Describe Azure management and governance (30–35%)

Question 45 Skipped

Which of the following is a **benefit** of **security and governance** in the cloud?

○ **Full control over physical security and on-premises infrastructure**

Explanation

Full control over physical security and on-premises infrastructure is not a benefit of security and governance in the cloud. Cloud providers are responsible for the physical security of the data centers where the cloud services are hosted, not the users.

Correct answer

◯ **Enhanced ability to monitor and enforce policies for data access and compliance**

Explanation

Enhanced ability to monitor and enforce policies for data access and compliance is a key benefit of security and governance in the cloud. Cloud platforms offer robust tools and services that allow organizations to set and enforce security policies, monitor data access, and ensure compliance with regulations.

◯ **No need for encryption since cloud providers handle security automatically**

Explanation

No need for encryption since cloud providers handle security automatically is not a valid statement. Encryption is still essential in the cloud to protect data at rest and in transit, even though cloud providers offer security features. Encryption adds an extra layer of protection and ensures data confidentiality. Users are responsible for enabling and configuring encryption, CSP doesn't handle all security automatically.

◯ **Ability to prevent all external threats using only firewalls**

Explanation

The ability to prevent all external threats using only firewalls is not a realistic expectation in cloud security. While firewalls are an important component of a security strategy, they are not sufficient on their own to protect against all external threats. A comprehensive security approach in the cloud involves multiple layers of defense.

Overall explanation

Cloud providers offer tools for **security and governance** to help organizations monitor and enforce access control, compliance, and data protection policies. This makes it easier to implement consistent governance across cloud resources.

Domain

Describe cloud concepts (25–30%)

Question 46 Skipped

_____ lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider.

○ **Azure Firewall**

Explanation

Azure Firewall is a cloud-based network security service that helps protect your Azure Virtual Network resources. While it provides network security features, it does not specifically enable the extension of on-premises networks into the Microsoft cloud over a private connection.

○ **Azure Virtual Network**

Explanation

Azure Virtual Network enables you to create isolated networks in the Azure cloud, allowing you to securely connect Azure resources. While it is essential for network segmentation and connectivity within Azure, it does not directly facilitate extending on-premises networks into the Microsoft cloud over a private connection.

○ **Azure Sentinel**

Explanation

Azure Sentinel is a cloud-native security information and event management (SIEM) service that provides intelligent security analytics for threat detection and response. While it enhances security in Azure environments, it does not directly enable the extension of on-premises networks into the Microsoft cloud over a private connection.

○ **Azure DNS**

Explanation

Azure DNS is a hosting service for DNS domains, providing name resolution using the Azure infrastructure. While DNS is crucial for network connectivity, it does not specifically enable the extension of on-premises networks into the Microsoft cloud over a private connection.

Correct answer

◯ **Azure ExpressRoute**

Explanation

Azure ExpressRoute allows you to establish a private connection between your on-premises network and Microsoft Azure cloud services. This private connection is facilitated through a connectivity provider, enabling you to extend your network into the cloud securely and with high bandwidth.

Overall explanation

From the Official Azure Documentation:

ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.

Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility. ExpressRoute connections don't go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet. For information on how to connect your network to Microsoft using ExpressRoute, see ExpressRoute connectivity models.

Reference: https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction?toc=%2Fazure%2Fvirtual-network%2Ftoc.json

Domain

Describe Azure architecture and services (35–40%)

Question 47 Skipped

Someone in your organization accidentally deleted an important Virtual Machine that has led to huge revenue losses. Your senior management has tasked you with investigating who was responsible for the deletion. Which Azure service can you leverage for this task?

○ **Azure Arc**

Explanation

Azure Arc is a service that extends Azure management and services to any infrastructure. It is used for managing resources across on-premises, multi-cloud, and edge environments. However, it is not specifically designed for investigating actions like the accidental deletion of a Virtual Machine in Azure.

○ **Azure Service Health**

Explanation

Azure Service Health provides personalized guidance and support when issues with Azure services affect you. While it can provide information on service incidents and outages, it is not the ideal tool for investigating specific actions like the deletion of a Virtual Machine.

Correct answer

○ **Azure Monitor**

Explanation

Azure Monitor is the correct choice for investigating the deletion of the Virtual Machine. Azure Monitor provides a comprehensive solution for collecting, analyzing, and acting on telemetry data from Azure resources. It includes features like activity logs, which can help you track who performed the deletion.

○ **Azure Advisor**

Explanation

Azure Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It provides recommendations for improving the security,

performance, and reliability of your resources, but it does not track or investigate specific actions like resource deletions.

◯ **Azure Event Hubs**

Explanation

Azure Event Hubs is a big data streaming platform and event ingestion service, which is used for collecting, transforming, and storing events. It is not specifically designed for tracking and investigating actions related to resource deletions in Azure.

Overall explanation

From the Official Azure Documentation:

Log Analytics is a tool in the Azure portal that's used to edit and run log queries with data in **Azure Monitor (Correct)** Logs.

You might write a simple query that returns a set of records and then use features of Log Analytics to sort, filter, and analyze them. Or you might write a more advanced query to perform statistical analysis and visualize the results in a chart to identify a particular trend.

Whether you work with the results of your queries interactively or use them with other Azure Monitor features, such as log query alerts or workbooks, Log Analytics is the tool that you'll use to write and test them.

Azure Advisor (incorrect) analyzes your configurations and usage telemetry and offers personalized, actionable recommendations to help you optimize your Azure resources for reliability, security, operational excellence, performance, and cost.

Azure Service Health (incorrect) helps you stay informed and take action, with alerts for outages and a personalised dashboard for service issues.

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview

Domain

Describe Azure management and governance (30–35%)

Question 48 Skipped

_____ is a unified cloud-native application protection platform that helps strengthen your security posture, enables protection against modern threats, and helps reduce risk throughout the cloud application lifecycle across multicloud and hybrid environments.

○ **Azure Bastion**

Explanation

Azure Bastion is a service that provides secure and seamless RDP and SSH access to Azure virtual machines. While it enhances network security for accessing VMs, it is not a unified cloud-native application protection platform like Microsoft Defender for Cloud.

○ **Azure Network Security Group**

Explanation

Azure Network Security Group is a basic firewall service that filters network traffic to and from Azure resources. It is not a comprehensive application protection platform like Microsoft Defender for Cloud, which offers advanced security features and threat protection.

Correct answer

○ **Microsoft Defender for Cloud**

Explanation

Microsoft Defender for Cloud is a comprehensive cloud-native application protection platform that offers advanced security features to enhance your security posture. It helps protect against modern threats, reduces risks, and ensures security throughout the cloud application lifecycle in multicloud and hybrid environments.

○ **Azure Firewall**

Explanation

Azure Firewall is a network security service that helps protect your Azure Virtual Network resources. While it provides network-level protection, it is not specifically designed as a unified cloud-native application protection platform like Microsoft Defender for Cloud.

○ **Microsoft Priva**

Explanation

Microsoft Priva is not a known service or platform in the Microsoft Azure ecosystem. It does not provide application protection or security features like Microsoft Defender for Cloud.

Overall explanation

From the official documentation: Microsoft Defender for Cloud is a unified cloud-native application protection platform that helps strengthen your security posture, enables protection against modern threats, and helps reduce risk throughout the cloud application lifecycle across multicloud and hybrid environments.

Reference: https://azure.microsoft.com/en-us/products/defender-for-cloud/

Domain

Describe Azure architecture and services (35–40%)

Question 49 Skipped

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

A company segments its Azure virtual network into a __ for app servers and connects it to another VNet in a different subscription using __ to enable secure communication.

(Both blanks accept ONE word only)

Correct answer

subnet, peering

Explanation

A company segments its Azure virtual network into a **subnet** for app servers and connects it to another VNet in a different subscription using **peering** to enable secure communication.

- **Subnet**: A subnet is a segment of a virtual network (VNet) in Azure that allows you to organize and manage network resources such as virtual machines (VMs), network interfaces, and other Azure resources within specific IP address ranges. By segmenting the VNet into subnets, you can control the flow of traffic and apply specific network security policies to different parts of the network.
- **Peering**: VNet peering is a feature that connects two virtual networks (VNets) in Azure, enabling them to communicate with each other securely. The communication is established using private IP addresses, and once peered, the VNets can communicate as if they are part of the same network, even if they exist in different subscriptions or regions. It provides low-latency and high-bandwidth communication between the VNets.

Domain

Describe Azure architecture and services (35–40%)

Question 50 Skipped

A firm adopts a security model in Azure that trusts users and devices within the corporate network by default, only requiring verification for external access requests. Does this align with the Zero Trust concept?

○ Yes

Correct answer

○ **No**

Explanation

No, this security model does not align with the Zero Trust concept. The Zero Trust model advocates for continuous verification and authentication of all users and devices, regardless of their location or network. By only requiring verification for external access requests, the firm is not following the principles of Zero Trust, which emphasize a least-privileged access approach and continuous monitoring for potential threats.

Overall explanation

The **Zero Trust** security model operates on the principle of **"never trust, always verify"**. This means that no user, device, or network is trusted by default, whether inside or outside the organization. Every access request is continuously verified regardless of where it originates.

In the scenario described, the firm **trusts users and devices within the corporate network by default**, which goes against the Zero Trust model. In Zero Trust, trust should not be granted based on location (inside or outside the network), and verification is required for every access request, regardless of the source.

Therefore, the model described does **not** align with the **Zero Trust** concept.

Domain

Describe Azure architecture and services (35–40%)

Question 51 Skipped

Which of the following can help you manage multiple Azure Subscriptions?

○ **Blueprints**

Explanation

Blueprints in Azure allow you to define a repeatable set of resources that adhere to organizational standards, patterns, and requirements. While blueprints help you automate the

deployment of resources, they are not specifically designed to manage multiple Azure Subscriptions.

Correct answer

◯ **Management Groups**

Explanation

Management Groups are containers that help you manage access, policy, and compliance across multiple Azure Subscriptions. They provide a way to efficiently manage access, policies, and compliance for all subscriptions within the management group.

◯ **Policies**

Explanation

Policies in Azure allow you to enforce rules and actions on resources to ensure compliance with your corporate standards and service level agreements. While policies are important for governance and compliance, they do not directly help you manage multiple Azure Subscriptions.

◯ **Resource Groups**

Explanation

Resource Groups are containers that hold related resources for an Azure solution. While they help you organize and manage resources within a subscription, they do not specifically help you manage multiple Azure Subscriptions.

Overall explanation

From the Official Azure Documentation:

If you have only a few subscriptions, it's fairly easy to manage them independently. But what if you have many subscriptions? Then you can create a management group hierarchy to help manage your subscriptions and resources.

For your subscriptions, Azure management groups help you efficiently manage:

- Access
- Policies
- Compliance

Each management group contains one or more subscriptions.

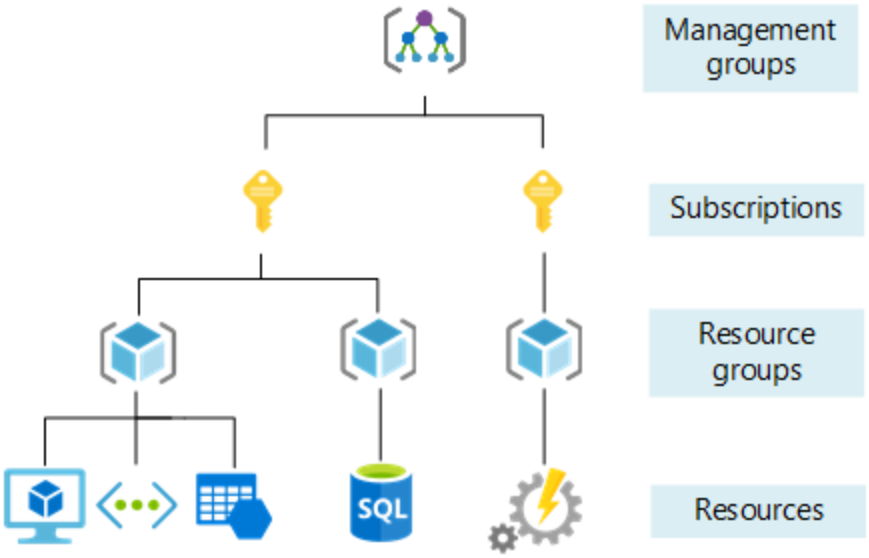
Azure arranges management groups in a single hierarchy. You define this hierarchy in your Azure Active Directory (Azure AD) tenant to align with your organization's structure and needs. The top level is called the *root management group*. You can define up to six levels of management groups in your hierarchy. Only one management group contains a subscription.

