

# Practice Test - 1 - Results

[Back to result overview](#)

## Attempt 1

All domains

80 all

1 correct

0 incorrect

79 skipped

0 marked

[Collapse all questions](#)

### Question 1 Correct

Yes or No:

If you assign permissions to a resource group, all the resources inside it inherit these permissions.

No

Your answer is correct

Yes

### Explanation

Yes, when you assign permissions to a resource group in Azure, all the resources contained within that resource group inherit those permissions. This simplifies access management and ensures consistency in permissions across all resources within the resource group.

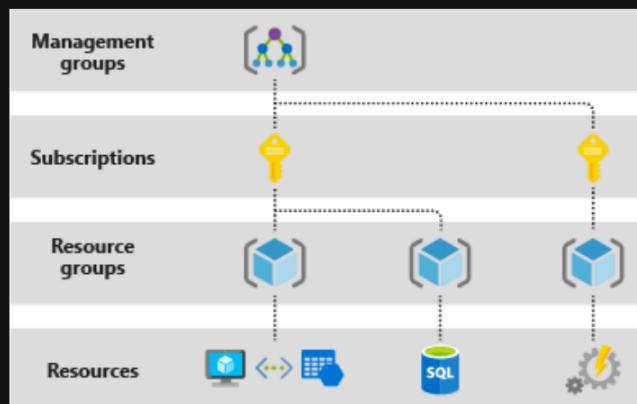
### Overall explanation

Yes, it is true that if you assign certain permissions to a resource group, then all the resources inside it inherit those permissions.

See below (**VERY IMPORTANT TO UNDERSTAND AND REMEMBER THIS DIAGRAM**):

# Understand scope

Azure provides four levels of scope: [management groups](#), subscriptions, resource groups, and resources. The following image shows an example of these layers.



You apply management settings at any of these levels of scope. The level you select determines how widely the setting is applied. Lower levels inherit settings from higher levels. For example, when you apply a [policy](#) to the subscription, the policy is applied to all resource groups and resources in your subscription. When you apply a policy on the resource group, that policy is applied to the resource group and all its resources. However, another resource group doesn't have that policy assignment.

You can deploy templates to tenants, management groups, subscriptions, or resource groups.

A resource group is a **container** that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization.

**Generally, we add resources that share the same lifecycle to the same resource group so you can easily deploy, update, and delete them as a group.**

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

## Domain

Describe Azure architecture and services

## Question 2 Skipped

When you as a consumer are implementing a Software as a Service (SaaS) solution, you are responsible for **configuring high availability**.

Review the bolded text. If the statement is already correct, select "No change is needed". If the statement is incorrect, choose the option below that would make the statement correct.

### **No change is needed**

#### **Explanation**

The original statement is incorrect because as a consumer implementing a Software as a Service (SaaS) solution, you are indeed responsible for configuring high availability to ensure the service is accessible and reliable.

### **creating a resource group**

#### **Correct answer**

### **configuring the SaaS solution**

#### **Explanation**

Configuring the SaaS solution is the correct responsibility of the consumer when implementing a Software as a Service (SaaS) solution. This includes setting up redundancy, failover mechanisms, and load balancing to achieve high availability.

### **installing the SaaS solution**

#### **Explanation**

Installing the SaaS solution is not the responsibility of the consumer when implementing a Software as a Service (SaaS) solution. The consumer's role is focused on utilizing and configuring the service, not on the installation process.

#### **Overall explanation**

**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 (such as Microsoft Office 365).

SaaS provides a complete software solution that you purchase on a pay-as-you-go basis from a [cloud service provider](#). You rent the use of an app for your organization,

and your users connect to it over the Internet, usually with a web browser. All of the underlying infrastructure, middleware, app software, and app data are located in the service provider's data center. The service provider manages the hardware and software, and with the appropriate service agreement, will ensure the availability and the security of the app and your data as well. SaaS allows your organization to get quickly up and running with an app at minimal upfront cost.

If you've used a web-based email service such as Outlook, Hotmail, or Yahoo! Mail, then you've already used a form of **SaaS**. With these services, you log into your account over the Internet, often from a web browser. The email software is located on the service provider's network, and your messages are stored there as well. You can access your email and stored messages from a web browser on any computer or Internet-connected device.

The previous examples are free services for personal use. For organizational use, you can rent productivity apps, such as email, collaboration, and calendaring; and sophisticated business applications such as customer relationship management (CRM), enterprise resource planning (ERP), and document management. You pay for the use of these apps by **subscription** or according to the **level of use**.



**Reference :** <https://azure.microsoft.com/en-us/overview/what-is-saas/>

## Domain

Describe Cloud Concepts

## Question 3 Skipped

**How many levels of depth can a management group tree support, excluding the root level and the subscription level?**

**Correct answer**

### **Explanation**

This choice states that a management group tree can support up to 6 levels of depth, excluding the root level and the subscription level. This information is correct as Azure allows for a maximum depth of 6 levels in the management group tree.

**7**

### **Explanation**

This choice suggests that a management group tree can support up to 7 levels of depth, excluding the root level and the subscription level. However, this information is incorrect as the management group tree in Azure can support up to 6 levels of depth.

**4**

### **Explanation**

This choice suggests that a management group tree can support up to 4 levels of depth, excluding the root level and the subscription level. However, this information is incorrect as the management group tree in Azure can support more levels of depth.

**5**

### **Explanation**

According to this choice, a management group tree can support up to 5 levels of depth, excluding the root level and the subscription level. This information is incorrect as the management group tree in Azure can support more levels of depth.

### **Overall explanation**

A management group tree can support up to **6 levels** of depth. This limit doesn't include the root level or the subscription level.

**Reference:** <https://learn.microsoft.com/en-us/training/modules/describe-core-architectural-components-of-azure/6-describe-azure-management-infrastructure>

## Domain

Describe Azure management and governance

### Question 4 Skipped

**Azure Virtual Machines (VM) are classified as which of the following?**

**Correct answer**

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

#### Explanation

Azure Virtual Machines (VM) are classified as Infrastructure-as-a-Service (IaaS) because they provide virtualized computing resources, such as processing power, memory, and storage, over the internet. Users have full control over the operating system and applications running on the VM.

**Platform-as-a-Service (PaaS)**

#### Explanation

Platform-as-a-Service (PaaS) offerings in Azure, such as Azure App Service, provide a platform for developers to build, deploy, and manage applications without having to manage the underlying infrastructure. Azure Virtual Machines do not fall under this category as they require management of the operating system and applications.

**Software-as-a-Service (SaaS)**

#### Explanation

Software-as-a-Service (SaaS) offerings in Azure, such as Microsoft 365, provide software applications that are accessed over the internet. Azure Virtual Machines do not fall under this category as they provide infrastructure resources rather than pre-built software applications.

**Database-as-a-Service (DaaS)**

## Explanation

Database-as-a-Service (DaaS) offerings in Azure, such as Azure SQL Database, provide managed database services without the need to manage the underlying infrastructure. Azure Virtual Machines do not fall under this category as they are used for general-purpose computing rather than specialized database services.

## Overall explanation

According to the **official** Azure website, Azure VMs are classified as IaaS since you are renting out physical hardware. Refer to this image :

# Infrastructure as a Service Series: Virtual Machines and Windows

Posted on 25 June, 2012



Microsoft Azure

Name	Status
DebugVM	Running
Windows2012VM2	Running
Windows2012VM1	Running

We recently announced the release of [Windows Azure Virtual Machines](#), an Infrastructure-as-a-Service (IaaS) offering in [Windows Azure](#). I wanted to share my insights into how you can quickly start to use and best take advantage of this service.

Since I helped build it, I will warn you: I do love it!

## Virtual Machines Migration Patterns

At a glance, Virtual Machines (VMs) consist of **infrastructure to deploy an application**. Specifically, this includes a persistent OS disk, possibly some persistent data disks, and internal/external networking glue to hold it all together. Despite the boring list, with these infrastructure ingredients, the possibilities are so much more exciting...

**Read more about this:** <https://azure.microsoft.com/en-in/services/virtual-machines/#features>

## Domain

Describe Cloud Concepts

## Question 5 Skipped

**Which of the following factors can affect the availability of an Azure service under the SLA?**

**Correct selection**

## **Hardware or software failures within Azure**

### **Explanation**

Hardware or software failures within Azure can significantly impact the availability of Azure services and are covered under the SLA commitments. These failures can lead to service interruptions or outages, affecting the availability guarantees provided by Microsoft.

## **Network disruptions outside of Azure**

### **Explanation**

Network disruptions outside of Azure are not typically covered under the Azure SLA as they are considered external factors that are beyond Microsoft's control. While they can impact the availability of Azure services, they are not included in the SLA commitments.

### **Correct selection**

## **Planned maintenance activities**

### **Explanation**

Planned maintenance activities are a factor that can affect the availability of an Azure service under the SLA. During planned maintenance, Azure services may experience downtime or reduced performance, impacting the availability guarantees outlined in the SLA.

### **Correct selection**

## **Natural disasters**

### **Explanation**

Natural disasters such as earthquakes, floods, or severe weather events can disrupt Azure data centers and infrastructure, leading to service outages and impacting availability. While natural disasters are rare, they are considered a factor that can affect the availability of Azure services under the SLA.

## Overall explanation

The **Service Level Agreement (SLA)** for Azure services guarantees a certain level of availability, which is expressed as a percentage of uptime over a specific period of time. However, certain factors can affect the availability of an Azure service, even if it is covered under the SLA.

**Network disruptions outside of Azure**, such as issues with your own internet service provider (ISP), can impact your ability to connect to Azure services and can affect their availability. However, these types of disruptions are outside of Microsoft's control, so they are **NOT** considered in the Azure SLA.

**Planned maintenance activities**, which are performed to update or maintain Azure services, can cause temporary downtime. However, Microsoft typically schedules maintenance activities during off-peak hours to minimize their impact on availability.

**Hardware or software failures** within Azure can cause disruptions to service availability. Microsoft implements measures to minimize the impact of these failures, such as redundancy and failover mechanisms, but they can still occur.

**Natural disasters**, such as earthquakes or hurricanes, can also impact the availability of Azure services, but this is outside of Microsoft's control.

**Reference:** <https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?>

## Domain

Describe Azure management and governance

## Question 6 Skipped

Yes or No:

**When you create a resource group, you need to provide a location for that resource group.**

**No**

#### Correct answer

Yes

#### Explanation

Yes, when creating a resource group in Azure, you are required to specify a location for that resource group. The location determines the Azure region where the metadata for the resource group is stored, and it also dictates the data residency and compliance of the resources within that group.

#### Overall explanation

From the official Azure docs:

**When you create a resource group, you need to provide a location for that resource group.**

You may be wondering, "Why does a resource group need a location? And, if the resources can have different locations than the resource group, why does the resource group location matter at all?"

The resource group stores metadata about the resources. When you specify a location for the resource group, you're specifying where that metadata is stored. For compliance reasons, you may need to ensure that your data is stored in a particular region.

More info from the docs -

# Resource groups

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

- All the resources in your resource group should share the same lifecycle. You deploy, update, and delete them together. If one resource, such as a server, needs to exist on a different deployment cycle it should be in another resource group.
- Each resource can exist in only one resource group.
- You can add or remove a resource to a resource group at any time.
- You can move a resource from one resource group to another group. For more information, see [Move resources to new resource group or subscription](#).
- The resources in a resource group can be located in different regions than the resource group.
- When you create a resource group, you need to provide a location for that resource group.

You may be wondering, "Why does a resource group need a location? And, if the resources can have different locations than the resource group, why does the resource group location matter at all?"

The resource group stores metadata about the resources. When you specify a location for the resource group, you're specifying where that metadata is stored. For compliance reasons, you may need to ensure that your data is stored in a particular region.

If a resource group's region is temporarily unavailable, you can't update resources in the resource group because the metadata is unavailable. The resources in other regions will still function as expected, but you can't update them. This condition doesn't apply to global resources like Azure Content Delivery Network, Azure DNS, Azure Traffic Manager, and Azure Front Door.