Azure provides four levels of management scope:

- Management groups
- Subscriptions
- Resource groups
- Resources

If you apply any access or policy at one level in the **hierarchy**, it propagates down to the lower levels. A resource owner or subscription owner can't alter an inherited policy. This limitation helps improve governance.

This inheritance model lets you arrange the subscriptions in your hierarchy, so each subscription follows appropriate policies and security controls.



Reference: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/organize-subscriptions

Domain

Describe Azure management and governance (30–35%)

Question 52 Skipped

True or False:

When you cancel an Azure subscription, a Resource Lock can block the subscription cancellation.

- ○ True

Correct answer

- ○ False

Overall explanation

From the Official Azure Documentation:

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**. In the left navigation panel, the subscription lock feature's name is **Resource locks**, while the resource group lock feature's name is **Locks**.

If you have a **Delete** lock on a resource and attempt to delete its resource group, the feature blocks the whole delete operation. Even if the resource group or other resources in the resource group are unlocked, the deletion doesn't happen. You never have a partial deletion.

When you cancel an Azure subscription:

- A resource lock doesn't block the subscription cancellation.
- Azure preserves your resources by deactivating them instead of immediately deleting them.
- Azure only deletes your resources permanently after a waiting period.

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

Domain

Describe Azure management and governance (30–35%)

Question 53 Skipped

You want to ensure that all virtual machines deployed in your Azure environment are configured with specific antivirus software. Which Azure service can you use to enforce this policy?

○ **Azure Advisor**

Explanation

Azure Advisor provides recommendations for optimizing your Azure resources based on best practices, cost efficiency, performance, and security. While it can offer guidance on security-related matters, it does not have the capability to enforce specific antivirus software configurations on virtual machines.

○ **Azure Monitor**

Explanation

Azure Monitor is a service for collecting, analyzing, and acting on telemetry data from your Azure resources. While it can provide insights into the performance and health of your virtual machines, it does not have the functionality to enforce specific antivirus software configurations on them.

◯ **Azure Security Center**

Explanation

Azure Security Center is focused on providing security management and threat protection for your Azure resources. While it can help identify security vulnerabilities and recommend solutions, it does not have the direct capability to enforce the installation of specific antivirus software on virtual machines.

Correct answer

◯ **Azure Policy**

Explanation

Azure Policy is the correct choice as it allows you to enforce specific configurations and settings across all resources in your Azure environment. By creating a policy that mandates the presence of specific antivirus software on virtual machines, you can ensure compliance and consistency across your deployments.

Overall explanation

The correct option is Azure Policy. Azure Policy is the service that allows you to enforce organizational standards and compliance across all your resources in Azure. With Azure Policy, you can create policies that enforce specific configurations and settings for resources, including virtual machines, at the time of deployment or during their lifecycle. In this scenario, you can create a policy that enforces the installation of specific antivirus software on all virtual machines, ensuring that all resources in your environment are compliant with your organization's security requirements.

Azure Advisor provides recommendations to optimize your resources, Azure Security Center helps to identify and remediate potential security threats, and Azure Monitor provides insights into the performance and health of your applications and resources. While these services are useful for monitoring and optimizing your environment, they do not enforce specific policies or configurations on your resources.

Other Options :

Azure Advisor: This service provides recommendations to optimize Azure resources based on best practices, but it does not have the capability to enforce policies.

Azure Security Center: This service focuses on security and threat protection for Azure resources. It provides recommendations to improve security posture and allows for continuous monitoring and alerting of security-related events, but it does not enforce policies related to antivirus software.

Azure Monitor: This service provides real-time monitoring and alerting for Azure resources, but it does not have the capability to enforce policies.

Reference: https://learn.microsoft.com/en-us/azure/governance/policy/overview#azure-policy-objects

Domain

Describe Azure management and governance (30–35%)

Question 54 Skipped

_____ is a strategy that employs a series of mechanisms to slow the advance of an attack that's aimed at acquiring unauthorized access to information. Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure.

Correct answer

◯ **Defense in Depth**

Explanation

Defense in Depth is a cybersecurity strategy that involves implementing multiple layers of security controls to protect against potential threats. Each layer adds an additional level of protection, making it more difficult for attackers to penetrate the system. This approach ensures that if one layer is compromised, there are other layers in place to prevent further unauthorized access.

◯ **Defense in Steps**

○ **Defense in Series**

Explanation

Defense in Series is not a commonly used term in cybersecurity and does not accurately describe the concept of employing multiple layers of security controls to slow down and prevent unauthorized access. Unlike Defense in Depth, this term does not convey the idea of having multiple layers of defense working in parallel to enhance security.

○ **Defense in Layers**

Overall explanation

From the Official Azure Documentation:

Defense in depth is a strategy that employs a series of mechanisms to slow the advance of an attack that's aimed at acquiring unauthorized access to information. Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure.

Microsoft applies a layered approach to security, both in its physical datacenters and across Azure services. The objective of defense in depth is to protect information and prevent it from being stolen by individuals who aren't authorized to access it

Reference: https://docs.microsoft.com/en-us/learn/modules/azure-well-architected-security/2-defense-in-depth

Domain

Describe Azure architecture and services (35–40%)

Question 55 Skipped

Which of the following protocols is used for federated authentication in Entra ID?

- ○ OpenID Connect
- ○ LDAP
- ○ OAuth 2.0

Correct answer

- ◯ SAML

Overall explanation

SAML (Security Assertion Markup Language) is the protocol used for federated authentication in Entra ID.

Federated authentication is a mechanism that allows users to use their existing credentials from a trusted identity provider (IdP) to authenticate with another application or service. In the context of Azure AD, federated authentication allows users to use their existing corporate credentials to authenticate with cloud-based applications and services.

Azure AD supports several federated authentication protocols, including Security Assertion Markup Language (SAML), OAuth 2.0, and OpenID Connect. SAML is widely used for federated authentication in enterprise environments, while OAuth 2.0 and OpenID Connect are commonly used in web and mobile applications.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/single-sign-on-saml-protocol

Domain

Describe Azure architecture and services (35–40%)

Question 56 Skipped

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

An organization enhances security in Azure by allowing users to sign in using a mobile authenticator app instead of passwords, leveraging Microsoft Entra ID's __ authentication method.

Correct answer

passwordless

Explanation

The correct answer is **"passwordless"** authentication method.

Full sentence: An organization enhances security in Azure by allowing users to sign in using a mobile authenticator app instead of passwords, leveraging Microsoft Entra ID's **passwordless** authentication method.

Microsoft Entra ID (formerly Azure AD) offers several **passwordless authentication** methods to enhance security and improve user experience. One such method allows users to sign in using a mobile authenticator app (such as **Microsoft Authenticator**) instead of traditional passwords. This method can help reduce the risk of password-based attacks, such as phishing and credential stuffing.

Passwordless authentication typically uses one of these methods:

- **Microsoft Authenticator app** (with push notifications)
- **Windows Hello** (biometric or PIN-based authentication)
- **FIDO2 security keys**

These methods increase security and streamline user access by eliminating the need for passwords.

Domain

Describe Azure architecture and services (35–40%)

Question 57 Skipped

In the **shared responsibility model** of cloud security, which of the following is **the responsibility of the cloud provider**?

Correct answer

◯ **Ensuring physical security of data centers**

Explanation

Ensuring the physical security of data centers is a key responsibility of the cloud provider in the shared responsibility model. This includes implementing measures such as access controls, surveillance systems, and environmental controls to protect the physical infrastructure where customer data is stored.

◯ **Configuring firewall settings for user applications**

Explanation

Configuring firewall settings for user applications is generally the responsibility of the cloud customer in the shared responsibility model. While the cloud provider may offer firewall services as part of their platform, it is up to the customer to configure and manage these settings to secure their applications.

◯ **Encrypting application-level data before sending it to the cloud**

Explanation

Encrypting application-level data before sending it to the cloud is typically the responsibility of the cloud customer in the shared responsibility model. While the cloud provider may offer encryption services, it is the customer's responsibility to implement encryption for their data before it is transmitted to the cloud.

◯ **Managing user authentication and access permissions**

Explanation

Managing user authentication and access permissions is typically the responsibility of the cloud customer in the shared responsibility model. The cloud provider may offer tools and

services to assist with this task, but ultimately, the customer is responsible for managing user access to their resources.

Overall explanation

In the **shared responsibility model**, the cloud provider is responsible for the physical security of the infrastructure (e.g., data centers), while the customer is responsible for configuring and securing their applications, data, and access controls.

Domain

Describe cloud concepts (25–30%)

Question 58 Skipped

Which of the following provides support for key migration workloads like Windows, SQL and Linux Server, databases, data, web apps, and virtual desktops?

○ **Azure Suggestions**

Explanation

Not a valid service.

○ **Azure Advisor**

Explanation

Azure Advisor is a service that provides best practices and recommendations for optimizing Azure resources, but it does not specifically focus on key migration workloads like Windows, SQL and Linux Server, databases, data, web apps, and virtual desktops.

Correct answer

○ **Azure Migrate**

Explanation

Azure Migrate is the correct choice as it is a service specifically designed to support key migration workloads like Windows, SQL and Linux Server, databases, data, web apps, and virtual desktops. It helps organizations assess their on-premises environment, migrate workloads to Azure, and optimize resources for the cloud.

○ **Azure Recommendations**

Explanation

Not a valid service.

Overall explanation

From the Official Azure Documentation:

Azure Migrate provides all the Azure migration tools and guidance you need to plan and implement your move to the cloud—and track your progress using a central dashboard that provides intelligent insights.

Multiple scenarios

Use a comprehensive approach to migrating your application and datacenter estate. Get support for key migration workloads like Windows, SQL and Linux Server, databases, data, web apps, and virtual desktops. Migrate to destinations including Azure Virtual Machines, Azure VMware Solution, Azure App Service, and Azure SQL Database. Migrations are holistic across VMware, Hyper-V, physical server, and cloud-to-cloud migration.

Reference: https://azure.microsoft.com/en-us/services/azure-migrate/#features

Domain

Describe Azure architecture and services (35–40%)

Question 59 Skipped

Your company has decided to migrate its on-premises virtual machines to Azure. Which Azure Virtual Machines feature allows you to migrate virtual machines without downtime?

- ○ Azure Spot Virtual Machines

Correct answer

- ◯ **Azure Site Recovery**

- ○ Azure Reserved Virtual Machines

- ○ Azure Virtual Machine Scale Sets

Overall explanation

The correct answer is Azure Site Recovery.

Azure Site Recovery (ASR) is a service offered by Azure that enables replication of virtual machines from on-premises environments to Azure or between Azure regions with little or no downtime. This allows for the migration of virtual machines to Azure without any disruption to business operations. After replication to Azure, the virtual machines can be launched and used as if they were in the on-premises environment.

Other Options :

Azure Reserved Virtual Machines: This is a purchasing option for Azure virtual machines where compute capacity can be reserved for one or three years at a lower cost than pay-as-you-go pricing. This option is not related to virtual machine migration.

Azure Spot Virtual Machines: This is a purchasing option for Azure virtual machines that allows the use of unused capacity in Azure data centers at a significant discount compared to pay-as-you-go pricing. This option is not related to virtual machine migration.

Azure Virtual Machine Scale Sets: This is a service that allows the creation and management of a group of identical virtual machines in Azure, designed to horizontally scale applications to meet increased demand. Although this service can be used in combination with virtual machine migration, it does not provide a solution for migrating virtual machines without downtime.

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

Question 60 Skipped

Your organization uses Microsoft Defender for Cloud and you receive an alert that suspicious activity has been detected on one of your cloud resources. What should you do?

Correct answer

- ○ **Investigate the alert and take appropriate action to remediate the threat if necessary.**

Explanation

Investigating the alert and taking appropriate action to remediate the threat if necessary is the correct course of action. It is important to address any suspicious activity detected by Microsoft Defender for Cloud to prevent potential security breaches.

- ○ **Delete the cloud resource to prevent the threat from spreading.**

Explanation

Deleting the cloud resource to prevent the threat from spreading is an extreme and unnecessary measure. It is important to investigate the alert first and take appropriate actions to remediate the threat without resorting to deleting the resource.