For more information about building reliable applications, see [Designing reliable Azure applications](#).

- A resource group can be used to scope access control for administrative actions. To manage a resource group, you can assign [Azure Policies](#), [Azure roles](#), or [resource locks](#).
- You can [apply tags](#) to a resource group. The resources in the resource group don't inherit those tags.
- A resource can connect to resources in other resource groups. This scenario is common when the two resources are related but don't share the same lifecycle. For example, you can have a web app that connects to a database in a different resource group.
- When you delete a resource group, all resources in the resource group are also deleted. For information about how Azure Resource Manager orchestrates those deletions, see [Azure Resource Manager resource group and resource deletion](#).

**Reference:** <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal>

## Domain

Describe Azure management and governance

## Question 7 Skipped

**Which protocol does Microsoft Entra ID primarily use for single sign-on (SSO)?**

FTP

### **Explanation**

FTP (File Transfer Protocol) is primarily used for transferring files between a client and a server. It is not the protocol that Microsoft Entra ID uses for single sign-on (SSO) purposes.

### **HTTP**

### **Explanation**

HTTP (Hypertext Transfer Protocol) is a protocol used for transferring data over the web. While it is commonly used for web browsing, it is not the primary protocol used by Microsoft Entra ID for single sign-on (SSO) functionality.

### **Correct answer**

### **SAML**

### **Explanation**

SAML (Security Assertion Markup Language) is the correct protocol primarily used by Microsoft Entra ID for single sign-on (SSO). SAML enables secure authentication and authorization between identity providers and service providers.

### **SNMP**

### **Explanation**

SNMP (Simple Network Management Protocol) is used for network management and monitoring, not for single sign-on (SSO) authentication and authorization processes like Microsoft Entra ID.

### **Overall explanation**

Single sign-on (SSO) allows users to authenticate once and gain access to multiple applications without having to sign in separately to each one. Microsoft Entra ID supports SSO using several protocols, with SAML (Security Assertion Markup Language) being a primary one. SAML is an open standard that allows identity providers (like Entra ID) to pass authorization credentials to service providers (applications). This enables a seamless and secure user experience by allowing users to authenticate just once with the identity provider and gain access to multiple

services. Other protocols supported by Entra ID for SSO include OAuth and OpenID Connect.

**Reference:** <https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview>

## Domain

Describe Azure architecture and services

### Question 8 Skipped

**Your organization has an on-premise infrastructure. The requirement from senior management is to migrate everything to the cloud.**

As an advisor, what would you recommend to deal with an unexpected Azure outage in a Data Center / Availability Zone?

#### Using cheap resources to lose lesser money

##### Explanation

Using cheap resources to lose lesser money may not be the most effective strategy for dealing with an unexpected Azure outage in a Data Center or Availability Zone. It is important to focus on implementing fault tolerance and resilience measures to ensure business continuity in the event of an outage.

#### Scalability

##### Explanation

Scalability refers to the ability to increase or decrease resources based on demand. While scalability is important for handling increased workload, it may not directly address the issue of an unexpected Azure outage in a Data Center or Availability Zone.

#### Elasticity

##### Explanation

Elasticity is the ability to automatically adjust resources based on workload fluctuations. While elasticity is crucial for optimizing resource usage and cost efficiency, it may not specifically address the need for dealing with an unexpected Azure outage in a Data Center or Availability Zone.

#### Correct answer

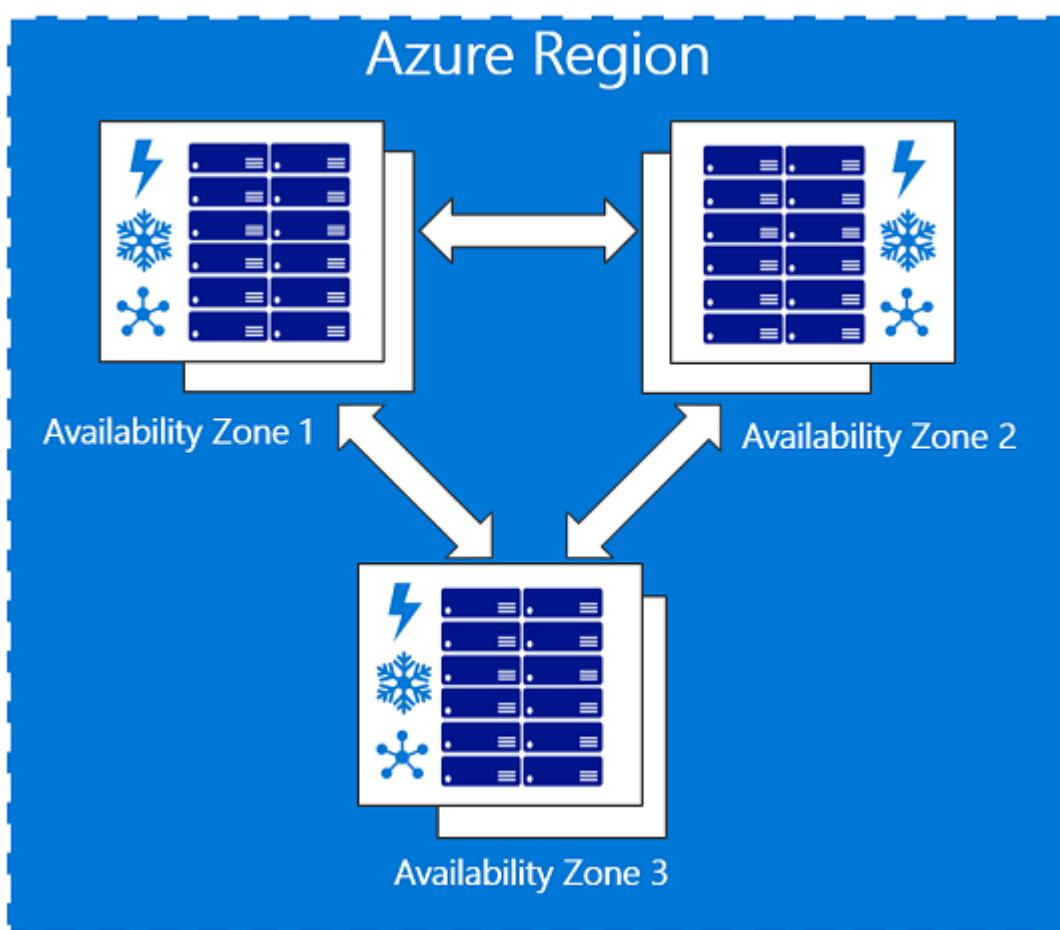
#### Fault Tolerance

#### Explanation

Fault Tolerance is the ability of a system to remain operational even when some of its components fail. Implementing fault tolerance measures such as redundancy, failover mechanisms, and backup systems can help mitigate the impact of an unexpected Azure outage in a Data Center or Availability Zone.

#### Overall explanation

There are several mechanisms built into Microsoft Azure to ensure services and applications remain available in the event of a failure. Such failures can include **hardware failures**, such as hard-disk crashes, or temporary **availability issues** of dependent services, such as storage or networking services. Azure and its software-controlled infrastructure are written in a way to anticipate and manage such failures.



In the event of a failure, the Azure infrastructure (**the Fabric Controller**) reacts immediately to restore services and infrastructure. For example, if a virtual machine (VM) fails due to a hardware failure on the physical host, the Fabric Controller moves that VM to another physical node based on the same hard disk stored in Azure storage. Azure is similarly capable of coordinating upgrades and updates in such a way as to avoid service downtime.

For **computing resources** (such as cloud services, traditional IaaS VMs, VM scale sets), the most important and fundamental concepts for enabling high availability are fault domains and upgrade domains. These have been part of Azure since its inception.

**Reference :** <https://azure.microsoft.com/en-us/blog/introducing-azure-availability-zones-for-resiliency-and-high-availability/>

## Domain

Describe Cloud Concepts

### Question 9 Skipped

A small startup is developing a custom e-commerce platform that requires *high scalability and flexibility to accommodate rapid growth*. Which cloud service model would be the most suitable for their initial development and deployment?

PaaS

Hybrid Cloud

SaaS

Correct answer

IaaS

## Overall explanation

**IaaS** (Infrastructure as a Service) provides the highest level of flexibility and control, allowing the startup to customize their infrastructure to meet their specific needs. They can scale resources up or down as required, and have full control over the operating system, applications, and data.

**Incorrect:**

**1. PaaS** (Platform as a Service) offers a pre-built platform for application development, but it might be restrictive for a startup that requires a highly customized e-commerce platform.

**2. SaaS** (Software as a Service) provides a complete application, which is not suitable for a startup developing its own platform.

**3. Hybrid Cloud** combines IaaS and PaaS, but it's overkill for a startup in its initial stages.

**Reference:** <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-iaas>

**Domain**

Describe Cloud Concepts

**Question 10 Skipped**

**What is the primary goal of the defense-in-depth model in cybersecurity?**

**Correct answer**

**To establish multiple layers of security controls to mitigate risks.**

**Explanation**

The primary goal of the defense-in-depth model in cybersecurity is to establish multiple layers of security controls to mitigate risks. By implementing a layered approach to security, organizations can better protect their systems, data, and assets from a wide range of cyber threats and attacks.

## **To outsource security responsibilities to third-party providers.**

### **Explanation**

The defense-in-depth model in cybersecurity does not involve outsourcing security responsibilities to third-party providers as the primary goal. While organizations may choose to work with third-party providers for certain security services, the defense-in-depth model focuses on building internal capabilities and implementing multiple layers of security controls to enhance overall cybersecurity.

## **To focus solely on physical security measures for data centers.**

### **Explanation**

Focusing solely on physical security measures for data centers is not the primary goal of the defense-in-depth model in cybersecurity. While physical security is an important aspect of overall security, the defense-in-depth model emphasizes the need for multiple layers of security controls to address various types of threats and vulnerabilities.

## **To create a single layer of security controls to prevent all threats.**

### **Explanation**

The defense-in-depth model in cybersecurity aims to establish multiple layers of security controls to mitigate risks, rather than relying on a single layer of security controls to prevent all threats. This approach helps to increase the overall security posture of an organization by adding redundancy and resilience to the security measures in place.

### **Overall explanation**

The defense-in-depth model involves implementing a series of security layers, each providing a different type of protection against threats. This approach minimizes the impact of a single security breach by adding multiple lines of defense.

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

## Domain

Describe Azure architecture and services

### Question 11 Skipped

**Which of the following services can automatically sign users in when they are on their corporate devices & connected to your corporate network?**

**Password Auth**

#### Explanation

Password Auth refers to the traditional method of using a username and password to authenticate users. While it is a common authentication method, it does not automatically sign users in when they are on their corporate devices and connected to the corporate network.

**Correct answer**

**Single-Sign-On (SSO)**

#### Explanation

Single-Sign-On (SSO) is a service that allows users to access multiple applications with one set of login credentials. It can automatically sign users in when they are on their corporate devices and connected to the corporate network, providing a seamless user experience.

**Multi-Factor Authentication (MFA)**

#### Explanation

Multi-Factor Authentication (MFA) is a security feature that requires users to provide multiple forms of verification before accessing a resource. While it enhances security, it does not automatically sign users in when they are on their corporate devices and connected to the corporate network.

**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. It is not related to automatically signing users in when they are on their corporate devices and connected to the corporate network.

## Overall explanation

From the official documentation: **Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO)** automatically signs users in when they are on their corporate devices connected to your corporate network. When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.

**With single sign-on**, users sign in once with one account to access domain-joined devices, company resources, software as a service (SaaS) applications, and web applications. After signing in, the user can launch applications from the Office 365 portal or the Azure AD MyApps access panel. Administrators can centralize user account management, and automatically add or remove user access to applications based on group membership.