- ○ **Wait for a follow-up email from Microsoft Support before taking any action.**

- ○ **Ignore the alert, as Microsoft Defender for Cloud will automatically handle any threats.**

Explanation

Ignoring the alert and assuming that Microsoft Defender for Cloud will automatically handle any threats is not a recommended approach. It is essential to investigate the alert and take appropriate action to ensure the security of your cloud resources.

Overall explanation

The correct answer is - Investigate the alert and take appropriate action to remediate the threat if necessary.

Microsoft Defender for Cloud can detect and alert you to potential threats to your cloud resources, **but it is up to you to investigate the alert and take appropriate action to remediate the threat.** Ignoring the alert or waiting for a follow-up email from Microsoft Support can leave your organization vulnerable to attack. Deleting the cloud resource may not necessarily eliminate the threat, and could cause other issues such as data loss.

Reference: https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

Domain

Describe Azure architecture and services (35–40%)

Question 61 Skipped

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

A government agency opts for a __ cloud to isolate sensitive data on its own infrastructure, while a media company uses a __ cloud for cost-effective streaming with global reach.

Correct answer

private, public

Explanation

- **Private cloud**: The **government agency** opts for a private cloud to ensure that **sensitive data** is isolated and stored on its own infrastructure. This cloud model provides full control over security, compliance, and customization, which is ideal for handling sensitive government data.

- **Public cloud**: The **media company** uses a public cloud for **streaming** because it offers **cost-effective** scalability with global reach. Public clouds like Azure or AWS provide vast infrastructure and services that allow businesses to scale their resources dynamically and reach a global audience without heavy upfront investments.

Domain

Describe cloud concepts (25–30%)

Question 62 Skipped

What is the primary purpose of a public endpoint in Azure?

○ **To enforce access control policies for resource groups.**

Explanation

Public endpoints do not enforce access control policies for resource groups. They are more focused on enabling external connectivity to Azure services, rather than managing access control within resource groups.

○ **To prevent communication between virtual networks.**

Explanation

Public endpoints are not designed to prevent communication between virtual networks. They are specifically used to enable external access to Azure services, rather than internal network communication.

Correct answer

○ **To provide a direct and secure connection to Azure services.**

Explanation

The primary purpose of a public endpoint in Azure is to provide a direct and secure connection to Azure services. This allows external users or applications to access Azure resources securely over the internet.

○ **To restrict incoming network traffic to specific IP ranges.**

Explanation

Public endpoints in Azure are not primarily used to restrict incoming network traffic to specific IP ranges. They are more focused on providing connectivity to Azure services from external sources.

Overall explanation

A **public** endpoint in Azure allows resources to be accessed over the public internet. It's used to expose services to clients or users who are not within the same network as the resource. Public endpoints are commonly used for services that need to be accessed from anywhere, such as web applications.

Reference: https://learn.microsoft.com/en-us/azure/storage/files/storage-files-networking-endpoints

Domain

Describe Azure architecture and services (35–40%)

Question 63 Skipped

In Azure, which of the following services can be accessed through private endpoints?

○ **Azure SQL Database.**

Correct answer

All of these.

Azure Storage accounts.

Azure App Service.

Azure Key Vault.

Overall explanation

Private endpoints can be used to access various Azure services, including Azure Storage accounts, Azure Key Vault, Azure App Service, and Azure SQL Database. By using private endpoints, you can connect to these services from within your virtual network, ensuring that the traffic remains within the Azure backbone network and doesn't traverse the public internet.

Reference: https://learn.microsoft.com/en-us/azure/private-link/private-link-overview

Domain

Describe Azure architecture and services (35–40%)

Question 64 Skipped

You've been planning to decommission your On-Prem database hosting Gigabytes of data. Which of the following is True about data ingress (moving into) for Azure?

Correct answer

It is free of cost

It is charged $0.05 per GB

- ◯ **It is charged per hour of data transferred**

- ◯ **It is charged $0.05 per TB**

Overall explanation

From the Official Azure Documentation:

Bandwidth refers to data moving in and out of Azure data centres, as well as data moving between Azure data centres; other transfers are explicitly covered by the Content Delivery Network, ExpressRoute pricing or Peering.

Data Transfer	Price
Data Transfer In	Free
Data transfer between Availability Zones(Egress and Ingress)*	$0.01 per GB
Data transfer within same Availability Zone	Free
Data transfer from Azure origin to Azure CDN**	Free
Data transfer from Azure origin to Azure Front Door	Free

To read more about Region transfer pricing, refer to the reference.

Reference: https://azure.microsoft.com/en-ca/pricing/details/bandwidth/

Domain

Describe Azure management and governance (30–35%)

Question 65 Skipped

Yes or No:

In a Public Cloud model, you get dedicated hardware, storage, and network devices than the other organizations or cloud “tenants".

Correct answer

- ◯ **No**

- ◯ **Yes**

Overall explanation

From the Official Azure Documentation:

Public clouds are the most common type of cloud computing deployment. The cloud resources (like servers and storage) are owned and operated by a third-party cloud service provider and delivered over the internet. With a public cloud, all hardware, software, and other supporting infrastructure are owned and managed by the cloud provider. Microsoft Azure is an example of a public cloud.

In a public cloud, you share the same hardware, storage, and network devices with other organisations or cloud “tenants,” and you access services and manage your account using a web browser. Public cloud deployments are frequently used to provide web-based email, online office applications, storage, and testing and development environments.

Reference: https://azure.microsoft.com/en-ca/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds/#deployment-options

Domain

Describe cloud concepts (25–30%)

Question 66 Skipped

In the _____ as a Service cloud service model, customers are responsible for managing applications, data, runtime, middleware, and operating systems, while the cloud provider manages the underlying infrastructure.

○ **Software**

Explanation

In the Software as a Service (SaaS) cloud service model, customers access software applications over the internet on a subscription basis. The cloud provider manages everything, including the infrastructure, operating systems, middleware, runtime, data, and applications. Customers only need to use the software without worrying about managing any underlying components.

○ **Platform**

Explanation

The Platform as a Service (PaaS) cloud service model provides customers with a platform to develop, run, and manage applications without the complexity of building and maintaining the infrastructure. In PaaS, the cloud provider manages the underlying infrastructure, operating systems, middleware, and runtime, while customers focus on developing and deploying their applications.

Correct answer

○ **Infrastructure**

Explanation

In the Infrastructure as a Service (IaaS) cloud service model, customers have control over the operating systems, middleware, runtime, applications, and data. They are responsible for managing these components, while the cloud provider manages the physical infrastructure, such as servers, storage, networking, and virtualization.

Overall explanation

In the **IaaS** cloud service model, customers are responsible for managing applications, data, runtime, middleware, and operating systems, while the cloud provider manages the underlying

infrastructure. Customers have more control and flexibility over their infrastructure compared to the other cloud service models, but also have more responsibility for managing their applications and workloads.

Reference: https://azure.microsoft.com/en-ca/resources/cloud-computing-dictionary/what-is-iaas/

Domain

Describe cloud concepts (25–30%)

Question 67 Skipped

_____ allows you to implement your system's logic into readily available blocks of code that can run anytime you need to respond to critical events.

○ Azure Kinect DK

Explanation

Azure Kinect DK is a developer kit for creating applications that utilize depth-sensing cameras and AI capabilities. While it can be used for building interactive experiences, it does not provide the functionality to implement system logic into code blocks for event-driven responses like Azure Functions do.

Correct answer

○ **Azure Functions**

Explanation

Azure Functions provide a serverless compute service that allows you to run code in response to events without the need to manage infrastructure. You can implement your system's logic into small blocks of code that can be triggered by various events, making it ideal for responding to critical events efficiently.

○ Azure Application Insights

Explanation

Azure Application Insights is a monitoring and analytics service that helps you understand how your application is performing. While it can provide insights into your system's behavior, it does not allow you to implement your system's logic into code blocks to respond to critical events.

◯ **Azure Quantum**

Explanation

Azure Quantum is a cloud service for quantum computing. It focuses on solving complex computational problems using quantum algorithms and does not offer the capability to implement system logic into code blocks for event-driven responses.

◯ **Azure Cognitive Services**

Explanation

Azure Cognitive Services offer pre-built AI models and APIs that enable you to add intelligent features to your applications. While they can enhance your system's capabilities, they do not provide the functionality to implement your system's logic into code blocks for event-driven responses.

Overall explanation

From the Official Azure Documentation:

Azure Functions is a serverless solution that allows you to write less code, maintain less infrastructure, and save on costs. Instead of worrying about deploying and maintaining servers, the cloud infrastructure provides all the up-to-date resources needed to keep your applications running.

You focus on the pieces of code that matter most to you, and Azure Functions handles the rest.

Azure Functions provides "compute on-demand" in **two** significant ways.

First, Azure Functions allows you to implement your system's logic into readily available blocks of code. These code blocks are called "functions". Different functions can run anytime you need

to respond to critical events.

Second, as requests increase, Azure Functions meets the demand with as many resources and function instances as necessary - but only while needed. As requests fall, any extra resources and application instances drop off automatically.

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

Domain

Describe cloud concepts (25–30%)

Question 68 Skipped

Your colleague is looking for an Azure service that can help them understand how their applications are performing and proactively identify issues that affect them , AND the resources they depend on.

What's your recommendation?

- ○ **Azure Service Health**

Explanation

Azure Service Health is focused on providing personalized guidance and support during Azure service incidents. While it can help in understanding the impact of service issues on resources, it is not designed for monitoring application performance or proactively identifying issues affecting applications.

- ○ **Azure Advisor**

Explanation

Azure Advisor is not the best recommendation for this scenario. While it provides recommendations for optimizing Azure resources and improving security, it does not offer the monitoring and performance insights needed to understand how applications are performing and identify issues affecting them.

○ **Azure Comprehend**

Correct answer

○ **Azure Monitor**

Explanation

Azure Monitor is the correct choice as it is a comprehensive monitoring solution that helps in understanding the performance of applications and identifying issues that may affect them. It provides insights into the health and performance of applications, infrastructure, and networks, allowing for proactive monitoring and issue resolution.

Overall explanation

From the Official Azure Documentation:

Azure Monitor helps you maximize the availability and performance of your applications and services. It delivers a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. This information helps you understand how your applications are performing and proactively identify issues that affect them and the resources they depend on.

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

Azure Comprehend is not an existing service.

Azure Advisor helps to quickly and easily optimize your Azure deployments. Azure Advisor analyzes your configurations and usage telemetry and offers personalized, actionable recommendations to help you optimize your Azure resources for reliability, security, operational excellence, performance, and cost.

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

Domain

Describe Azure management and governance (30–35%)

Question 69 Skipped

_____ brings signals together, to make decisions, and enforce organizational policies. In simple terms, they are if-then statements, if a user wants to access a resource, then they must complete an action.

Correct answer

◯ **Conditional Access**

Explanation

Conditional Access brings signals together, evaluates them based on predefined policies, and enforces organizational policies. It essentially consists of if-then statements, where if a user wants to access a resource, then they must complete a specific action to meet the conditions set in the policy.

◯ **Active Directory Access**

Explanation

Active Directory Access is not the correct choice in this context. While Active Directory is a directory service that manages user identities and permissions, it does not specifically refer to the concept of if-then statements and policy enforcement as described in the question.

◯ **Logical Access**

Explanation

Logical Access is not the correct choice in this context. While logical access control involves using logic-based rules to determine access rights, it does not specifically refer to the if-then statements and policy enforcement described in the question.

◯ **Demand Access**

Explanation

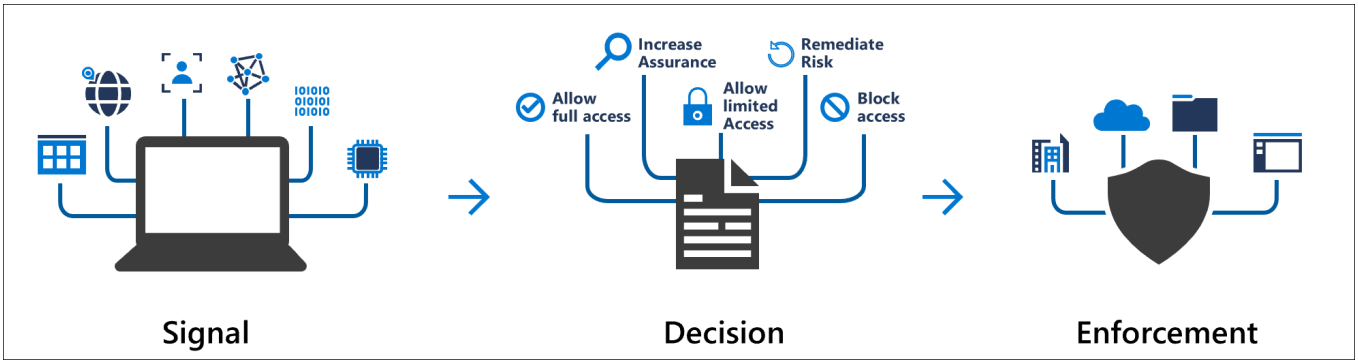
Demand Access is not the correct choice in this context. Demand Access typically refers to the ability for users to request access to resources as needed, rather than the predefined if-then statements and policy enforcement described in the question.

Overall explanation

From the Official Azure Documentation:

The modern security perimeter now extends beyond an organization's network to include user and device identity. Organizations can use identity-driven signals as part of their access control decisions.

Conditional Access brings signals together, to make decisions, and enforce organizational policies. Azure AD Conditional Access is at the heart of the new identity-driven control plane.



Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to do multi-factor authentication to access it.

Administrators are faced with two primary goals:

- Empower users to be productive wherever and whenever
- Protect the organization's assets

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Domain

Describe Azure architecture and services (35–40%)

Question 70 Skipped

Your startup plans to migrate to Azure soon, but for all the resources, you would like control of the underlying Operating System and Middleware.

Which of the following cloud models would make the most sense?

○ **Platform as a Service (PaaS)**

Explanation

Platform as a Service (PaaS) provides a platform for developers to build, deploy, and manage applications without the complexity of infrastructure management. While it offers control over the application and data, it does not provide control over the underlying operating system and middleware, which is a requirement for the startup.

○ **Software as a Service (SaaS)**

Explanation

Software as a Service (SaaS) provides ready-to-use software applications over the internet without the need for managing underlying infrastructure, operating systems, or middleware. This model does not offer control over the underlying OS and Middleware, making it not suitable for the startup's requirement.

Correct answer

○ **Infrastructure as a Service (IaaS)**

Explanation

Infrastructure as a Service (IaaS) provides virtualized computing resources over the internet, including servers, storage, and networking. With IaaS, the startup can have control over the

underlying operating system and middleware, making it the most suitable cloud model for their requirement.

○ **Anything as a Service (XaaS)**

Explanation

Anything as a Service (XaaS) is a general term that refers to any service delivered over the internet. While it can encompass various cloud service models, it does not specifically address the startup's need for control over the underlying operating system and middleware.

Overall explanation

From the Official Azure Documentation:

Infrastructure as a service (IaaS) is a type of cloud computing service that offers essential compute, storage, and networking resources on demand, on a pay-as-you-go basis. IaaS is one of the four types of cloud services, along with software as a service (SaaS), platform as a service (PaaS), and serverless.

Migrating your organization's infrastructure to an IaaS solution helps you reduce maintenance of on-premises data centers, save money on hardware costs, and gain real-time business insights. IaaS solutions give you the flexibility to scale your IT resources up and down with demand. They also help you quickly provision new applications and increase the reliability of your underlying infrastructure.

IaaS lets you bypass the cost and complexity of buying and managing physical servers and datacenter infrastructure. Each resource is offered as a separate service component, and you only pay for a particular resource for as long as you need it. A cloud computing service provider like Azure manages the infrastructure, while you purchase, install, configure, and manage your own software—including operating systems, middleware, and applications.

Incorrect Answers:

A: **Software as a service (SaaS)** allows users to connect to and use cloud-based apps over the Internet. Common examples are email, calendaring, and office tools. In this scenario, you need to run your own apps, but the OS, Middleware and Runtime are managed by the cloud provider.

B: **Platform as a service (PaaS)** is a complete development and deployment environment in the cloud. PaaS includes infrastructure servers, storage, and networking but also middleware,

development tools, business intelligence (BI) services, database management systems, and more. PaaS is designed to support the complete web application lifecycle: building, testing, deploying, managing, and updating. Here as well, the OS, Middleware and Runtime are managed by the cloud provider.

C: Anything As a Service : Irrelevant to the question completely.

References:

https://www.redhat.com/cms/managed-files/iaas-paas-saas-diagram5.1-1638x1046.png

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

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

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

Domain

Describe cloud concepts (25–30%)

Question 71 Skipped

Which of the following endpoints for a managed instance enables data access to your managed instance from outside a virtual network?

○ **Private**

Explanation

The Private endpoint for a managed instance restricts data access to only within the virtual network. It does not allow connections from outside the virtual network, ensuring that data remains secure and isolated within the network.

○ **External**

Explanation

The External endpoint is not a recognized endpoint type for a managed instance in Azure. It does not specify a valid method for enabling data access from outside a virtual network to a managed instance.

Correct answer

◯ **Public**

Explanation

The Public endpoint for a managed instance allows data access to the managed instance from outside the virtual network. It enables connections from the public internet to the managed instance, providing access to resources outside the virtual network.

◯ **Hybrid**

Explanation

The Hybrid endpoint for a managed instance is not a valid option for enabling data access from outside a virtual network. It typically refers to a combination of on-premises and cloud resources, rather than enabling external access to a managed instance.

Overall explanation

Public endpoint for a managed instance enables data access to your managed instance from outside the virtual network. You are able to access your managed instance from multi-tenant Azure services like Power BI, Azure App Service, or an on-premises network. By using the public endpoint on a managed instance, you do not need to use a VPN, which can help avoid VPN throughput issues.

Reference: https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/public-endpoint-configure?view=azuresql

Domain

Describe Azure architecture and services (35–40%)

Question 72 Skipped

Which of the following **does NOT** directly impact **Azure costs**?

Correct answer

- ◯ **The number of resources deployed in the same virtual network**

Explanation

The number of resources deployed in the same virtual network does not directly impact Azure costs. While the total number of resources may affect overall performance and management costs, it does not have a direct correlation with the pricing of Azure services.

- ◯ **The type of Azure subscription (e.g., Pay-As-You-Go vs. Reserved)**

Explanation

The type of Azure subscription, such as Pay-As-You-Go or Reserved, directly impacts Azure costs. Different subscription types have different pricing models and discounts, which can significantly affect the overall expenses.

- ◯ **The number of CPU cores used by virtual machines**

Explanation

The number of CPU cores used by virtual machines directly impacts Azure costs. Virtual machines are billed based on the number of CPU cores, memory, and storage used, so increasing the number of CPU cores will result in higher costs.

- ◯ **The region where resources are deployed**

Explanation

The region where resources are deployed can impact Azure costs due to varying pricing in different regions. Some regions may have higher costs for certain resources, affecting overall expenses.

Overall explanation

Azure costs are typically influenced by the region where resources are deployed, the type of subscription, and the resources themselves (such as the number of CPU cores in virtual machines). The number of resources within a virtual network doesn't directly affect costs unless those resources are consuming compute, storage, or network bandwidth.

Domain

Describe Azure management and governance (30–35%)

Question 73 Skipped

Which of the following is a benefit of using Azure Cloud Shell for managing Azure resources?

○ **It allows for easier integration with third-party tools and services**

Explanation

Azure Cloud Shell does not specifically enable easier integration with third-party tools and services. Its main purpose is to provide a consistent and accessible command-line interface for managing Azure resources, rather than facilitating integration with external tools and services.

Correct answer

○ **It eliminates the need to install and configure command-line interfaces on your local machine**

Explanation

Azure Cloud Shell eliminates the need to install and configure command-line interfaces on your local machine, making it convenient and efficient for managing Azure resources. This simplifies

the setup process and allows users to access the Azure environment quickly without the hassle of manual installations.

◯ **It offers more advanced features than other Azure management tools**

Explanation

Azure Cloud Shell does offer a variety of features for managing Azure resources, but it may not necessarily have more advanced features than other Azure management tools. The focus is on providing a streamlined and accessible command-line interface for managing resources in the Azure environment.

◯ **It provides faster access to Azure resources**

Explanation

While Azure Cloud Shell does provide access to Azure resources, the speed of access is not necessarily faster compared to other Azure management tools. The primary benefit lies in the convenience of not having to install and configure command-line interfaces on your local machine.

Overall explanation

'It eliminates the need to install and configure command-line interfaces on your local machine' is correct because Azure Cloud Shell provides a browser-based command-line interface that allows you to manage your Azure resources without having to install and configure command-line interfaces on your local machine. This makes it easier and more convenient to manage your Azure resources from any device and location.

Other options:

It provides faster access to Azure resources is incorrect because the speed of access to Azure resources is not determined by the management tool used, but rather by factors such as network latency and the size and complexity of the resources being accessed.

It offers more advanced features than other Azure management tools is incorrect because Azure Cloud Shell provides the same set of features as other Azure management tools, such as Azure CLI and Azure PowerShell, and does not offer any advanced features that are not available in other tools.

It allows for easier integration with third-party tools and services is incorrect because the integration of Azure Cloud Shell with third-party tools and services is not any easier or more seamless than the integration of other Azure management tools.

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

Domain

Describe Azure management and governance (30–35%)

Question 74 Skipped

Which service would you use to reduce the overhead of manually assigning permissions to a set of resources?

○ **Azure Logic Apps**

Explanation

Azure Logic Apps is a cloud service that helps you automate and orchestrate tasks, business processes, and workflows. While it can be used to automate certain tasks related to permissions, it is not specifically designed to reduce the overhead of manually assigning permissions to a set of resources.

○ **Azure Policy**

Explanation

Azure Policy is a service that helps you enforce organizational standards and compliance by applying rules and policies to your Azure resources. While it can help in ensuring that resources comply with specific policies, it does not directly reduce the manual overhead of assigning permissions to a set of resources.

Correct answer

○ **Azure Resource Manager**

Explanation

Azure Resource Manager is the correct choice as it allows you to manage and organize Azure resources in groups called resource groups. By using Azure Resource Manager, you can apply role-based access control (RBAC) to the resource group level, making it easier to assign permissions to a set of resources collectively rather than individually, reducing manual overhead.

○ **Azure Trust Center**

Explanation

Azure Trust Center focuses on providing information about Microsoft's commitment to security, privacy, compliance, and transparency. While it is important for understanding Microsoft's security practices, it does not directly help in reducing the overhead of manually assigning permissions to a set of resources.

Overall explanation

From the Official Azure Documentation:

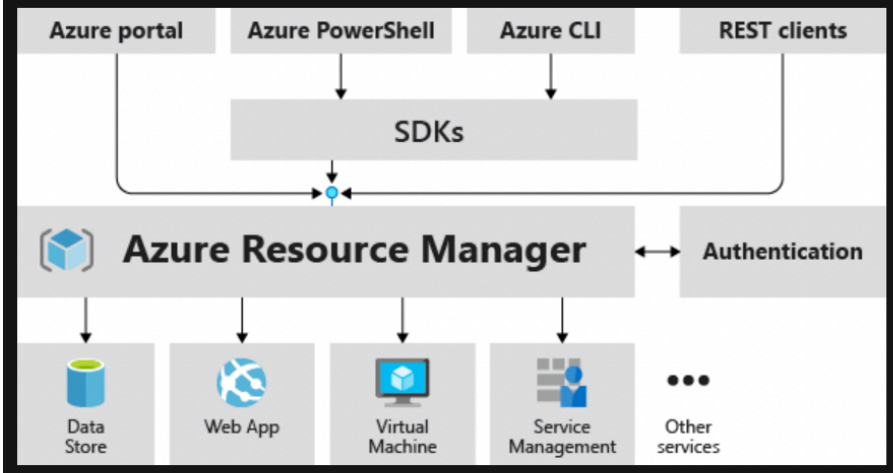
Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account. You use management features, like access control, locks, and tags, to secure and organize your resources after deployment.

To learn about Azure Resource Manager templates (ARM templates), see the ARM template overview.

Consistent management layer

When you send a request through any of the Azure APIs, tools, or SDKs, Resource Manager receives the request. It authenticates and authorizes the request before forwarding it to the appropriate Azure service. Because all requests are handled through the same API, you see consistent results and capabilities in all the different tools.

The following image shows the role Azure Resource Manager plays in handling Azure requests.



All capabilities that are available in the portal are also available through PowerShell, Azure CLI, REST APIs, and client SDKs. Functionality initially released through APIs will be represented in the portal within 180 days of initial release.

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

Domain

Describe Azure management and governance (30–35%)

Question 75 Skipped

Yes or No:

All resources in a VNet can communicate outbound to the internet, by default.