**Reference :** <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on>

## Domain

Describe Azure architecture and services

## Question 12 Skipped

**Which of the following affect costs in Azure? (Choose 2)**

### Availability Zone

## Explanation

Availability Zones in Azure are designed for high availability and fault tolerance, but they do not directly impact costs. While using Availability Zones may incur additional costs for redundancy and resiliency, it is not a direct factor that affects costs in Azure.

#### **Correct selection**

##### **Location**

#### **Explanation**

The location of resources in Azure can impact costs due to differences in pricing based on regions and data transfer costs between regions. Choosing a specific location for your resources can affect the overall cost of running services in Azure.

#### **Correct selection**

##### **Instance size**

#### **Explanation**

The instance size of virtual machines or other resources in Azure directly affects costs. Larger instance sizes typically come with higher costs, so selecting the appropriate instance size based on your workload requirements is crucial for cost optimization in Azure.

#### **Knowledge center usage**

#### **Explanation**

Knowledge center usage is not a factor that directly affects costs in Azure. Knowledge center usage refers to accessing documentation, guides, and resources for learning about Azure services, which is not related to cost considerations for running resources in Azure.

#### **Overall explanation**

##### **According to the official docs:**

The instance size and the location (eg -US or Europe etc ) affect the prices. The knowledge center is completely free to use, and you aren't charged for an Availability

Zone.

**Reference :** <https://azure.microsoft.com/en-us/pricing/>

### Domain

Describe Azure management and governance

### Question 13 Skipped

**A large enterprise with a complex IT infrastructure wants to migrate its legacy on-premises applications to the cloud without significant changes to its existing environment. Which cloud service model would be the best choice for this migration?**

**Hybrid Cloud**

**SaaS**

**Correct answer**

**IaaS**

**PaaS**

### Overall explanation

**IaaS** provides the **most** flexibility to replicate an on-premises environment in the cloud. The enterprise can migrate its servers and applications with minimal changes to the underlying infrastructure.

### Incorrect:

1. **PaaS** and **SaaS** involve significant changes to the application environment, which is not ideal for migrating legacy applications.

2. **Hybrid Cloud** might be considered if the enterprise wants to keep some applications on-premises, but the primary focus here is on migrating existing applications, making IaaS the best choice.

**Reference:** <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-iaas>

## Domain

Describe Cloud Concepts

### Question 14 Skipped

**A small development team is building a proof-of-concept (POC) for a new mobile application. The team needs a flexible environment to experiment with different technologies and frameworks rapidly. Which cloud service model would best support this?**

**Correct answer**

**PaaS**

#### Explanation

Platform as a Service (PaaS) is the best cloud service model for a small development team building a proof-of-concept for a new mobile application. PaaS offers a flexible environment where developers can focus on building and deploying applications without worrying about managing the underlying infrastructure. It allows for rapid experimentation with different technologies and frameworks.

**SaaS**

#### Explanation

Software as a Service (SaaS) provides ready-to-use software applications over the internet. While SaaS is convenient for end-users, it may not be the ideal choice for a development team looking to experiment with different technologies and frameworks rapidly as it does not offer the level of flexibility and control provided by PaaS.

**Hybrid Cloud**

## Explanation

Hybrid Cloud is a combination of public and private cloud environments. While it offers flexibility in terms of workload placement and data management, it may not be the best choice for a small development team building a proof-of-concept for a new mobile application that requires a flexible environment for rapid experimentation with different technologies and frameworks.

## IaaS

### Explanation

Infrastructure as a Service (IaaS) provides virtualized computing resources over the internet. While it offers flexibility in terms of scalability and resource management, it may not be the best choice for a small development team looking to experiment with different technologies and frameworks rapidly as it still requires managing and maintaining the underlying infrastructure.

## Overall explanation

**PaaS** provides a rapid development environment with pre-configured tools and services, allowing the development team to experiment with different technologies without managing the underlying infrastructure.

Incorrect answers:

1. **IaaS** requires more setup and management for rapid prototyping.
2. **SaaS** is for delivering complete applications, not for building POCs.
3. **Hybrid Cloud** might be considered for specific components, but PaaS is generally the best choice for rapid prototyping.

**Reference:** <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-paas/>

## Domain

Describe Cloud Concepts

## **Question 15 Skipped**

**Which cloud service model places the greatest responsibility on the customer for security?**

**Correct answer**

**IaaS**

### **Explanation**

Infrastructure as a Service (IaaS) places the greatest responsibility on the customer for security, as they are responsible for securing the virtual machines, operating systems, applications, and data running on the cloud infrastructure provided by the service provider.

**All models share equal responsibility**

### **Explanation**

All cloud service models do not share equal responsibility for security. Each model has a different level of responsibility assigned to the customer, with IaaS typically placing the most responsibility on the customer for security.

**SaaS**

### **Explanation**

Software as a Service (SaaS) places the least responsibility on the customer for security, as the service provider is responsible for securing the application and data. Customers typically only need to secure their own data and access to the application.

**PaaS**

### **Explanation**

Platform as a Service (PaaS) places some responsibility on the customer for security, as they are responsible for securing their applications and data, while the service provider manages the underlying infrastructure and platform.

## Overall explanation

IaaS provides the **least** amount of managed services, meaning the customer has the **most** responsibility for security, including operating system patching, application security, and data protection.

**Reference:** <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

## Domain

Describe Cloud Concepts

### Question 16 Skipped

**Which of the following services provides a personalized view of the health of the Azure services, regions, and resources you rely on?**

#### Azure Monitor

##### Explanation

Azure Monitor is a platform service that provides a comprehensive solution for collecting, analyzing, and acting on telemetry data from Azure and other sources. While it can provide insights into the performance and health of resources, it does not offer a personalized view like Azure Service Health.

#### Azure Advisor

##### Explanation

Azure Advisor is a personalized guide to Azure best practices that analyzes your Azure usage and configurations to provide recommendations for improving security, performance, and cost efficiency. It does not specifically focus on providing a view of the health of Azure services and resources.

#### Azure Resource Health

##### Explanation

Azure Resource Health provides information about the current and past health of individual Azure resources. It does not offer a personalized view of the overall health of Azure services, regions, and resources.

#### Correct answer

### Azure Service Health

#### Explanation

Azure Service Health provides a personalized view of the health of Azure services, regions, and resources that you rely on. It offers proactive notifications and guidance when Azure service issues affect you.

#### Overall explanation

#### From the Official Azure Documentation:

[Azure Service Health](#) provides a personalized view of the health of the Azure services, regions, and resources you rely on. The status.azure.com website, which displays only major issues that broadly affect Azure customers, doesn't provide the full picture. But Azure Service Health displays both major and smaller, localized issues that affect you. Service issues are rare, but it's important to be prepared for the unexpected. You can set up alerts that help you triage outages and planned maintenance. After an outage, Service Health provides official incident reports, called root cause analyses (RCAs), which you can share with stakeholders.

**Reference:** <https://docs.microsoft.com/en-ca/learn/modules/monitoring-fundamentals/2-identify-product-options>

#### Domain

Describe Azure management and governance

#### Question 17 Skipped

**You want to deploy a file share that can be accessed from multiple Azure virtual machines without setting up a separate file server. Which Azure service can you use to achieve this?**

**Correct answer**

## Azure Storage Account

### Explanation

Azure Storage Account is the correct choice for deploying a file share that can be accessed from multiple Azure virtual machines. Azure Storage provides scalable, secure, and highly available storage solutions, including Azure File Shares, which can be mounted as network drives on virtual machines.

## Azure Virtual Network

### Explanation

Azure Virtual Network is used to create isolated networks in Azure, allowing resources to communicate securely with each other. While it is essential for connecting resources within a virtual network, it does not provide file sharing capabilities like Azure Storage Account.

## Azure App Service

### Explanation

Azure App Service is a platform-as-a-service (PaaS) offering for hosting web applications, mobile backends, and RESTful APIs. It is not designed for file sharing or serving as a file server for multiple virtual machines to access files.

## Azure SQL Database

### Explanation

Azure SQL Database is a fully managed relational database service that is used for storing and managing structured data. It is not designed for file sharing or serving as a file server for multiple virtual machines to access files.

## Overall explanation

This is a tricky question. **Azure Storage Account** is the correct answer as it provides Azure Files, which can be used to create a file share accessible from multiple virtual machines. Remember, we always need to choose the BEST option from the ones provided. Even though Azure Files would've been the ideal option, but since its not one of the options we need to go with the best option possible.

Other Options:

- **Azure SQL Database** is a database service and not suitable for sharing files among multiple virtual machines.
- **Azure Virtual Network** is a networking service and not suitable for file sharing.
- **Azure App Service** is a platform for hosting web applications and not suitable for file sharing.

**Reference:** <https://azure.microsoft.com/en-us/products/storage/files/>

## Domain

Describe Azure architecture and services

## Question 18 Skipped

**A customer is using an Infrastructure as a Service (IaaS) model. Which of the following is primarily the customer's responsibility?**

**Protecting the underlying network infrastructure**

### Explanation

Protecting the underlying network infrastructure is typically the responsibility of the cloud service provider in an Infrastructure as a Service (IaaS) model. The provider is responsible for ensuring the security and availability of the network infrastructure that supports the virtual machines.

**Ensuring the availability of the cloud platform**

### Explanation

Ensuring the availability of the cloud platform is primarily the responsibility of the cloud service provider in an Infrastructure as a Service (IaaS) model. The provider is responsible for maintaining the overall availability and performance of the cloud platform, including the underlying infrastructure and services.

#### **Correct answer**

### **Patching the operating system of virtual machines**

#### **Explanation**

Patching the operating system of virtual machines is primarily the customer's responsibility in an Infrastructure as a Service (IaaS) model. Customers are responsible for maintaining and updating the software and operating systems running on the virtual machines they deploy in the cloud.

### **Securing the physical data center**

#### **Explanation**

Securing the physical data center is primarily the responsibility of the cloud service provider in an Infrastructure as a Service (IaaS) model. The customer is not responsible for securing the physical infrastructure where the virtual machines are hosted.

#### **Overall explanation**

In IaaS, the customer has more responsibility for managing the operating system and applications. Patching the operating system is a crucial security measure that falls under the customer's purview.

**Reference:** <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

#### **Domain**

Describe Cloud Concepts

## Question 19 Skipped

**Is it possible for anyone to modify an Azure resource that has a delete lock applied to it?**

**No, a delete lock prevents all users from modifying or deleting the resource**

### Explanation

A delete lock prevents the deletion of a resource, but it does not prevent modifications. Users, including administrators, can still make changes to the resource even with a delete lock applied.

**No, but a delete lock can be temporarily disabled to make modifications**

### Explanation

While it is true that a delete lock can be temporarily disabled to make modifications, it is not necessary to disable the lock to modify the resource. Administrators can make modifications to the resource without disabling the delete lock.

### Correct answer

**Yes, it is possible for the admin to do so**

### Explanation

Yes, it is possible for the admin to modify an Azure resource that has a delete lock applied to it. Delete locks prevent accidental deletion of a resource, but they do not restrict modifications by administrators who have the necessary permissions.

**Yes, but only by users with the least privileges**

### Explanation

This statement is incorrect. Users with the least privileges may not have the necessary permissions to modify an Azure resource with a delete lock applied to it. Delete locks are primarily for preventing accidental deletions, not modifications.

## Overall explanation

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

## Question 20 Skipped

**You want to restrict access to certain Azure resources based on departmental requirements within your organization. Which Azure feature would you use?**

### Resource groups

### Explanation

Resource groups are containers that hold related resources for an Azure solution. While they can help organize and manage resources, they do not provide the level of access control needed to restrict access based on departmental requirements within an organization.

### Correct answer

### Subscriptions

## **Explanation**

Subscriptions in Azure provide a way to group and manage resources, billing, and access control. By using subscriptions, you can set permissions and access controls at the subscription level to restrict access to certain Azure resources based on departmental requirements within your organization.

## **Microsoft Entra ID**

### **Explanation**

Azure Active Directory (AAD) is a cloud-based identity and access management service that helps your employees sign in and access resources. While AAD is essential for managing user identities and access to Azure resources, it is not specifically designed to restrict access to certain Azure resources based on departmental requirements within an organization.

## **Management groups**

### **Explanation**

Management groups are containers that help you manage access, policies, and compliance for multiple subscriptions. While they can be used to enforce governance controls across subscriptions, they do not directly restrict access to specific Azure resources based on departmental requirements.

## **Overall explanation**

In this scenario, you would use **subscriptions** to restrict access to certain Azure resources based on departmental requirements. Subscriptions can be used to apply different access-management policies, reflecting different organizational structures. Azure applies access-management policies at the subscription level, which allows you to manage and control access to the resources that users provision within specific subscriptions.

## **Other options -**

- **Resource groups:** Resource groups are primarily used to organize resources that are related to the same project or have the same lifecycle. They are not specifically designed for access control based on departmental requirements.

- **Management groups:** Management groups are used to efficiently manage access, policies, and compliance for multiple subscriptions, providing a level of scope above subscriptions. They are more suitable for large-scale governance rather than restricting access based on departmental requirements.
- **Azure Active Directory:** While Azure Active Directory (Azure AD) is responsible for handling authentication and authorization, it alone cannot restrict access to certain Azure resources based on departmental requirements. Instead, Azure AD is used in conjunction with other features like subscriptions to control access.

**Reference:** <https://learn.microsoft.com/en-us/training/modules/describe-core-architectural-components-of-azure/6-describe-azure-management-infrastructure>

## Domain

Describe Azure management and governance

## Question 21 Skipped

**Which of the following services would you help achieve the following:**

- 1) Create and manage a group of load balanced VMs.
- 2) Provide high availability and application resiliency by distributing VMs across availability zones
- 3) Allows your application to automatically scale as resource demand changes

## Azure Region Pairs

### Explanation

Azure Region Pairs are used for pairing Azure regions for data residency, compliance, and disaster recovery purposes. They do not directly relate to creating and managing a group of load balanced VMs, providing high availability, or enabling automatic scaling for applications.

**Correct answer**

## Azure Scale Sets

## **Explanation**

Azure Scale Sets allow you to create and manage a group of load balanced VMs, providing high availability and application resiliency by distributing VMs across availability zones. They also enable your application to automatically scale as resource demand changes, making them the correct choice for the given requirements.

## **Azure Resource Groups**

### **Explanation**

Azure Resource Groups are logical containers that hold related resources for an Azure solution. While they help manage and organize Azure resources, they do not specifically address the requirements of creating and managing a group of load balanced VMs, providing high availability, or enabling automatic scaling for applications.

## **Azure Subscriptions**

### **Explanation**

Azure Subscriptions are used to manage billing, access control, and resource limits for Azure services. They are not directly related to creating and managing a group of load balanced VMs, providing high availability, or enabling automatic scaling for applications.

## **Overall explanation**

**A great article from the official Microsoft documentation:**

# What are virtual machine scale sets?

Article • 07/11/2022 • 3 minutes to read • 11 contributors



Azure virtual machine scale sets let you create and manage a group of load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide the following key benefits:

- Easy to create and manage multiple VMs
- Provides high availability and application resiliency by distributing VMs across availability zones or fault domains
- Allows your application to automatically scale as resource demand changes
- Works at large-scale

With Flexible orchestration, Azure provides a unified experience across the Azure VM ecosystem. Flexible orchestration offers high availability guarantees (up to 1000 VMs) by spreading VMs across fault domains in a region or within an Availability Zone. This enables you to scale out your application while maintaining fault domain isolation that is essential to run quorum-based or stateful workloads, including:

**Reference :** <https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/overview>

## Domain

Describe Azure architecture and services

## Question 22 Skipped

### How does Defender for Cloud contribute to the security of Azure-native services?

#### Correct answer

**By natively integrating with Azure services to provide monitoring and protection.**

#### Explanation

This choice is correct because Defender for Cloud natively integrates with Azure services to provide monitoring and protection. It leverages Azure's capabilities to secure Azure-native services and resources, offering comprehensive security features within the Azure environment.

**By focusing solely on Azure App Service protection.**

### **Explanation**

Defender for Cloud does not solely focus on Azure App Service protection. It provides security monitoring and protection for a wide range of Azure services beyond just Azure App Service.

### **By enforcing access controls on physical hardware.**

### **Explanation**

Defender for Cloud does not enforce access controls on physical hardware. Instead, it focuses on securing Azure-native services and resources within the Azure cloud environment.

### **By automatically deploying Log Analytics agents to Azure machines.**

### **Explanation**

Defender for Cloud does not automatically deploy Log Analytics agents to Azure machines. While Log Analytics may be used for monitoring and analysis, Defender for Cloud itself natively integrates with Azure services to provide security monitoring and protection.

### **Overall explanation**

Defender for Cloud, being an Azure-native service, natively integrates with Azure services, monitoring and protecting them without requiring additional deployment. This integration enhances the security posture of Azure resources.

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

### **Domain**

Describe Azure architecture and services

### **Question 23 Skipped**

\_\_\_\_\_ is the mission-critical cloud, delivering breakthrough innovation to US government customers and their partners. Only US federal, state, local, and tribal governments and their partners have access to this dedicated instance, with operations controlled by screened US citizens.

Azure United States

Correct answer

Azure Government

Azure Nation

Azure US

### Overall explanation

From the official docs:

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

Reference: <https://en-us/global-infrastructure/government/get-started/>

### Domain

Describe Azure architecture and services

### Question 24 Skipped

Yes or No:

**Deleting a resource groups deletes all the resources inside it as well.**

**No**

**Correct answer**

**Yes**

### **Explanation**

Yes, deleting a resource group in Azure will also delete all the resources contained within that resource group. This includes virtual machines, storage accounts, databases, and any other resources provisioned within the resource group. It is important to be cautious when deleting a resource group as it will result in the permanent deletion of all resources within it.

### **Overall explanation**

#### **From the Azure official docs:**

Deleting the resource group will **remove** the resource group **as well as all the resources** in that resource group. This can be useful for the management of resources. For example, a virtual machine has several components (the VM itself, virtual disks, network adapter etc.).

By placing the VM in its own resource group, you can delete the VM along with all its associated components by deleting the resource group.

Another example is when creating a test environment. You could place the entire test environment (Network components, virtual machines etc.) in one resource group. You can then delete the entire test environment by deleting the resource group.

**Reference:** <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal>

### **Domain**

Describe Azure management and governance

### **Question 25 Skipped**

**Yes or no:**

**All resource types support Tags in Azure.**

**Yes**

**Correct answer**

**No**

### **Explanation**

Not all resource types in Azure support Tags. Some resource types may not have the capability to have Tags applied to them. It is essential to understand which resource types allow for the use of Tags and which do not in Azure.

### **Overall explanation**

No, according to the official documentation, Tags **CANNOT** be applied to all resource types. See below:

## **Limitations**

The following limitations apply to tags:

- Not all resource types support tags. To determine if you can apply a tag to a resource type, see [Tag support for Azure resources](#).
- Management groups currently don't support tags.

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

### **Domain**

Describe Azure architecture and services

## Question 26 Skipped

Your company plans to deploy multiple Virtual Machines in Azure. As the lead architect, you must ensure that all these virtual machines are available if a single data center fails.

**Solution: You deploy the virtual machines to two or more Availability Zones.**

Would this solution meet the goal?

**Correct answer**

**Yes**

### Explanation

Yes, deploying the virtual machines to two or more Availability Zones in Azure would meet the goal of ensuring availability in case a single data center fails. Availability Zones are physically separate data centers within an Azure region, each with its own power, cooling, and networking. By distributing the virtual machines across multiple Availability Zones, you can achieve higher availability and resilience to failures.

**No**

### Overall explanation

Absolutely! The answer is in the question itself. If one data center goes down, we can make sure our VM is still running in another data center. This is the entire concept of fault tolerance - Make sure you have enough backups to prevent downtime.

### Availability Zones -

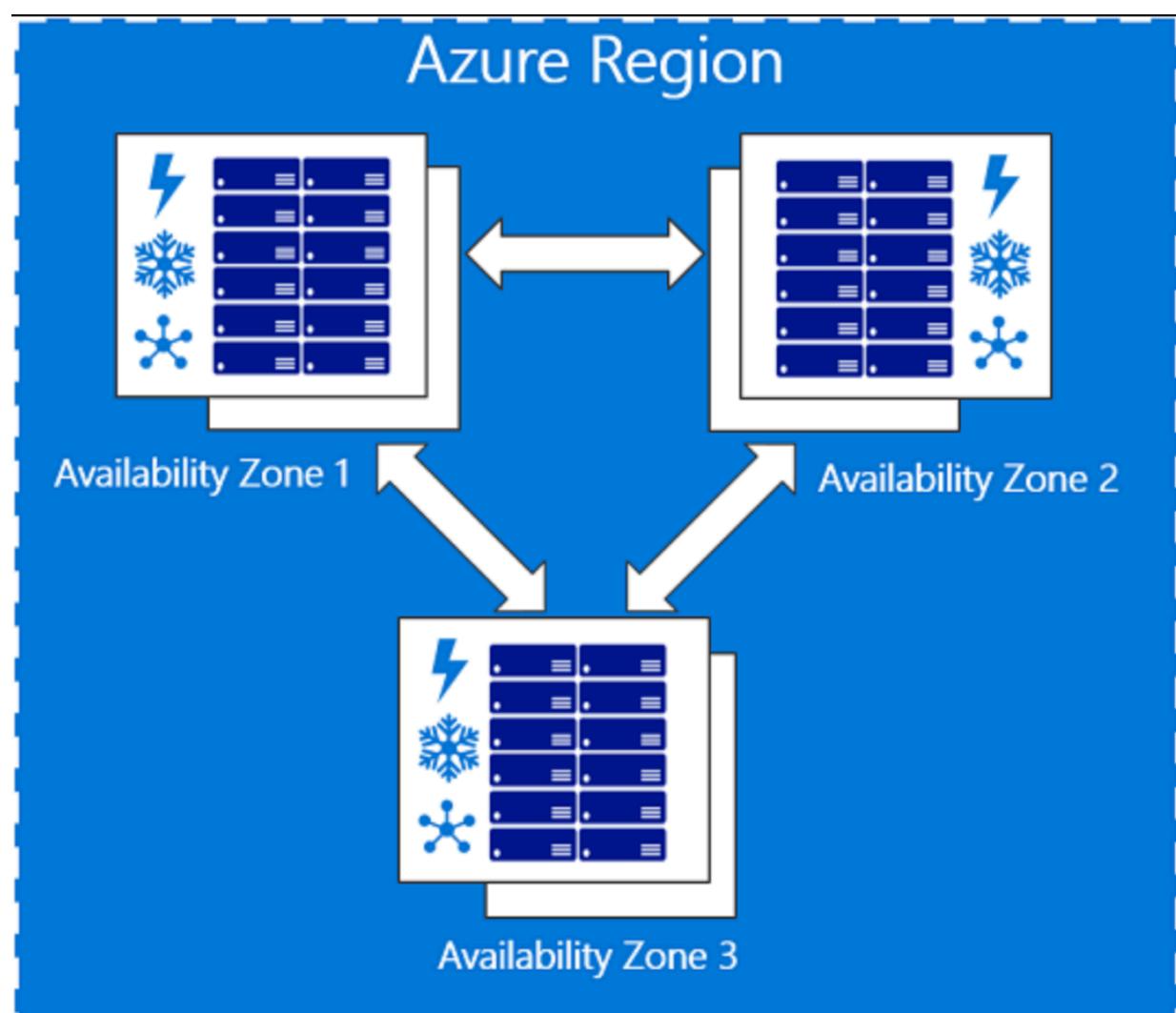
- An Availability Zone is a high-availability offering that protects your applications and data from datacenter failures. Availability Zones are **unique physical locations** within an Azure region. Each zone is made up of one or more datacenters equipped with **independent power, cooling, and networking (VERY IMPORTANT PLEASE NOTE)**.
- To ensure resiliency, there's a minimum of **three** separate zones in all enabled regions. The physical separation of Availability Zones within a region protects applications and data from datacenter failures. Zone-redundant services

replicate your applications and data across Availability Zones to protect from single-points-of-failure. With Availability Zones, Azure offers **industry best 99.99% VM uptime SLA**.