Correct answer

○ **Yes**

Explanation

Yes, all resources in a Virtual Network (VNet) can communicate outbound to the internet by default. This is because Azure automatically creates a default route that allows outbound traffic from all resources within the VNet to reach the internet. This default route enables resources to access services outside the VNet, such as Azure services, the internet, and on-premises resources.

○ **No**

Overall explanation

From the Official Azure Documentation:

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

All resources in a VNet can communicate outbound to the internet, by default. You can communicate inbound to a resource by assigning a public IP address or a public Load Balancer. You can also use public IP or public Load Balancer to manage your outbound connections. To learn more about outbound connections in Azure, see Outbound connections, Public IP addresses, and Load Balancer.

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

Domain

Describe Azure architecture and services (35–40%)

Question 76 Skipped

Which of the following can you use to set spending thresholds?

○ **Azure Pricing Calculator**

Explanation

Azure Pricing Calculator is a tool that helps estimate the cost of Azure services based on usage and configurations. While it is useful for cost estimation, it does not offer features to set spending thresholds or budget limits for monitoring and controlling spending.

Correct answer

○ **Azure Cost Management + Billing**

Explanation

Azure Cost Management + Billing allows you to set spending thresholds and budget limits to monitor and control your Azure spending. By setting these thresholds, you can receive alerts when your spending approaches or exceeds the defined limits, helping you manage costs effectively.

○ **Azure Policy**

Explanation

Azure Policy is not specifically designed to set spending thresholds. While Azure Policy can be used to enforce rules and policies for resource management and compliance, it does not offer direct features for setting budget limits or spending thresholds.

○ **Azure TCO Calculator**

Explanation

Azure TCO Calculator is a tool used to estimate the total cost of ownership for running workloads in Azure. It helps in understanding the cost implications of using Azure services but does not provide functionality to set spending thresholds or budget limits.

Overall explanation

From the Official Azure Documentation:

With Azure products and services, you only pay for what you use. As you create and use Azure resources, you're charged for the resources. Because of the deployment ease for new resources, the costs of your workloads can jump significantly without proper analysis and monitoring. You use Cost Management + Billing features to:

- Conduct billing administrative tasks such as paying your bill
- Manage billing access to costs
- Download cost and usage data that was used to generate your monthly invoice
- Proactively apply data analysis to your costs
- Set spending thresholds
- Identify opportunities for workload changes that can optimize your spending

Reference: https://docs.microsoft.com/en-us/azure/cost-management-billing/cost-management-billing-overview

Domain

Describe Azure management and governance (30–35%)

Question 77 Skipped

_____ asynchronously replicates the same applications and data across other Azure regions for disaster recovery protection.

○ **Auto-Region Replicas**

Explanation

Auto-Region Replicas is not a standard term in Azure services for replicating applications and data across regions. The term "replicas" typically refers to copies or duplicates of data or applications, but the term "Auto-Region Replicas" is not a recognized term in Azure for disaster recovery protection.

○ **Across-Region Replication**

Explanation

Across-Region Replication is not a specific term used in Azure services for replicating applications and data across different regions. The term "Cross-region replication" is more commonly used to describe this process in Azure.

Correct answer

◯ **Cross-region replication**

Explanation

Cross-region replication is the process of replicating applications and data across different Azure regions to ensure disaster recovery protection. This ensures that in case of a regional outage or disaster, the applications and data can be quickly recovered and accessed from another region.

◯ **Auto-Region Replication**

Explanation

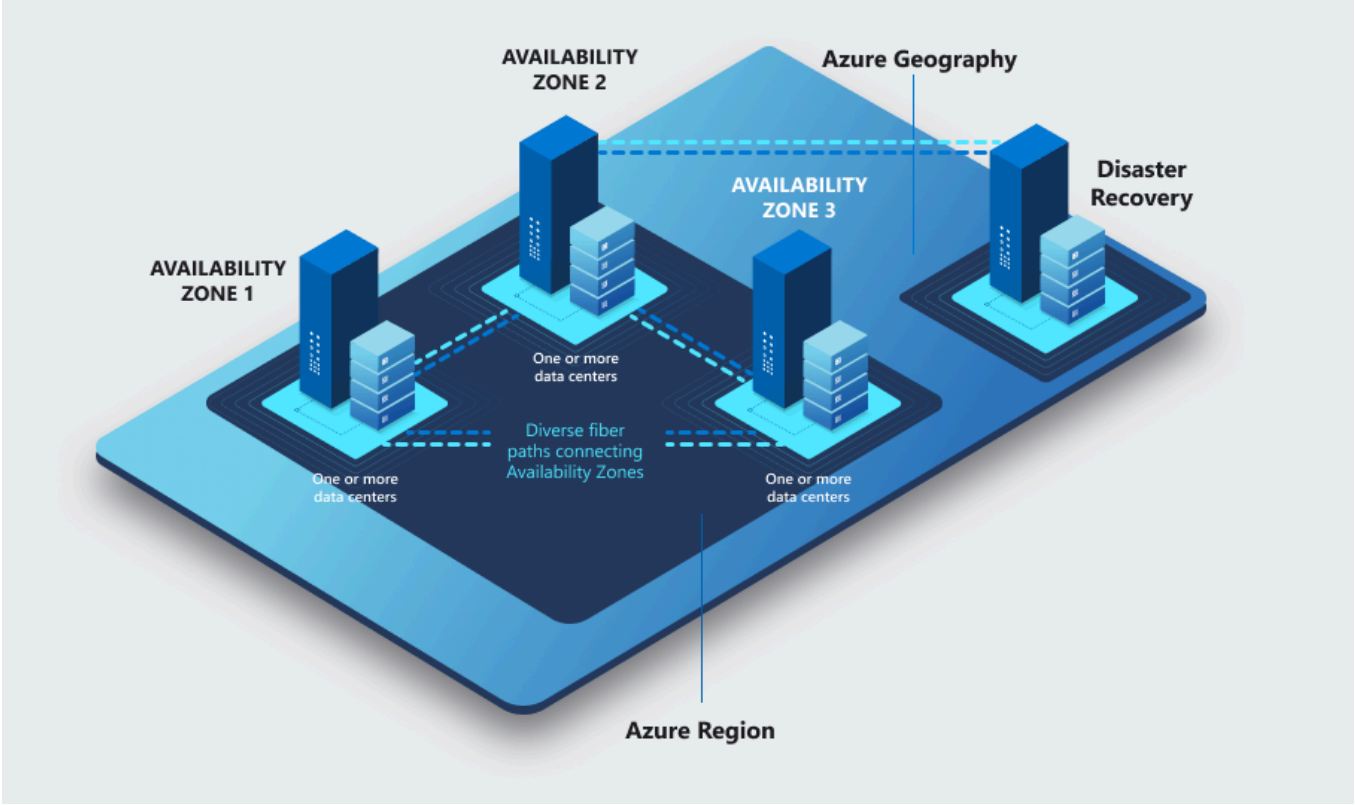
Auto-Region Replication is not a standard term in Azure services. While Azure provides automated replication and failover options for disaster recovery, the term "Auto-Region Replication" is not commonly used in this context.

Overall explanation

From the Official Azure Documentation:

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.



Some Azure services take advantage of cross-region replication to ensure business continuity and protect against data loss. Azure provides several storage solutions that make use of cross-region replication to ensure data availability. For example, Azure geo-redundant storage (GRS) replicates data to a secondary region automatically. This approach ensures that data is durable even if the primary region isn't recoverable.

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

Domain

Describe Azure architecture and services (35–40%)

Question 78 Skipped

Which of the following is a Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) for all of your Azure, On-Premises, AND Multicloud (Amazon AWS and Google GCP) resources?

Correct answer

○ **Microsoft Defender for Cloud**

Explanation

Microsoft Defender for Cloud is a comprehensive Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) solution that provides security for Azure, On-Premises, and Multicloud resources. It offers advanced threat protection, security posture management, and cloud workload protection across various cloud environments.

◯ **Azure Sentinel**

Explanation

Azure Sentinel is a cloud-native security information and event management (SIEM) service that provides intelligent security analytics and threat intelligence across the enterprise. While it offers advanced security monitoring and threat detection capabilities, it is not specifically designed as a Cloud Security Posture Management (CSPM) or Cloud Workload Protection Platform (CWPP) solution for all cloud resources.

◯ **Azure DDoS Protection**

Explanation

Azure DDoS Protection is a service that provides protection against Distributed Denial of Service (DDoS) attacks on Azure applications and resources. While it enhances the security of Azure applications by mitigating DDoS attacks, it is not a comprehensive Cloud Security Posture Management (CSPM) or Cloud Workload Protection Platform (CWPP) solution for all cloud resources.

◯ **Azure Key Vault**

Explanation

Azure Key Vault is a cloud service that securely stores and manages sensitive information such as keys, secrets, and certificates. While it plays a crucial role in securing and managing cryptographic keys and secrets, it is not a Cloud Security Posture Management (CSPM) or Cloud Workload Protection Platform (CWPP) solution for all cloud resources.

◯ **Azure Front Door**

Explanation

Azure Front Door is a global, secure entry point for web applications that offers protection, acceleration, and scalability. While it enhances the performance and security of web applications, it is not specifically designed as a Cloud Security Posture Management (CSPM) or Cloud Workload Protection Platform (CWPP) solution for all cloud resources.

Overall explanation

From the Official Azure Documentation:

Microsoft Defender for Cloud is a Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) for all of your Azure, on-premises, and multicloud (Amazon AWS and Google GCP) resources. Defender for Cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises:

- **Defender for Cloud secure score** **continually assesses** your security posture so you can track new security opportunities and precisely report on the progress of your security efforts.
- **Defender for Cloud recommendations** **secures** your workloads with step-by-step actions that protect your workloads from known security risks.
- **Defender for Cloud alerts** **defends** your workloads in real-time so you can react immediately and prevent security events from developing.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

Domain

Describe Azure architecture and services (35–40%)

Question 79 Skipped

Which of the following can repeatedly deploy your infrastructure throughout the development lifecycle and have confidence your resources are deployed in a consistent manner?

- ○ Azure Templates

Explanation

Azure Templates is not a specific tool or service in Azure. It may refer to Azure Resource Manager templates, which are used for infrastructure deployment, but the term itself is not commonly used in the context of Azure deployment practices.

◯ **Management groups**

Explanation

Management groups in Azure are used for organizing and managing multiple subscriptions in a hierarchy. While they can help with governance and policy enforcement across subscriptions, they are not specifically designed for deploying infrastructure in a consistent manner throughout the development lifecycle.

◯ **The Azure API Management service**

Explanation

The Azure API Management service is not designed for infrastructure deployment or managing resources in a consistent manner throughout the development lifecycle. It is primarily used for managing APIs and controlling access to them, rather than deploying and managing infrastructure resources.

Correct answer

◯ **Azure Resource Manager templates**

Explanation

Azure Resource Manager templates allow you to define the infrastructure and configuration of your Azure resources in a declarative template format. By using these templates, you can repeatedly deploy your infrastructure throughout the development lifecycle in a consistent and reliable manner, ensuring that your resources are deployed as intended every time.

Overall explanation

Azure Resource Manager Templates is correct since templates are idempotent (Same), which means you can deploy the same template many times and get the same resource types in the same state.

Reference: https://docs.microsoft.com/en-us/azure/azure-resource-manager/template-deployment-overview

Domain

Describe Azure management and governance (30–35%)

Question 80 Skipped

A development team is tasked with building an application where resources are provisioned only when required, with minimal overhead for managing infrastructure. The application should scale automatically in response to user requests, and costs should be directly tied to actual usage. Which of the following best describes the appropriate Azure service for this scenario?

○ **Azure Kubernetes Service (AKS)**

Explanation

Azure Kubernetes Service (AKS) is a managed Kubernetes service that allows you to deploy, manage, and scale containerized applications using Kubernetes. While AKS provides scalability and automation features, it may not be the most suitable option for a scenario where resources are provisioned only when required with minimal overhead, as it still requires manual management of infrastructure.

Correct answer

○ **Azure Functions with serverless compute**

Explanation

Azure Functions with serverless compute is the correct choice for this scenario. Azure Functions allow you to run event-driven code without having to explicitly provision or manage infrastructure. They automatically scale based on demand, ensuring resources are only

provisioned when needed. Costs are directly tied to actual usage, making it a cost-effective and efficient solution for the described scenario.