Azure services that support Availability Zones fall into two categories:

- 1) Zonal services** – where a resource is pinned to a specific zone (for example, virtual machines, managed disks, Standard IP addresses), or
- 2) Zone-redundant services** – when the Azure platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).

To achieve comprehensive business continuity on Azure, build your application architecture using the combination of Availability Zones with Azure region pairs. You can synchronously replicate your applications and data using Availability Zones within an Azure region for high-availability and asynchronously replicate across Azure regions for disaster recovery protection.



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

## Domain

Describe Cloud Concepts

### Question 27 Skipped

**How does the defense-in-depth model enhance cybersecurity compared to relying solely on perimeter security?**

**It reduces the need for user authentication.**

#### Explanation

The defense-in-depth model does not reduce the need for user authentication; in fact, it emphasizes the importance of multi-factor authentication and other security measures to protect against unauthorized access.

**It eliminates the need for regular security updates.**

#### Explanation

The defense-in-depth model does not eliminate the need for regular security updates. In fact, it emphasizes the importance of keeping systems and software up to date with the latest security patches to address vulnerabilities and protect against emerging threats. Regular security updates are a critical component of a comprehensive cybersecurity strategy.

#### Correct answer

**It provides protection against both external and internal threats.**

#### Explanation

The defense-in-depth model provides protection against both external threats, such as cyberattacks from outside the organization, and internal threats, such as insider threats or accidental data breaches. By implementing multiple layers of security controls, organizations can better defend against a wide range of cybersecurity risks.

**It isolates the network from the internet entirely.**

## Explanation

While the defense-in-depth model may include network segmentation to isolate critical assets, it does not completely isolate the network from the internet. It focuses on creating multiple layers of security controls to protect against various types of threats.

## Overall explanation

The defense-in-depth model focuses on multiple layers of security, including internal defenses. This strategy provides safeguards against both external threats (outside attackers) and internal threats (compromised insiders).

The remaining options don't make any sense and rather **reduce** the security configuration.

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

## Domain

Describe Azure architecture and services

## Question 28 Skipped

**Which of the following is an accurate description of Azure ExpressRoute?**

**A service that enables you to manage and monitor Azure resources from a single, unified dashboard.**

## Explanation

Managing and monitoring Azure resources from a single, unified dashboard is a function of Azure Monitor and Azure Management Portal, not Azure ExpressRoute. Azure ExpressRoute is specifically designed for establishing private network connections between on-premises infrastructure and Azure.

**A service that provides backup and disaster recovery solutions for Azure resources.**

## Explanation

Backup and disaster recovery solutions for Azure resources are typically provided by services like Azure Backup and Azure Site Recovery, not Azure ExpressRoute. Azure ExpressRoute is focused on network connectivity rather than data protection.

## Correct answer

**A service that provides dedicated, private network connectivity between your on-premises infrastructure and Azure datacenters.**

## Explanation

Azure ExpressRoute is a service that offers dedicated, private network connectivity between your on-premises infrastructure and Azure datacenters. This allows for a more secure and reliable connection compared to using the public internet.

**A service that allows you to connect your on-premises infrastructure to Azure over the public internet.**

## Explanation

Connecting your on-premises infrastructure to Azure over the public internet is typically done through VPN gateways, not Azure ExpressRoute. Azure ExpressRoute provides a dedicated, private network connection for more secure and reliable connectivity.

## Overall explanation

**Azure ExpressRoute** is a service that provides dedicated, private network connectivity between your on-premises infrastructure and Azure datacenters. This allows you to extend your on-premises network into Azure, providing a more secure and reliable connection than the public internet.

- **A service that allows you to connect your on-premises infrastructure to Azure over the public internet:** This is incorrect because Azure ExpressRoute does not use the public internet for connectivity. Instead, it provides a private, dedicated connection.
- **A service that provides backup and disaster recovery solutions for Azure resources:** This is incorrect because Azure ExpressRoute is not specifically

designed for backup and disaster recovery. While it can be used in conjunction with these solutions, it is primarily used for private connectivity.

- **A service that enables you to manage and monitor Azure resources from a single, unified dashboard:** This is incorrect because Azure ExpressRoute is not a management or monitoring tool for Azure resources. It is a connectivity service that enables you to extend your on-premises network into Azure.

**Reference:** <https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction>

### Domain

Describe Azure architecture and services

### Question 29 Skipped

**Which of the following factors influence the cost of Azure resources? (Select all that apply)**

**Correct selection**

**Consumption**

### Explanation

Consumption refers to the amount of usage or resources consumed within Azure. The more resources you use or the higher the usage, the higher the cost will be. Monitoring and optimizing consumption can help control costs.

**Correct selection**

**Resource type**

### Explanation

The type of Azure resource being used directly impacts its cost. Different resource types have varying pricing structures and cost models, so choosing the right resource type is essential for managing costs effectively.

## Maintenance

### Explanation

Maintenance costs are not directly related to the cost of Azure resources. While maintenance activities may incur additional costs, they are not a factor that directly influences the cost of using Azure resources.

### Correct selection

### Geography

### Explanation

The geographic location where Azure resources are deployed can impact their cost. Different regions may have different pricing for resources, and data transfer costs can vary based on the distance between regions. Choosing the right geography for resource deployment can help optimize costs.

### Overall explanation

The correct answers are - **Resource type, Consumption, and Geography**. These factors influence the cost of Azure resources. Maintenance, on the other hand, is an important aspect of managing resources to control costs but does not directly influence the cost of the resources themselves.

**Reference:** <https://learn.microsoft.com/en-us/training/modules/describe-cost-management-azure/2-describe-factors-affect-costs-azure>

### Domain

Describe Azure management and governance

### Question 30 Skipped

**Which of the following is NOT a benefit of using Microsoft Entra ID?**

### Correct answer

## **Unlimited data storage**

### **Explanation**

Unlimited data storage is not a benefit of using Microsoft Entra ID. While Microsoft Entra ID provides centralized identity management, simplified access to applications, and enhanced security features, it does not offer unlimited data storage as a feature.

## **Enhanced security with multi-factor authentication**

### **Explanation**

Microsoft Entra ID enhances security by offering multi-factor authentication, which adds an extra layer of protection to user accounts. This additional security measure helps prevent unauthorized access and protects sensitive data from potential security threats.

## **Centralized identity management**

### **Explanation**

Microsoft Entra ID provides centralized identity management, allowing users to access multiple applications and services with a single set of credentials. This centralization simplifies user management and enhances security by reducing the risk of unauthorized access.

## **Simplified access to applications**

### **Explanation**

Microsoft Entra ID simplifies access to applications by providing a seamless and consistent authentication experience for users. It eliminates the need for multiple sets of credentials and allows users to access applications easily and securely.

## **Overall explanation**

**Microsoft Entra ID** provides several benefits, including centralized identity management, simplified access to applications through single sign-on, and enhanced security with features like multi-factor authentication and conditional access. However, it is not designed to offer unlimited data storage. Entra ID focuses on

identity and access management rather than data storage. For unlimited data storage, organizations would typically use other Azure services like Azure Blob Storage or Azure SQL Database. Therefore, while Entra ID significantly enhances identity and access security, it does not address data storage needs directly.

**Reference:** <https://www.microsoft.com/en-ca/security/business/identity-access/microsoft-entra-id>

## Domain

Describe Azure architecture and services

### Question 31 Skipped

**A medium-sized business is looking to migrate its customer relationship management (CRM) system to the cloud. The business requires customization options but also wants to minimize the IT overhead associated with managing the underlying infrastructure. Which cloud service model would be most suitable?**

**Correct answer**

**PaaS**

#### Explanation

PaaS (Platform as a Service) would be the most suitable cloud service model for the medium-sized business in this scenario. PaaS offers customization options for developing, testing, and deploying applications without the need to manage the underlying infrastructure. This helps minimize IT overhead while still allowing for customization of the CRM system.

**IaaS**

#### Explanation

IaaS (Infrastructure as a Service) provides businesses with virtualized computing resources over the internet. While it offers customization options, it still requires the business to manage the underlying infrastructure, which may not align with the goal of minimizing IT overhead for the medium-sized business looking to migrate its CRM system to the cloud.

## Hybrid Cloud

### Explanation

Hybrid Cloud combines on-premises infrastructure with public or private cloud services. While it offers flexibility and customization options, it may not necessarily minimize IT overhead, as managing a hybrid cloud environment can be complex and require additional resources. For the medium-sized business looking to reduce IT overhead, a different cloud service model like PaaS would be more suitable.

## SaaS

### Explanation

SaaS (Software as a Service) provides businesses with access to software applications over the internet. While SaaS solutions are fully managed and require minimal IT overhead, they may not offer the level of customization options required by the medium-sized business for its CRM system migration.

### Overall explanation

**PaaS** offers a balance between customization and managed infrastructure. It provides a platform for developing and deploying applications, allowing the business to customize the CRM system to their needs without managing the underlying infrastructure.

### Incorrect:

**1. IaaS** gives full control but also requires managing the entire infrastructure, which is contrary to the business' desire to minimize IT overhead.

**2. SaaS** typically offers limited customization options, as the CRM system is pre-built.

**3. Hybrid Cloud** might be considered if the business has existing on-premises CRM components, but for a full migration, PaaS is often the best choice.

**Reference:** <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-paas/>

## Domain

Describe Cloud Concepts

### Question 32 Skipped

**What is the significance of implementing security controls at the "data" layer in the defense-in-depth model?**

**It reduces the impact of denial of service (DoS) attacks.**

#### Explanation

While implementing security controls at the "data" layer may indirectly reduce the impact of denial of service (DoS) attacks by ensuring data availability, the primary purpose of these controls is to protect sensitive data and maintain its confidentiality, integrity, and availability.

**It prevents network-based attacks against resources.**

#### Explanation

Implementing security controls at the "data" layer does not directly prevent network-based attacks against resources. Network-based attacks are typically mitigated at the network layer through measures such as firewalls, intrusion detection systems, and network segmentation.

#### Correct answer

**It protects sensitive data and ensures confidentiality, integrity, and availability.**

#### Explanation

The significance of implementing security controls at the "data" layer in the defense-in-depth model is to protect sensitive data and ensure confidentiality, integrity, and availability. These controls help safeguard data from unauthorized access, modification, or disclosure, thereby maintaining the overall security of the organization's data assets.

**It ensures the physical security of data storage.**

#### **Explanation**

Implementing security controls at the "data" layer focuses on protecting the data itself rather than the physical security of data storage. Physical security measures, such as access controls and surveillance, are more relevant to the physical security of data storage locations.

#### **Overall explanation**

The "data" layer in the defense-in-depth model is responsible for controlling access to business and customer data. It ensures that sensitive data is properly secured and complies with regulatory requirements, ensuring its confidentiality, integrity, and availability.

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

#### **Domain**

Describe Azure architecture and services

### **Question 33 Skipped**

**Which of the following is a feature of Microsoft Entra ID?**

#### **Virtual Machines**

#### **Explanation**

Virtual Machines are a separate Azure service and not a feature of Microsoft Entra ID. They provide scalable computing resources in the cloud but are not directly related to Microsoft Entra ID.

**Correct answer**

#### **Managed Identities**

## **Explanation**

Managed Identities are a feature of Microsoft Entra ID that provides an identity for services to authenticate with Azure resources securely. It eliminates the need to store credentials in code and ensures seamless integration with Azure services.

## **Resource Groups**

### **Explanation**

Resource Groups are containers that hold related Azure resources for organizational and management purposes. They are not a feature of Microsoft Entra ID but are used to group and manage resources within an Azure subscription.

## **SQL Databases**

### **Explanation**

SQL Databases are a separate Azure service for storing and managing relational databases. While they can be integrated with Microsoft Entra ID for authentication and access control, they are not a specific feature of Microsoft Entra ID.

## **Overall explanation**

**Managed Identities** is a feature in Microsoft Entra ID that helps manage the credentials needed to authenticate to Azure services without having to store credentials in code. This feature is especially useful for Azure resources that need to interact with other Azure services securely. With Managed Identities, an identity is automatically created in Entra ID for your service, which can then be used to obtain tokens to access other services. This eliminates the need for developers to handle secrets and credentials, thus reducing the risk of credential leaks and simplifying identity management.

**Reference:** <https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview>

## **Domain**

Describe Azure architecture and services

## **Question 34 Skipped**

Yes or No:

**A resource group can contain resources from multiple Azure regions.**

**No**

**Correct answer**

**Yes**

### **Explanation**

Yes, a resource group in Azure can contain resources from multiple Azure regions. Resource groups are logical containers that hold related resources for an Azure solution. They help manage and organize resources and do not limit the resources to a specific region. This allows for flexibility in organizing resources across different regions within the same resource group.

### **Overall explanation**

#### **From the official documentation:**

Resources from multiple different regions can be placed in a resource group. The resource group only contains metadata about the resources it contains.

# Resource groups

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

- All the resources in your resource group should share the same lifecycle. You deploy, update, and delete them together. If one resource, such as a server, needs to exist on a different deployment cycle it should be in another resource group.
- Each resource can exist in only one resource group.
- You can add or remove a resource to a resource group at any time.
- You can move a resource from one resource group to another group. For more information, see [Move resources to new resource group or subscription](#).
- The resources in a resource group can be located in different regions than the resource group.
- When you create a resource group, you need to provide a location for that resource group.

You may be wondering, "Why does a resource group need a location? And, if the resources can have different locations than the resource group, why does the resource group location matter at all?"

The resource group stores metadata about the resources. When you specify a location for the resource group, you're specifying where that metadata is stored. For compliance reasons, you may need to ensure that your data is stored in a particular region.

If a resource group's region is temporarily unavailable, you can't update resources in the resource group because the metadata is unavailable. The resources in other regions will still function as expected, but you can't update them. This condition doesn't apply to global resources like Azure Content Delivery Network, Azure DNS, Azure Traffic Manager, and Azure Front Door.

For more information about building reliable applications, see [Designing reliable Azure applications](#).

- A resource group can be used to scope access control for administrative actions. To manage a resource group, you can assign [Azure Policies](#), [Azure roles](#), or [resource locks](#).
- You can [apply tags](#) to a resource group. The resources in the resource group don't inherit those tags.
- A resource can connect to resources in other resource groups. This scenario is common when the two resources are related but don't share the same lifecycle. For example, you can have a web app that connects to a database in a different resource group.
- When you delete a resource group, all resources in the resource group are also deleted. For information about how Azure Resource Manager orchestrates those deletions, see [Azure Resource Manager resource group and resource deletion](#).

**Reference:** <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview>

## Domain

Describe Azure management and governance

## Question 35 Skipped

**Yes or No:**

**Inter-Region transfer of data is always free of cost.**

**Yes**

#### **Explanation**

Inter-Region transfer of data in Azure is not always free of cost. While there are certain scenarios where data transfer between Azure regions may be free, such as within the same region or between regions in the same geography, there are cases where charges may apply for transferring data across different regions or geographies.

**Correct answer**

**No**

#### **Explanation**

The correct choice is No because inter-Region transfer of data in Azure is not always free of cost. Depending on the specific Azure services being used and the regions involved in the data transfer, charges may apply for transferring data across different regions. It is important to review the Azure pricing documentation for detailed information on data transfer costs between regions.

#### **Overall explanation**

**Look at the following details from the official documentation:**

Is data transfer between Azure services located in two regions charged? ^

Yes. Outbound data transfer is charged at the normal rate and inbound data transfer is free.

## Inter Region

Intra-continental Data Transfer	Price
Between regions within North America	\$0.02 per GB
Between regions within Europe	
Between regions within Asia	\$0.08 per GB
Between regions within Oceania	
Between regions within Middle East and Africa	
Between regions within South America	\$0.16 per GB

**Reference:** <https://azure.microsoft.com/en-us/pricing/details/bandwidth/>

## Domain

Describe Azure management and governance

### Question 36 Skipped

**Which of the following is NOT a responsibility of the cloud service provider (CSP) in the shared responsibility model?**

**Correct answer**

**Ensuring data privacy**

#### Explanation

Ensuring data privacy is primarily the responsibility of the customer in the shared responsibility model. While the cloud service provider (CSP) may provide tools and services to help customers protect their data, ultimately it is the customer's responsibility to ensure the privacy and security of their data.

**Providing network connectivity**

#### Explanation

Providing network connectivity is typically the responsibility of the cloud service provider (CSP) in the shared responsibility model. The CSP is responsible for ensuring that customers have reliable and secure network connectivity to access their cloud services and resources.

## **Securing the physical data center**

### **Explanation**

Securing the physical data center is typically the responsibility of the cloud service provider (CSP) in the shared responsibility model. The CSP is responsible for ensuring the physical security of the data center facilities, including protection against unauthorized access, environmental controls, and disaster recovery measures.

## **Protecting the operating system of virtual machines**

### **Explanation**

Protecting the operating system of virtual machines is a shared responsibility between the cloud service provider (CSP) and the customer. The CSP is responsible for ensuring the security of the underlying infrastructure, while the customer is responsible for securing the operating system and any applications running on the virtual machines.

## **Overall explanation**

While CSPs have responsibilities to protect the underlying infrastructure and services, data privacy is primarily the responsibility of the **customer**. The CSP provides the tools and resources to protect data, but the customer is responsible for implementing appropriate data protection measures.

**Reference:** <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

### **Domain**

Describe Cloud Concepts

### **Question 37 Skipped**

**Is an internet connection necessary for using cloud computing?**

**Correct answer**

**No**

#### **Explanation**

This choice is correct because an internet connection is not a strict requirement for using cloud computing. While many cloud services and resources are accessed over the internet, there are scenarios where cloud computing can be utilized in offline or restricted network environments, making an internet connection not necessary for all cloud computing use cases.

**Yes**

#### **Explanation**

This choice is incorrect because an internet connection is not always necessary for using cloud computing. While an internet connection is typically required to access cloud services and resources, some cloud computing models, such as private cloud or hybrid cloud, can be used within a closed network environment without internet connectivity.

#### **Overall explanation**

The answer is no. Cloud computing services can be used over the internet, but they can also be used through private networks or dedicated connections, such as Azure ExpressRoute, which provides a dedicated, private network connection between on-premises infrastructure and Azure data centers. Some cloud services can also be accessed offline or through local networks.

For example, Azure Stack is a hybrid cloud solution that allows you to use Azure services on-premises, without an internet connection. This can be useful for organizations that have limited or unreliable internet connectivity but still want to take advantage of the benefits of cloud computing.

Similarly, some cloud providers offer edge computing solutions that allow you to run cloud workloads on devices located at the edge of the network, such as in a factory or remote location, without needing a constant internet connection.

In general, however, most cloud services do require an internet connection to access and use them. This is because the underlying infrastructure and resources that support these services are typically hosted in data centers that are connected to the internet.

**Reference:** <https://learn.microsoft.com/en-us/azure-stack/operator/azure-stack-overview?view=azs-2206>

## Domain

Describe Azure architecture and services

### Question 38 Skipped

**Can you apply a read-only lock to an Azure resource that already has a delete lock applied to it?**

**No, a delete lock overrides all other locks and prevents any modifications or deletions**

#### Explanation

No, a delete lock does not prevent the application of a read-only lock to an Azure resource. While the delete lock prevents any modifications or deletions to the resource, a read-only lock can still be applied to restrict modifications while allowing viewing access.

#### Correct answer

**Yes, but only by the owner of the subscription**

#### Explanation

Yes, the owner of the subscription can apply a read-only lock to an Azure resource that already has a delete lock applied to it. The read-only lock will restrict any modifications to the resource while still allowing the owner to view the resource and its settings.

**No, but a read-only lock can be temporarily disabled to make modifications**

#### Explanation

No, a read-only lock cannot be temporarily disabled to make modifications to an Azure resource that already has a delete lock applied to it. The delete lock takes precedence

over all other locks and prevents any changes to the resource until the delete lock is removed.

## Overall explanation

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.

Try this out in the Azure portal, you should be able to add a read-only lock to a resource having a CanNotDelete lock already!

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

## Domain

Describe Azure management and governance

## Question 39 Skipped

**What Azure service provides recommendations to optimize your cloud spending based on your usage patterns?**

### Azure Monitor

#### Explanation

Azure Monitor is a service that provides insights into the performance and health of your Azure resources. While it helps you monitor and analyze your Azure environment,

it does not specifically focus on providing recommendations to optimize cloud spending based on usage patterns.

#### Correct answer

### Azure Cost Management and Billing

#### Explanation

Azure Cost Management and Billing is the correct choice as it provides recommendations to optimize your cloud spending based on your usage patterns. It offers cost analysis, budgeting tools, and cost optimization recommendations to help you manage and optimize your Azure spending effectively.

### Azure Advisor

#### Explanation

Azure Advisor provides recommendations for improving the security, performance, and reliability of your Azure resources. While it offers valuable insights, it does not specifically focus on optimizing cloud spending based on usage patterns.

### Azure Policy

#### Explanation

Azure Policy is a service that helps you enforce organizational standards and compliance controls on your Azure resources. While it is important for governance and compliance, it does not provide recommendations for optimizing cloud spending based on usage patterns.

#### Overall explanation

**Azure Cost Management and Billing** is the correct answer & provides recommendations to optimize your cloud spending based on your usage patterns. The service provides insights and cost management tools to help you monitor, allocate, and optimize your cloud costs.

#### Other options:

- **Azure Advisor** is a service that provides personalized recommendations to help you optimize your Azure resources for high availability, security, performance, and cost. Azure Advisor also provides recommendations to optimize your cloud spending, but its primary focus is on providing guidance for improving the security, reliability, and performance of your Azure resources. While it may include some cost optimization recommendations, it is not solely focused on cost management and billing like Azure Cost Management and Billing. In such questions we'll always choose the BEST choice possible.
- **Azure Monitor** is a service that provides a single pane of glass to monitor the performance and health of your applications and infrastructure in Azure.
- **Azure Policy** is a service that enables you to enforce governance policies for your Azure resources to ensure compliance with organizational standards and regulations.

**Reference:** <https://learn.microsoft.com/en-us/azure/cost-management-billing/cost-management-billing-overview>

## Domain

Describe Azure management and governance

### Question 40 Skipped

You are the senior architect of XYZ organization and the senior management has requested to migrate all on-prem resources to the cloud.

The requirement is that only **Platform as a Service (PaaS)** solutions must be used in Azure.

**Solution: To begin, you create an Azure App Service and Azure SQL databases.**

Would this meet the goal?

**Correct answer**

**Yes**

## Explanation

Yes, creating an Azure App Service and Azure SQL databases aligns with the requirement of using Platform as a Service (PaaS) solutions in Azure. Azure App Service is a fully managed platform for building, deploying, and scaling web apps, while Azure SQL databases provide a fully managed relational database service. Both of these services fall under the category of PaaS offerings in Azure, making this solution suitable for the migration of on-prem resources to the cloud.

## No

### Explanation

This statement is incorrect. Creating an Azure App Service and Azure SQL databases meets the requirement of using Platform as a Service (PaaS) solutions in Azure. Azure App Service and Azure SQL databases are both PaaS offerings that provide managed services for web applications and relational databases, respectively. Therefore, this solution aligns with the goal of migrating on-prem resources to the cloud using PaaS solutions.