○ **Azure Virtual Machines with Autoscale**

Explanation

Azure Virtual Machines with Autoscale allow you to automatically adjust the number of virtual machines in a scale set based on demand. While this can help with scaling, it still requires manual management of virtual machines and may not provide the most cost-effective solution for a scenario where resources are provisioned only when required with minimal overhead.

○ **Virtual Machine Scale Sets**

Explanation

Virtual Machine Scale Sets allow you to create and manage a group of identical, load-balanced virtual machines. While they can automatically scale based on demand, they still require manual management of infrastructure and may not provide the most cost-effective solution for a scenario where resources are provisioned only when required with minimal overhead.

Overall explanation

Azure Functions provides a **serverless compute** model, where resources are provisioned only when the code is executed, and scaling happens automatically based on demand. Costs are tied directly to actual usage, and there is no need for infrastructure management, which fits the scenario perfectly. **Virtual Machine Scale Sets** and **AKS** require more infrastructure management, while **Azure Virtual Machines** with autoscale can also scale based on demand but are still tied to virtual machine instances rather than a fully serverless approach.

Domain

Describe cloud concepts (25–30%)

Question 81 Skipped

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

Match each Azure service type to the party responsible for securing the **application code**.

Valid options (Case Sensitive):

- Customer
- Microsoft

A) IaaS: __
B) PaaS: __
C) SaaS: __

Correct answer

Customer, Customer, Microsoft

Explanation

- **IaaS (Infrastructure-as-a-Service)**: In an IaaS model, the **customer** is responsible for securing the application code, as they manage the operating system, middleware, and applications. Azure provides the infrastructure, but the customer takes on the responsibility for securing everything above that level.

- **PaaS (Platform-as-a-Service)**: In PaaS, the **customer** is still responsible for securing the application code. Microsoft manages the underlying infrastructure and platform, but the customer handles their own code, configurations, and applications.

- **SaaS (Software-as-a-Service)**: In SaaS, the **provider (Microsoft)** manages the application and its security, as the customer only uses the software. The customer does not modify or manage the application code, as it's fully managed by the SaaS provider.

This highlights the different levels of responsibility for security across Azure's service models.

Domain

Describe cloud concepts (25–30%)

Question 82 Skipped

Yes or No:

It is possible to deploy a new Azure Virtual Network (VNet) using PowerAutomate on a Google Chromebook.

- ○ Yes

Correct answer

- ○ No

Overall explanation

No, PowerApps is **not** a part of Azure!

Domain

Describe Azure architecture and services (35–40%)

Question 83 Skipped

Which type of scaling focuses on adjusting the capabilities of resources, such as increasing processing power?

- ○ Static scaling

Explanation

Static scaling involves manually adjusting the resources to a fixed capacity and does not allow for automatic adjustments based on workload changes. It does not focus on dynamically

increasing processing power as needed.

○ **Horizontal scaling**

Explanation

Horizontal scaling involves adding more instances of resources, such as servers, to distribute the workload across multiple machines. It does not focus on adjusting the capabilities of individual resources like increasing processing power.

Correct answer

○ **Vertical scaling**

Explanation

Vertical scaling, also known as scaling up, involves increasing the capabilities of individual resources, such as increasing the processing power, memory, or storage capacity of a single server. This type of scaling is suitable for adjusting resource capabilities to meet increased demands.

○ **Elastic scaling**

Explanation

Elastic scaling refers to the ability to automatically adjust the resources based on the workload or demand. While it can include both horizontal and vertical scaling, the focus is on dynamically scaling resources up or down based on the current needs, rather than specifically increasing processing power.

Overall explanation

From the official docs:

Vertical scaling involves adjusting the capabilities of resources, such as adding more CPUs or RAM to a virtual machine. It focuses on enhancing the capacity of individual resources.

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.

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 84 Skipped

A company needs to store large volumes of archival data in Azure with minimal access frequency, while ensuring resilience and cost efficiency. The data must be replicated across multiple availability zones within the same region for high availability. Which combination of storage tier and replication strategy is best suited for this scenario?

- ○ **Archive tier with GRS**

Explanation

Archive tier storage is designed for data with low access frequency and is the most cost-effective option for storing archival data. However, GRS (Geo-redundant storage) replicates data to a secondary region, which may not be necessary for data that only requires replication within the same region.

- ○ **Hot tier with LRS**

Explanation

Hot tier storage is optimized for frequently accessed data and may not be cost-efficient for storing archival data with minimal access frequency. LRS (Locally redundant storage) replicates data within the same data center, which may not provide the desired high availability across multiple availability zones.

Correct answer

◯ **Archive tier with ZRS**

Explanation

Archive tier storage is the most suitable option for storing archival data with minimal access frequency, as it offers the lowest storage costs. ZRS (Zone-redundant storage) replicates data across availability zones within the same region, ensuring high availability and resilience for the data without the additional cost of geo-replication.

◯ **Cool tier with ZRS**

Explanation

Cool tier storage is suitable for data that is accessed less frequently but still requires quick access when needed. Also, ZRS (Zone-redundant storage) replicates data across availability zones within the same region for high availability, which may not be necessary for archival data with minimal access frequency.

Overall explanation

Correct Answer: Archive tier with ZRS

- **Archive tier**: This is the lowest-cost storage option in Azure Blob Storage, designed for infrequently accessed data, such as archival data. It is a perfect fit for storing large volumes of data that are rarely accessed, as the Archive tier is optimized for cost-efficiency.
- **ZRS (Zone-Redundant Storage)**: ZRS replicates your data across three availability zones within a single Azure region, ensuring high resilience and availability. ZRS is appropriate for scenarios where you need redundancy within a region but at a lower cost compared to geo-replication options like GRS.

Why the other options are incorrect:

- **Cool tier with ZRS**: The **Cool tier** is designed for infrequently accessed data, but it's typically used for data that will be accessed more often than Archive tier

data. It would not be the most cost-effective option for data that is rarely accessed. **ZRS** would provide resilience within a region, but this combination does not offer the deepest cost savings for archival data.

- **Archive tier with GRS**: **GRS (Geo-Redundant Storage)** replicates data across regions, offering more resilience than ZRS but at a higher cost. Since the scenario specifies data in a single region with **three zones**, **ZRS**is a better match for this requirement. **GRS** would be overkill for a single-region scenario and would increase the cost unnecessarily.
- **Hot tier with LRS**: The **Hot tier** is designed for frequently accessed data, not archival data. **LRS (Locally Redundant Storage)** provides replication within a single data center in a region, but it does not provide the cross-zone redundancy required by the scenario. It's not suitable for infrequent access data, especially at a lower cost.

Domain

Describe Azure architecture and services (35–40%)

Question 85 Skipped

Is it possible for you to run BOTH Bash and Powershell based scripts from the Azure Cloud shell?

○ **No**

Explanation

No, this statement is incorrect. It is possible to run both Bash and Powershell based scripts from the Azure Cloud Shell. The Cloud Shell supports multiple shell environments, including Bash and Powershell, to provide flexibility and convenience for users managing Azure resources.

Correct answer

○ **Yes**

Explanation

Yes, it is possible to run both Bash and Powershell based scripts from the Azure Cloud Shell. The Azure Cloud Shell provides an integrated command-line experience for managing Azure

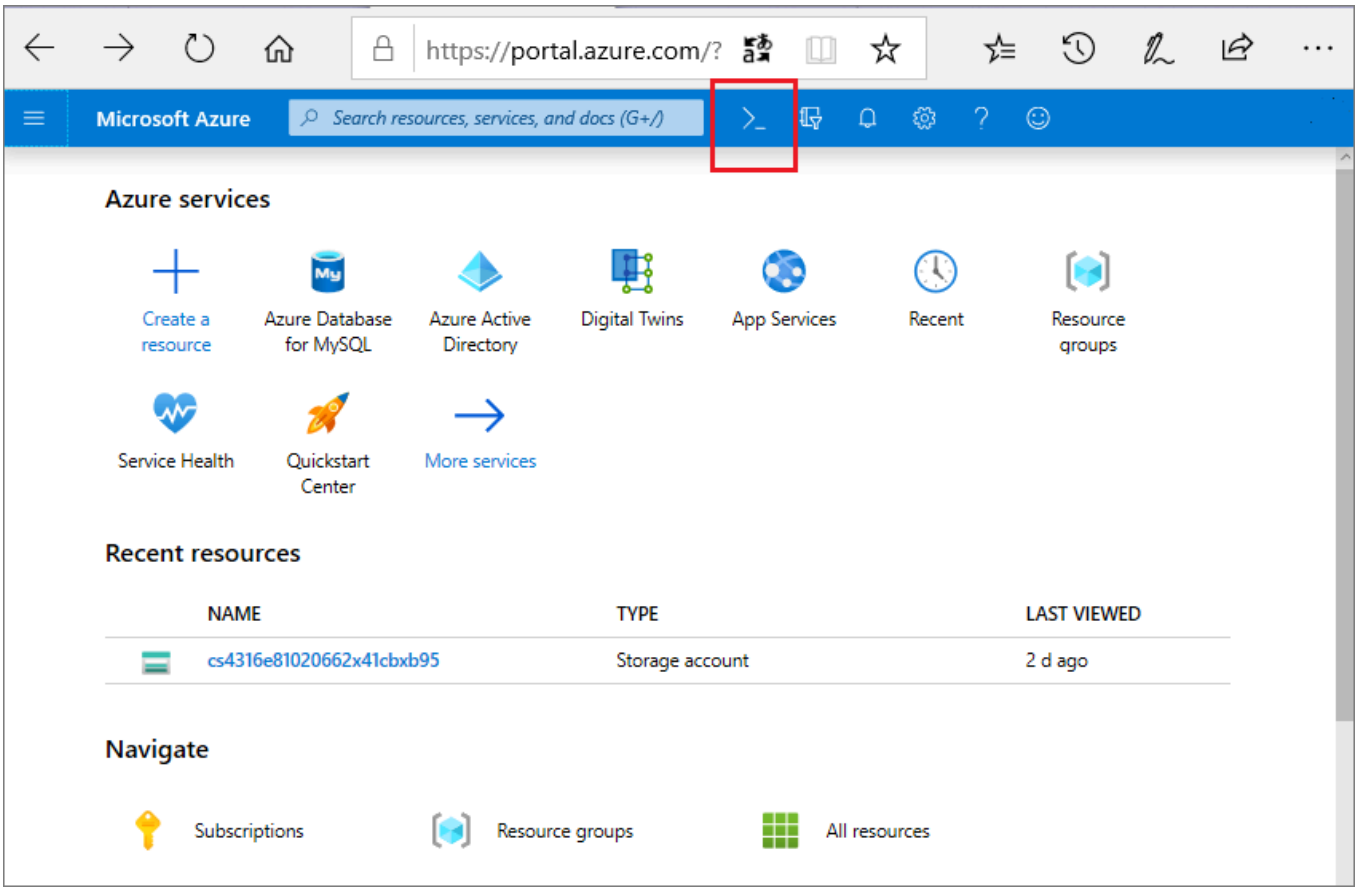
resources. It supports both Bash and Powershell environments, allowing users to choose the scripting language that best suits their needs for interacting with Azure services and resources.

Overall explanation

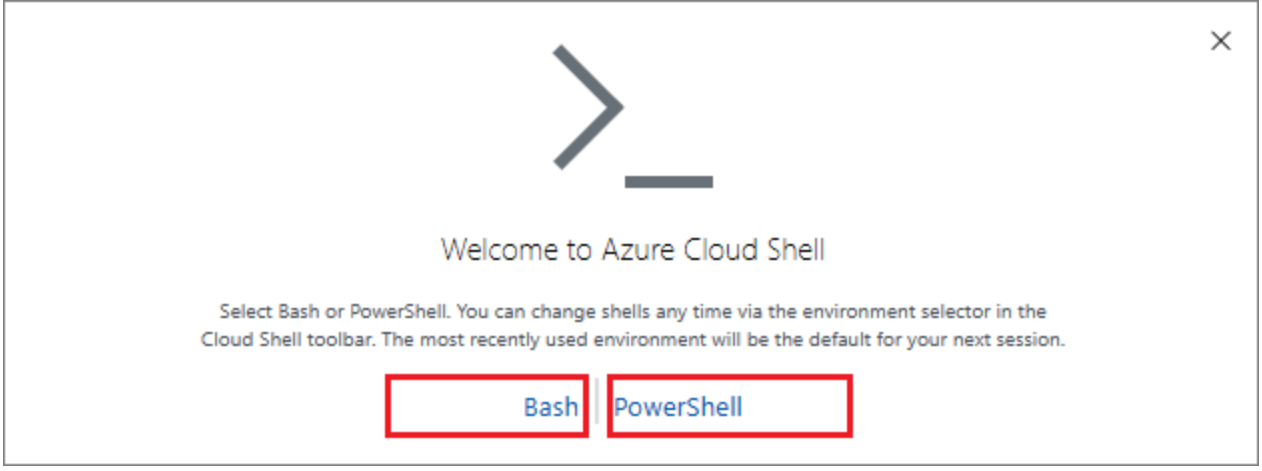
From the Official Azure Documentation:

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.**

Select **Cloud Shell**.