### Overall explanation

Please always remember - Azure App Service and Azure SQL Databases are both PaaS services!

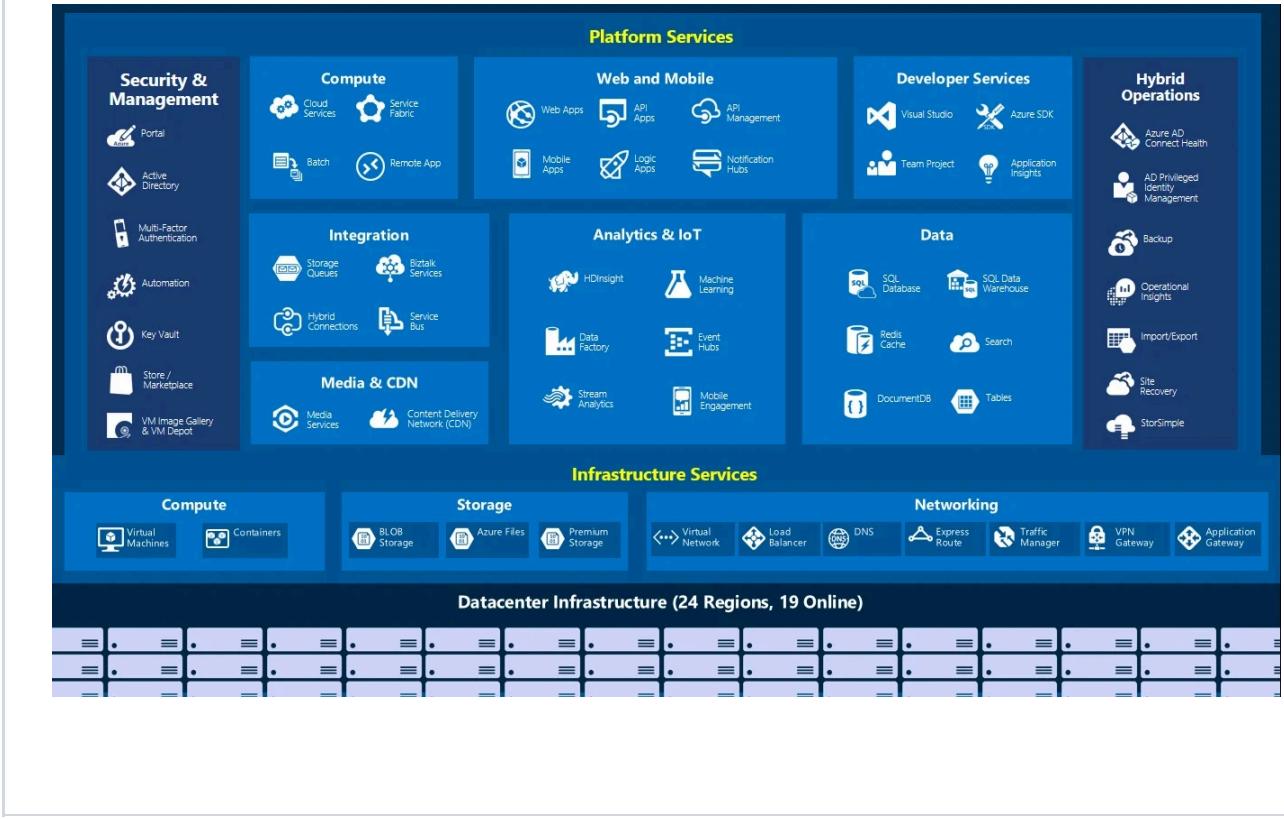
**Azure App Service** - Allows us to quickly build, deploy, and scale web apps created with popular frameworks such as .NET, .NET Core, Node.js, Java, PHP, Ruby, or Python, in containers or running on any operating system. It offers rigorous, enterprise-grade performance, security, and compliance requirements by using the fully managed platform for your operational and monitoring tasks.

**Reference:** <https://azure.microsoft.com/en-in/services/app-service/>

**Azure SQL Database** - Microsoft Azure SQL Database is a managed cloud database provided as a part of Microsoft Azure. A cloud database is a database that runs on a cloud computing platform, and access to it is provided as a service. Managed database services take care of scalability, backup, and high availability of the database.

**Reference:** <https://azure.microsoft.com/en-in/services/sql-database/>

Please refer to the image below, and make sure you remember it properly. A lot of the questions in the exam can be answered using this image alone:



## Domain

Describe Cloud Concepts

### Question 41 Skipped

In the defense-in-depth model, what is the role of the "network" layer?

#### Correct answer

**It limits communication between resources and enforces access controls.**

#### Explanation

The network layer in the defense-in-depth model is responsible for limiting communication between resources and enforcing access controls. It includes implementing network segmentation, firewalls, and network access controls to prevent unauthorized access and ensure secure communication between resources.

**It focuses on securing access to applications.**

#### Explanation

Securing access to applications is typically the responsibility of the application layer in the defense-in-depth model. This layer focuses on protecting the application code, data, and interfaces from unauthorized access or attacks.

### **It ensures the physical security of computing hardware.**

#### **Explanation**

Ensuring the physical security of computing hardware is typically the responsibility of the physical security layer in the defense-in-depth model. This layer focuses on protecting the physical infrastructure, such as data centers, servers, and networking equipment, from unauthorized access or tampering.

### **It secures access to virtual machines.**

#### **Explanation**

Securing access to virtual machines falls under the responsibility of the identity and access management layer in the defense-in-depth model. This layer focuses on controlling user access, permissions, and authentication to resources.

### **Overall explanation**

The "network" layer in the defense-in-depth model is responsible for limiting communication between resources, which helps prevent the spread of attacks. It enforces access controls to ensure that only necessary communication occurs and reduces the risk of an attack affecting other systems.

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

### **Domain**

Describe Azure architecture and services

### **Question 42 Skipped**

Yes or No:

**One of the definitions of the Hybrid cloud model is to use multiple Public Clouds in conjunction with a Private Cloud.**

**No**

**Correct answer**

**Yes**

### **Explanation**

Yes, one of the definitions of the Hybrid cloud model is indeed to use multiple Public Clouds in conjunction with a Private Cloud. This approach allows organizations to leverage the benefits of both public and private cloud environments, enabling them to optimize performance, security, and cost-effectiveness based on their specific needs and workloads.

### **Overall explanation**

#### **From the official docs:**

A hybrid cloud—sometimes called a cloud hybrid—is a computing environment that combines an **on-premises** datacenter (also called a [private cloud](#)) with a [public cloud](#), allowing data and applications to be shared between them. Some people define hybrid cloud to include “**multicloud**” configurations where an organization uses more than one public cloud in addition to their on-premises datacenter.

**Reference:** <https://azure.microsoft.com/en-gb/overview/what-is-hybrid-cloud-computing/>

### **Domain**

Describe Cloud Concepts

### **Question 43 Skipped**

**What is the primary purpose of Microsoft Defender for Cloud?**

**To automate the deployment of virtual machines in the cloud.**

**Explanation**

Automating the deployment of virtual machines is not the primary purpose of Microsoft Defender for Cloud. Its main focus is on security monitoring and threat protection in cloud environments.

**Correct answer**

**To monitor security posture and protect against threats in cloud, on-premises, hybrid, and multi-cloud environments.**

**Explanation**

The primary purpose of Microsoft Defender for Cloud is to monitor the security posture of cloud environments and protect against threats across various deployment scenarios, including cloud, on-premises, hybrid, and multi-cloud environments.

**To provide network segmentation for virtual machines.**

**Explanation**

While network segmentation can be a part of overall security measures, Microsoft Defender for Cloud's primary focus is on security monitoring and threat protection rather than providing network segmentation for virtual machines.

**To provide a physical security layer for computing hardware.**

**Explanation**

Microsoft Defender for Cloud is focused on cybersecurity and threat protection, rather than physical security for computing hardware. It helps to secure cloud environments and protect against various cyber threats.

**Overall explanation**

From the official Microsoft documentation:

Defender for Cloud is a monitoring tool for security posture management and threat protection. It monitors your cloud, on-premises, hybrid, and multi-cloud environments to provide guidance and notifications aimed at strengthening your security posture.

Defender for Cloud provides the tools needed to harden your resources, track your security posture, protect against cyber attacks, and streamline security management. Deployment of Defender for Cloud is easy, it's already natively integrated to Azure.

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

## Domain

Describe Azure management and governance

### Question 44 Skipped

**Which of the following Azure storage solutions meets ALL the following requirements:**

- 1) The ability to handle unstructured data (document, graph, key-value)
- 2) Automatically index all data, regardless of the data model.
- 3) Multi-region writes and data distribution to any Azure region.

#### Azure Database for MariaDB

##### Explanation

Azure Database for MariaDB does not meet all the specified requirements. While it can handle unstructured data, it does not automatically index all data regardless of the data model. It also does not offer multi-region writes and data distribution to any Azure region, making it an incorrect choice for the given requirements.

#### Azure SQL Edge

##### Explanation

Azure SQL Edge does not meet all the specified requirements. While it can handle unstructured data, it does not automatically index all data regardless of the data model. It also does not offer multi-region writes and data distribution to any Azure region, making it an incorrect choice for the given requirements.

## Azure Files

### Explanation

Azure Files do not meet all the specified requirements. While they can handle unstructured data, they do not automatically index all data regardless of the data model. They also do not offer multi-region writes and data distribution to any Azure region, making them an incorrect choice for the given requirements.

## Azure Cache for Redis

### Explanation

Azure Cache for Redis does not meet all the specified requirements. While it can handle unstructured data, it does not automatically index all data regardless of the data model. It also does not offer multi-region writes and data distribution to any Azure region, making it an incorrect choice for the given requirements.

## Azure SQL Databases

### Explanation

Azure SQL Databases do not meet all the specified requirements. While they can handle unstructured data, they do not automatically index all data regardless of the data model. They also do not offer multi-region writes and data distribution to any Azure region, making them an incorrect choice for the given requirements.

### Correct answer

## Azure Cosmos DB

### Explanation

Azure Cosmos DB is the correct choice as it meets all the specified requirements. It can handle unstructured data such as documents, graphs, and key-value pairs. It automatically indexes all data regardless of the data model. Additionally, it offers multi-region writes and data distribution to any Azure region, making it a suitable choice for the given requirements.