Select **Bash** or **PowerShell**.



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

Domain

Describe Azure management and governance (30–35%)

Question 86 Skipped

In which scenario would you use the Business-to-Business (B2B) collaboration feature in Entra ID?

- ○ **Allowing customers to sign up for your e-commerce website.**
- ○ **Enabling employees to access internal applications.**
- ○ **Providing internal access to company reports.**

Correct answer

- ○ **Granting external vendors access to a shared project workspace.**

Explanation

Granting external vendors access to a shared project workspace is a common scenario where the B2B collaboration feature in Azure AD would be used. It allows organizations to securely

collaborate with external partners by providing them access to specific resources or applications.

Overall explanation

Business-to-Business (B2B) collaboration in Entra ID is used to collaborate with users external to your organization, such as vendors or partners. It allows you to securely share resources like documents and applications while maintaining control over access.

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

Domain

Describe Azure management and governance (30–35%)

Question 87 Skipped

A company pays only for Azure resources it uses, adjusting costs based on demand. Which concepts apply? (Select all that apply.)

☐ **Fixed pricing model**

Explanation

The fixed pricing model does not align with the company's ability to adjust costs based on demand. It involves a set price regardless of resource usage, which may not be suitable for a company looking to optimize costs based on fluctuating demand.

☐ **Capital expenditure model**

Explanation

The capital expenditure model involves upfront investment in resources, which is not in line with the company's requirement to adjust costs based on demand. This model typically

requires a fixed budget and does not offer the same flexibility as a consumption-based or pay-as-you-go pricing model.

Correct selection

☐ **Pay-as-you-go pricing**

Explanation

The pay-as-you-go pricing model enables the company to pay for Azure resources as they are used, providing flexibility and scalability in adjusting costs based on demand. This aligns with the company's requirement to adjust costs based on resource usage.

Correct selection

☐ **Consumption-based model**

Explanation

The consumption-based model allows the company to pay for Azure resources based on actual usage. This means that costs can be adjusted according to demand, making it a flexible and cost-effective pricing model for businesses.

Overall explanation

- **Consumption-based model:** This model is based on paying for resources only when they are used, meaning that as demand increases or decreases, costs adjust accordingly. This is exactly what the scenario describes.

- **Pay-as-you-go pricing: Pay-as-you-go** is a specific form of the **consumption-based model**, where companies pay for the actual amount of resources they use, without the need for upfront payments or long-term commitments. The cost is directly tied to usage, which aligns perfectly with the scenario.

Why the other options are incorrect:

- **Fixed pricing model:** In the **fixed pricing model**, the company pays a set amount regardless of the actual usage, which is not what the scenario describes. The company in the question is adjusting costs based on usage, so this does not apply.

- **Capital expenditure model:** A **capital expenditure (CapEx)** model involves large upfront investments in physical infrastructure, which is not the case here. The company is only paying for what they use, which is a key characteristic of operational expenditure (OpEx), not capital expenditure.

Domain

Describe cloud concepts (25–30%)

Question 88 Skipped

An _____ is a collection of policy definitions that are grouped together towards a specific goal or purpose in mind.

○ **Azure Collection**

Explanation

Azure Collection is not a valid term in Azure terminology. There is no concept of a collection specifically related to policy definitions in Azure. It does not accurately describe a group of policy definitions with a common goal or purpose.

○ **Azure Bundle**

Explanation

Azure Bundle is not a recognized term in Azure terminology related to policy definitions. It does not accurately describe a collection of policy definitions grouped together towards a specific goal or purpose in mind.

○ **Azure Group**

Explanation

Azure Group typically refers to a resource group in Azure, which is used to logically group related resources for management and billing purposes. It is not specifically related to policy definitions or governance in Azure.

Correct answer

◯ **Azure Initiative**

Explanation

An Azure Initiative is a collection of policy definitions that are grouped together towards a specific goal or purpose in mind. It allows organizations to manage compliance and governance across their Azure resources by defining a set of policies that align with their objectives.

Overall explanation

From the Official Azure Documentation:

An Azure initiative is a collection of Azure policy definitions that are grouped together towards a specific goal or purpose in mind. Azure initiatives simplify management of your policies by grouping a set of policies together as one single item. For example, you could use the PCI-DSS built-in initiative which has all the policy definitions that are centered around meeting PCI-DSS compliance.

Similar to Azure Policy, initiatives have **definitions** (a bunch of policies) , assignments and parameters. Once you determine the definitions that you want, you would assign the initiative to a scope so that it can be applied.

Reference: Azure Policy Initiatives vs Azure Policies: When should I use one over the other? (microsoft.com)

Domain

Describe Azure management and governance (30–35%)

Question 89 Skipped

As the Cloud Admin of your organization, you want to Block your employees from accessing your apps from specific locations. Which of the following can help you achieve this?

○ **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 SSO enhances user experience and security, it does not offer the functionality to block access to apps from specific locations.

○ **Azure Sentinel**

Explanation

Azure Sentinel is a cloud-native security information and event management (SIEM) service that provides intelligent security analytics and threat detection. While Azure Sentinel is crucial for monitoring and responding to security incidents, it does not directly help in blocking access to apps from specific locations.

Correct answer

◯ **Microsoft Entra ID Conditional Access**

Explanation

Microsoft Entra ID Conditional Access allows you to control access to your apps based on specific conditions, such as location, device compliance, and user risk. By configuring conditional access policies, you can block access to your apps from specific locations, ensuring that only authorized users can access them.

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

Explanation

Azure Role Based Access Control (RBAC) is used to manage user access to resources in Azure based on their roles. While RBAC is essential for controlling permissions within Azure

resources, it does not provide the capability to block access to apps based on specific locations.

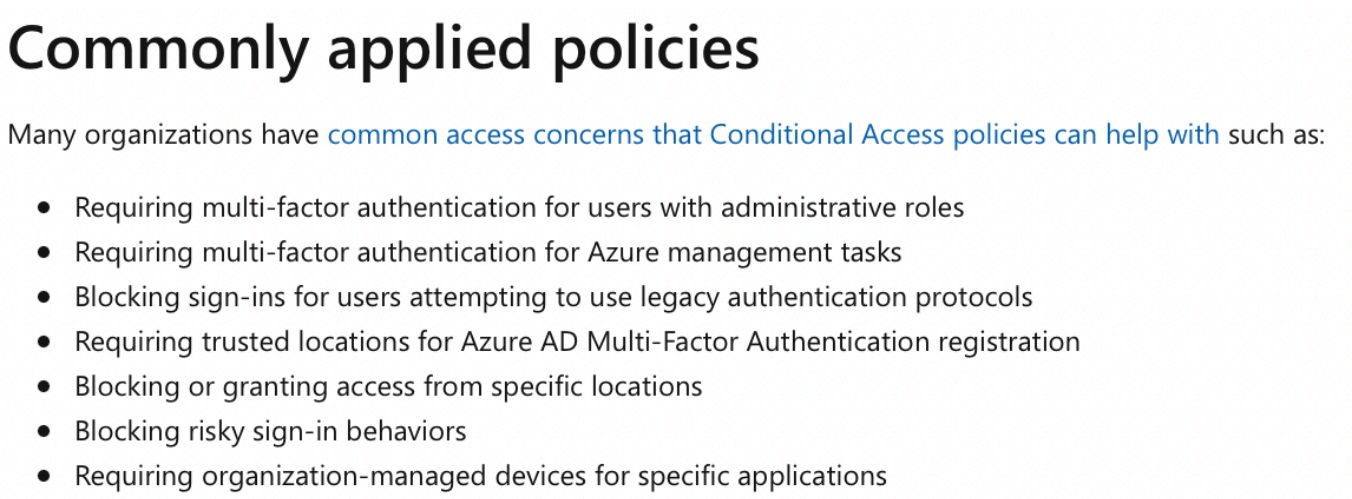
Overall explanation

From the Official Azure Documentation:

The modern security perimeter now extends beyond an organization's network to include user and device identity. Organizations can use identity-driven signals as part of their access control decisions.

Conditional Access brings signals together, to make decisions, and enforce organizational policies. Microsoft Entra ID Conditional Access is at the heart of the new identity-driven control plane.

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to do multi-factor authentication to access it.



Commonly applied policies

Many organizations have common access concerns that Conditional Access policies can help with such as:

- Requiring multi-factor authentication for users with administrative roles
- Requiring multi-factor authentication for Azure management tasks
- Blocking sign-ins for users attempting to use legacy authentication protocols
- Requiring trusted locations for Azure AD Multi-Factor Authentication registration
- Blocking or granting access from specific locations
- Blocking risky sign-in behaviors
- Requiring organization-managed devices for specific applications

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Domain

Describe Azure architecture and services (35–40%)

Question 90 Skipped

_____ **Infrastructure as Code** involves writing scripts in languages like Bash or PowerShell. You explicitly state commands that are executed to produce a desired outcome.

- Defined

Correct answer

- **Imperative**

- Ad-Hoc

- Declarative

Overall explanation

From the official documentation :

Imperative Infrastructure as Code involves writing scripts in languages like Bash or PowerShell. You explicitly state commands that are executed to produce a desired outcome. When you use imperative deployments, it's up to you to manage the sequence of dependencies, error control, and resource updates.

Reference: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/infrastructure-as-code

Domain

Describe Azure management and governance (30–35%)

Question 91 Skipped

Which of the following can help you download cost and usage data that was used to generate your monthly invoice?

○ **Azure Monitor**

Explanation

Azure Monitor is a service that helps you monitor the performance and health of your Azure resources. While it provides valuable insights into your resource usage, it does not specifically offer the capability to download detailed cost and usage data for billing purposes.

○ **Azure Advisor**

Explanation

Azure Advisor is a service that provides recommendations to help you optimize your Azure resources for performance, security, and cost. However, it does not offer the functionality to download cost and usage data for your monthly invoice.

Correct answer

◯ **Azure Cost Management**

Explanation

Azure Cost Management is the correct choice as it provides tools to help you analyze, manage, and optimize your Azure costs. It allows you to download detailed cost and usage data that was used to generate your monthly invoice, helping you understand your spending and make informed decisions.

○ **Azure Resource Manager**

Explanation

Azure Resource Manager is not the correct choice for downloading cost and usage data for your monthly invoice. While it helps you manage your Azure resources, it does not provide detailed cost and usage data for billing purposes.

Overall explanation

From the Official Azure Documentation:

By using the Microsoft cloud, you can significantly improve the technical performance of your business workloads. It can also reduce your costs and the overhead required to manage organizational assets. However, the business opportunity creates a risk because of the potential for waste and inefficiencies that are introduced into your cloud deployments. Cost Management + Billing is a suite of tools provided by Microsoft that help you analyze, manage, and optimize the costs of your workloads. Using the suite helps ensure that your organization is taking advantage of the benefits provided by the cloud.

With Azure products and services, you only pay for what you use. As you create and use Azure resources, you're charged for the resources. Because of the deployment ease for new resources, the costs of your workloads can jump significantly without proper analysis and monitoring. You use Cost Management + Billing features to:

- Conduct billing administrative tasks such as paying your bill
- Manage billing access to costs
- Download cost and usage data that was used to generate your monthly invoice
- Proactively apply data analysis to your costs
- Set spending thresholds
- Identify opportunities for workload changes that can optimize your spending

Reference: https://docs.microsoft.com/en-us/azure/cost-management-billing/cost-management-billing-overview

Domain

Describe Azure management and governance (30–35%)

Question 92 Skipped

Which of the following services can help applications absorb unexpected traffic bursts, which prevents servers from being overwhelmed by a sudden flood of requests?

- ○ **Azure Decouple Storage**

Explanation

Azure Decouple Storage is not a valid Azure service. It is important to ensure the accuracy of service names when selecting options in Azure-related questions.

○ **Azure Message Storage**

Explanation

Azure Message Storage is not a valid Azure service. It is crucial to have a good understanding of the available Azure services to accurately identify which ones can help applications absorb unexpected traffic bursts.

Correct answer

○ **Azure Queue Storage**

Explanation

Azure Queue Storage is a service that helps applications absorb unexpected traffic bursts by providing a reliable messaging solution. It allows applications to decouple components and scale independently, making it an ideal choice for preventing servers from being overwhelmed by sudden spikes in traffic.

○ **Azure Table Storage**

Explanation

Azure Table Storage is a NoSQL data store used for storing structured data. While it can be used for various purposes, it is not specifically designed to help applications absorb unexpected traffic bursts or prevent servers from being overwhelmed by sudden floods of requests.

Overall explanation

From the Official Azure Documentation:

Azure Queue Storage is a service for storing large numbers of messages. You access messages from anywhere in the world via authenticated calls using HTTP or HTTPS. A queue message can be up to 64 KB in size. A queue may contain millions of messages, up to the total capacity limit of a storage account. Queues are commonly used to create a backlog of work to process asynchronously.

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

Domain

Describe Azure architecture and services (35–40%)

Question 93 Skipped

Which of the following services can you use to calculate your estimated hourly or monthly costs for using Azure?

- ○ **Azure Total Cost of Ownership (TCO) calculator**

Explanation

The Azure Total Cost of Ownership (TCO) calculator is used to estimate the total cost of ownership for running workloads on Azure compared to an on-premises environment. It is not specifically designed to calculate hourly or monthly costs for using Azure services.

Correct answer

- ○ **Azure Pricing Calculator**

Explanation

The Azure Pricing Calculator allows you to estimate your hourly or monthly costs for using Azure services. You can select the services you plan to use, adjust the usage details, and get an estimate of the costs involved.

- ○ **Azure Cost Management**

Explanation

Azure Cost Management is a tool that helps you monitor, allocate, and optimize your Azure costs. While it provides insights into your spending and usage, it is not primarily used for calculating estimated hourly or monthly costs for using Azure services.

○ Azure Calculator

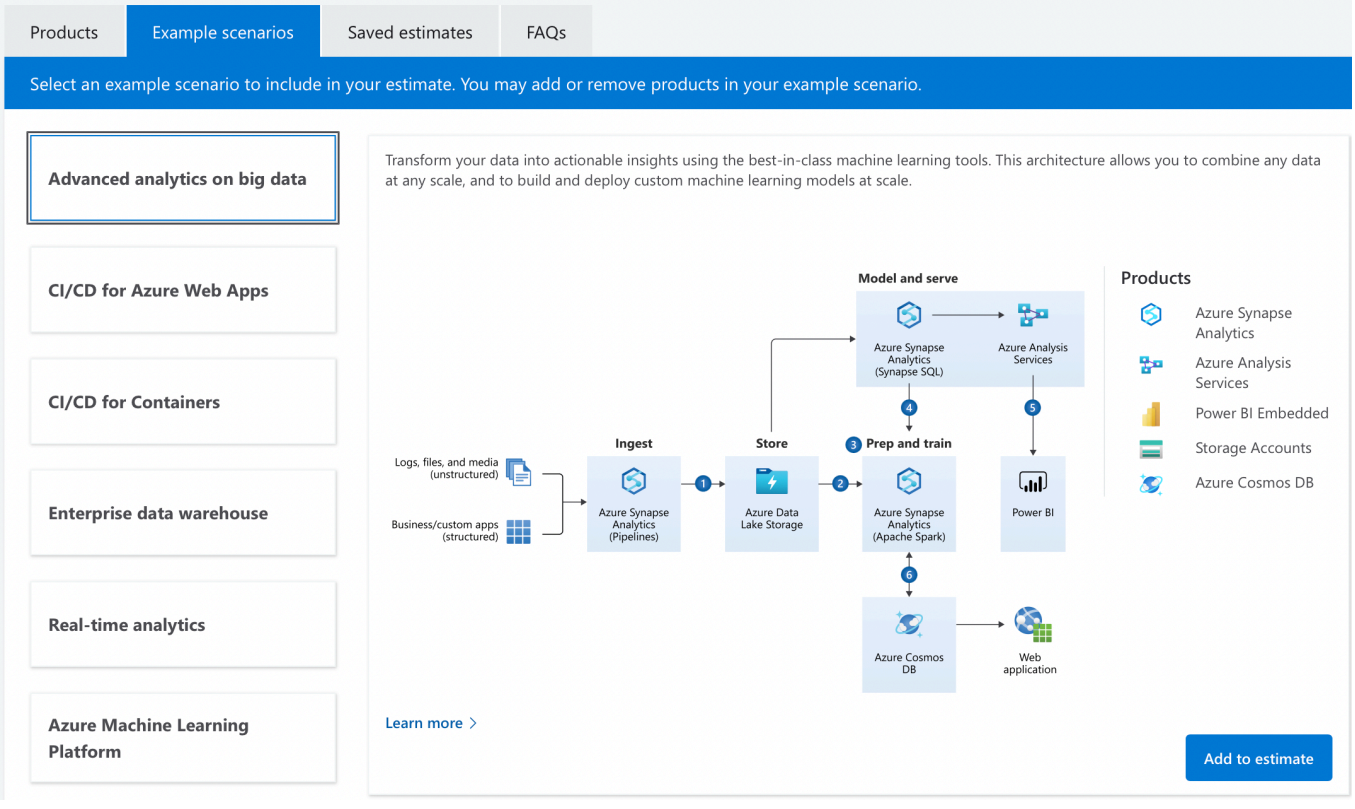
Explanation

The Azure Calculator is a tool that allows you to estimate the costs of running specific Azure services. However, it is not specifically designed to calculate estimated hourly or monthly costs for using Azure services across different services and usage scenarios.

Overall explanation

From the Official Azure Documentation:

You can use the **Azure Pricing Calculator** to calculate your estimated hourly or monthly costs for using Azure. **Azure TCO** on the other hand is primarily used to estimate the cost savings you can realize by migrating your workloads to Azure.



Reference: https://azure.microsoft.com/en-ca/pricing/calculator/

Domain

Describe Azure management and governance (30–35%)

Question 94 Skipped

Yes or No:

It is possible to have multiple Subscriptions inside a Management Group.

○ **No**

Correct answer

○ **Yes**

Explanation

Yes, it is possible to have multiple Subscriptions inside a Management Group in Azure. A Management Group is a logical container that allows you to manage access, policies, and compliance for multiple Azure Subscriptions. This hierarchical structure helps organize resources and apply governance controls across all Subscriptions within the Management Group.

Overall explanation

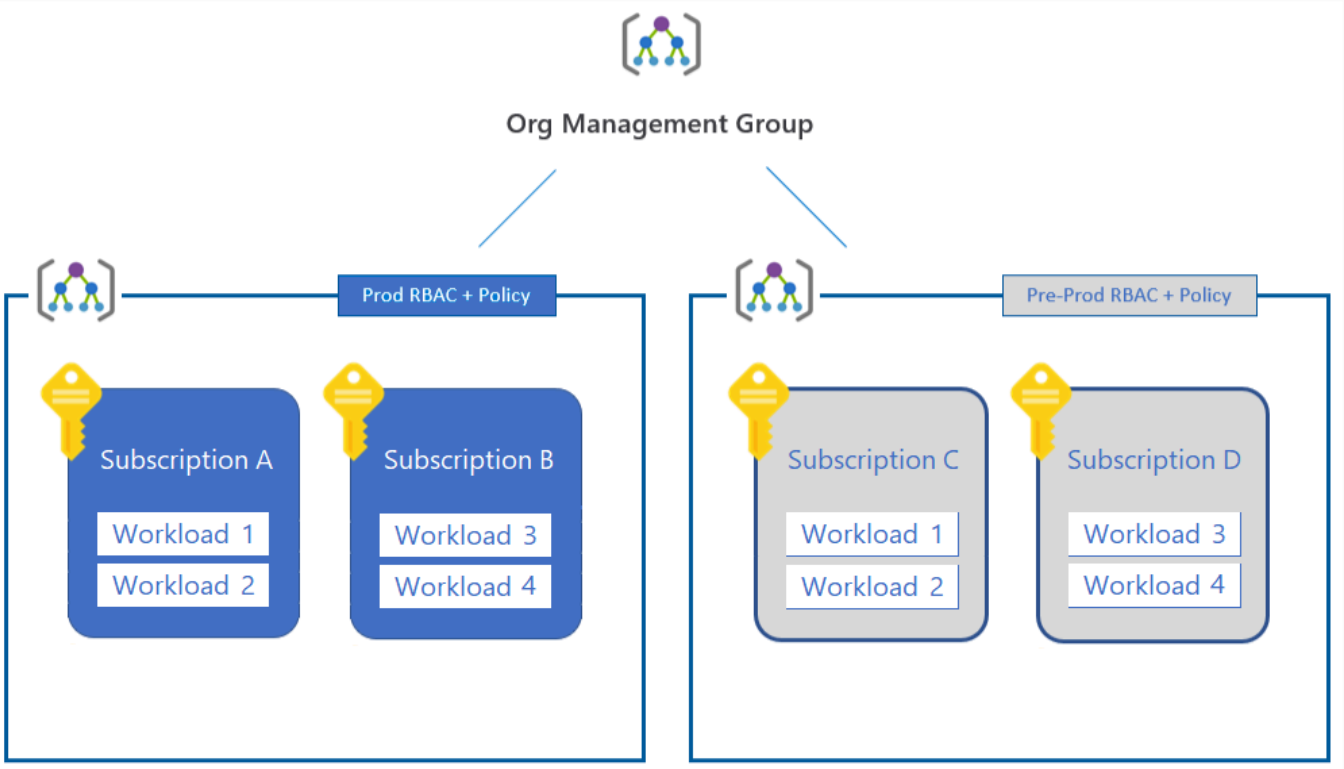
From the Official Azure Documentation:

When you define your management group hierarchy, first create the root management group. Then move all existing subscriptions in the directory into the root management group. New subscriptions always go into the root management group initially. Later, you can move them to another management group.

What happens when you move a subscription to an existing management group? The subscription inherits the policies and role assignments from the management group hierarchy

above it. Establish many subscriptions for your Azure workloads. Then create other subscriptions to contain Azure services that other subscriptions share.

Do you expect your Azure environment to grow? Then create management groups for production and nonproduction now, and apply appropriate policies and access controls at the management group level. As you add new subscriptions to each management group, those subscriptions inherit the appropriate controls.



Reference: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/organize-subscriptions

Domain

Describe Azure management and governance (30–35%)

Question 95 Skipped

Which cloud pricing model is best suited for a company that has long-term, predictable needs and prefers the stability of fixed monthly payments while also ensuring that they are not overpaying for unused capacity during periods of low demand?

- ○ **Spot pricing model**

Explanation

The spot pricing model offers resources at a discounted rate based on available capacity, making it a cost-effective option for non-critical workloads or tasks that can be interrupted. However, it may not provide the stability of fixed monthly payments that a company with long-term, predictable needs is seeking as Spot Instances are NOT guaranteed.

◯ **Consumption-based model**

Explanation

The consumption-based model charges customers based on the resources they consume, making it suitable for variable workloads. However, it may not provide the stability of fixed monthly payments that a company with long-term, predictable needs is looking for.

◯ **Pay-as-you-go pricing**

Explanation

Pay-as-you-go pricing is a flexible model where customers pay for the resources they use, typically on an hourly or per-minute basis. This model is not the best choice for a company with long-term, predictable needs looking for stable, fixed monthly payments.

Correct answer

◯ **Reserved pricing model**

Explanation

The reserved pricing model allows customers to commit to a specific amount of resources for a set period, typically one to three years, at a discounted rate. This model is best suited for a company with long-term, predictable needs that prefers fixed monthly payments and wants to avoid overpaying for unused capacity during periods of low demand.

Overall explanation

The **Reserved pricing model** is best for companies with predictable long-term needs because it provides discounted pricing in exchange for committing to a specific amount of resources

over one or three years. This model ensures cost stability and avoids the risk of overpaying, as it locks in a fixed cost while accommodating predictable workloads. In contrast, **Pay-as-you-go** and **Consumption-based** models are more flexible but may result in higher costs for predictable workloads.

Domain

Describe cloud concepts (25–30%)