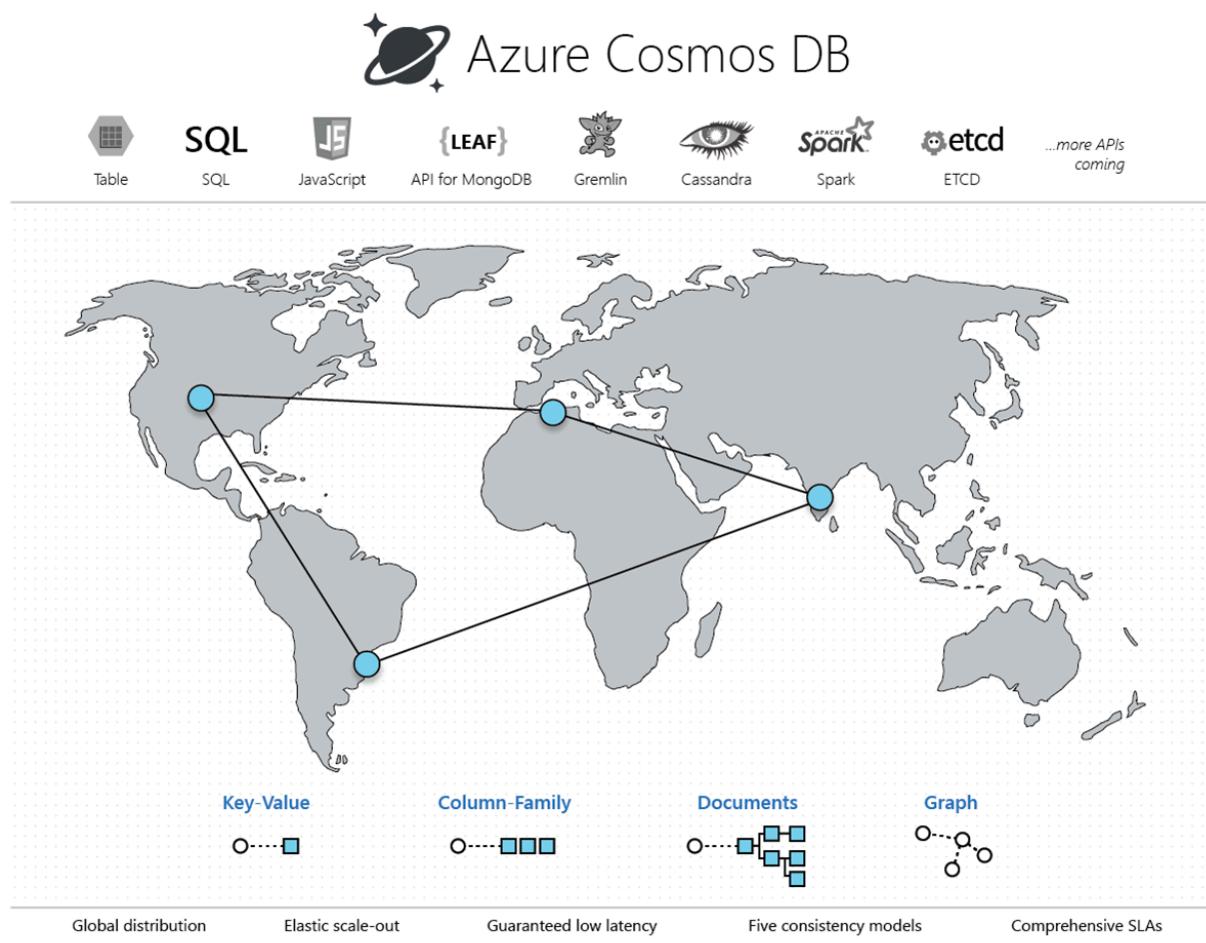
## Overall explanation

### From the official documentation:

Today's applications are required to be highly responsive and always online. To achieve low latency and high availability, instances of these applications need to be deployed in datacenters that are close to their users. Applications need to respond in real time to large changes in usage at peak hours, store ever increasing volumes of data, and make this data available to users in milliseconds.

**Azure Cosmos DB** is Microsoft's globally distributed, multi-model database service. With the click of a button, Cosmos DB enables you to elastically and independently scale throughput and storage across any number of Azure regions worldwide. You can elastically scale throughput and storage, and take advantage of fast, single-digit-millisecond data access using your favorite API including: SQL, MongoDB, Cassandra, Tables, or Gremlin. Cosmos DB provides comprehensive [service level agreements](#) (SLAs) for throughput, latency, availability, and consistency guarantees, something no other database service offers.

Azure Cosmos DB is a great way to store unstructured and JSON data. Combined with Azure Functions, Cosmos DB makes storing data quick and easy with much less code than required for storing data in a relational database.



### References:

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

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-integrate-store-unstructured-data-cosmosdb?tabs=csharp>

## Domain

Describe Azure architecture and services

### Question 45 Skipped

**You have dozens of Virtual Machines (VM) hosted in Azure. The lead architect has asked for your suggestions to migrate all the VMs to an Azure Pay-As-You-Go subscription. Which expenditure model would apply to the stated requirement?**

**Scalable**

**Correct answer**

**Operational**

## Explanation

The Operational expenditure model, also known as Pay-As-You-Go, is suitable for migrating Virtual Machines (VMs) to an Azure subscription where you pay for the resources you use on a consumption basis. This model is flexible and aligns with the requirement to move the VMs to an Azure Pay-As-You-Go subscription.

**Capital**

## Explanation

The Capital expenditure model involves upfront investment in resources that are depreciated over time. This model is not suitable for migrating VMs to an Azure Pay-As-You-Go subscription, as it does not align with the requirement to pay for resources on a consumption basis.

**Fault Tolerant**

## Overall explanation

Fault Tolerant and Scalable are wrong answers because such payment models don't exist. Capital expenditure is also incorrect since we aren't going to be paying anything up front. Operational makes the most sense since it means '**pay as you go**', i.e paying only for what you consume and nothing else.

**Reference:** <https://azure.microsoft.com/en-ca/pricing/purchase-options/pay-as-you-go>

## Domain

Describe Cloud Concepts

### Question 46 Skipped

**Select the characteristics of the Public Cloud from the following:**

**Organizations are responsible for hardware maintenance and updates.**

#### Explanation

In the Public Cloud, organizations are not responsible for hardware maintenance and updates. Cloud providers handle the maintenance and updates of the underlying infrastructure, freeing up users from these tasks.

**Unsecured connections**

#### Explanation

Unsecured connections are not a characteristic of the Public Cloud. Public Cloud providers implement various security measures to ensure data protection and secure connections for users.

**Hardware must be purchased for start-up and maintenance.**

#### Explanation

Public Cloud services do not require organizations to purchase hardware for start-up and maintenance. Instead, cloud providers manage the hardware infrastructure,

allowing users to focus on their applications and services.

#### **Correct selection**

**Applications can be quickly provisioned and deprovisioned.**

#### **Explanation**

Applications can be quickly provisioned and deprovisioned in the Public Cloud, allowing organizations to rapidly deploy and remove resources as needed. This agility and flexibility are essential for adapting to changing business requirements.

#### **Correct selection**

**No capital expenditure to scale up**

#### **Explanation**

One of the key benefits of the Public Cloud is that it eliminates the need for capital expenditure to scale up. Users can easily adjust their resources based on demand without the upfront costs associated with traditional IT infrastructure.

#### **Correct selection**

**Metered pricing**

#### **Explanation**

Metered pricing is a characteristic of the Public Cloud, where users are charged based on their actual usage of resources. This pay-as-you-go model allows for cost-effective scalability and flexibility.

#### **Overall explanation**

**From the Azure Docs:**

# Cloud model comparison

## Public cloud

- No capital expenditures to scale up.
- Applications can be quickly provisioned and deprovisioned.
- Organizations pay only for what they use.

## Private cloud

- Hardware must be purchased for start-up and maintenance.
- Organizations have complete control over resources and security.
- Organizations are responsible for hardware maintenance and updates.

## Hybrid cloud

- Provides the most flexibility.
- Organizations determine where to run their applications.
- Organizations control security, compliance, or legal requirements.

With the public cloud, you get pay-as-you-go pricing and you pay only for what you use, no CapEx costs are involved.

With the public cloud, you have self-service management. You are responsible for the deployment and configuration of the cloud resources such as virtual machines or web sites. The underlying hardware that hosts the cloud resources is managed by the cloud provider.

### Incorrect Answers:

**Hardware must be purchased for start-up and maintenance** - You don't have to purchase any hardware on the public cloud. The underlying hardware is shared so you could have multiple customers using cloud resources hosted on the same physical hardware. Moreover, this is a characteristic of the private cloud.

**Unsecured Connections** - Connections to the public cloud are secure.

**Organizations are responsible for hardware maintenance and updates -** This is a characteristic of the Private Cloud.

**References :** <https://docs.microsoft.com/en-gb/learn/modules/principles-cloud-computing/4-cloud-deployment-models>

## Domain

Describe Cloud Concepts

### Question 47 Skipped

**Which of the following is a serverless solution that allows you to write less code, maintain less infrastructure, and save on costs.?**

**Correct answer**

#### Azure Functions

#### Explanation

Azure Functions is a serverless compute service that allows you to run event-triggered code without having to explicitly provision or manage infrastructure. It is designed to help you write less code, maintain less infrastructure, and save on costs by only paying for the resources used during execution.

#### Azure App Service

#### Explanation

Azure App Service is a fully managed platform for building, deploying, and scaling web apps. While it offers a platform for hosting web applications, it is not a serverless solution that allows you to write less code, maintain less infrastructure, and save on costs compared to Azure Functions.

#### Azure Logic Apps

## Explanation

Azure Logic Apps is a cloud-based service that helps you automate and orchestrate tasks, business processes, and workflows when you need to integrate apps, data, systems, and services across enterprises or organizations. While it provides automation capabilities, it is not specifically designed to be a serverless solution for writing less code and maintaining less infrastructure.

## Azure DevOps

### Explanation

Azure DevOps is a set of services for teams to plan, build, and ship software across a variety of platforms. While it is a valuable tool for managing the software development lifecycle, it is not a serverless solution that allows you to write less code, maintain less infrastructure, and save on costs.

## Overall explanation

**Azure Functions** allows you to run small pieces of code (called "functions") without worrying about application infrastructure. With Azure Functions, the cloud infrastructure provides all the up-to-date servers you need to keep your application running at scale.

A function is "**triggered**" by a specific type of event. [Supported triggers](#) include responding to changes in data, responding to messages, running on a schedule, or as the result of an HTTP request.

Few of the features of Azure Functions are:

# Features

Some key features of Azure Functions include:

- **Serverless applications:** Functions allow you to develop [serverless](#) applications on Microsoft Azure.
- **Choice of language:** Write functions using your choice of [C#](#), [Java](#), [JavaScript](#), [Python](#), and [PowerShell](#).
- **Pay-per-use pricing model:** Pay only for the time spent running your code. See the Consumption hosting plan option in the [pricing section](#).
- **Bring your own dependencies:** Functions supports NuGet and NPM, giving you access to your favorite libraries.
- **Integrated security:** Protect HTTP-triggered functions with OAuth providers such as Azure Active Directory, Facebook, Google, Twitter, and Microsoft Account.
- **Simplified integration:** Easily integrate with Azure services and software-as-a-service (SaaS) offerings.
- **Flexible development:** Set up continuous integration and deploy your code through [GitHub](#), [Azure DevOps Services](#), and other [supported development tools](#).

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

## Domain

Describe Azure architecture and services

## Question 48 Skipped

**The shared responsibility model is important because:**

**It helps to avoid security incidents.**

## Explanation

While the shared responsibility model does play a role in helping to avoid security incidents by clearly defining responsibilities, its primary purpose is not solely focused on preventing incidents. It is more about establishing accountability and understanding the division of security responsibilities.

## **It reduces the cost of cloud services.**

### **Explanation**

The shared responsibility model does not directly impact the cost of cloud services. It is more about ensuring that security measures are appropriately implemented by both the CSP and the customer, rather than reducing the overall cost of cloud services.

## **It ensures complete security of cloud environments.**

### **Explanation**

The shared responsibility model does not guarantee complete security of cloud environments. It is designed to clarify the roles and responsibilities of the CSP and the customer in security measures, but it does not ensure absolute security. It is a collaborative effort to enhance security, not a guarantee of complete protection.

### **Correct answer**

## **It clearly defines the roles of the CSP and customer in security.**

### **Explanation**

The shared responsibility model is crucial as it clearly outlines the responsibilities of both the Cloud Service Provider (CSP) and the customer in terms of security. This helps in understanding who is responsible for what aspects of security, ensuring a collaborative approach to maintaining a secure cloud environment.

### **Overall explanation**

The shared responsibility model is essential for establishing **clear expectations** between the CSP and the customer regarding security responsibilities. While it doesn't guarantee the prevention of security incidents, it helps in understanding who is accountable for specific security measures.

**Reference:** <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

### **Domain**

### Question 49 Skipped

\_\_\_\_\_ offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol or Network File System (NFS) protocol. This means it can be used to completely replace or supplement traditional on-premises file servers or NAS devices.

#### Azure SQL Database

##### Explanation

Azure SQL Database is a fully managed relational database service that is used for storing and managing structured data. It is not designed to offer fully managed file shares accessible via SMB or NFS protocols, making it an incorrect choice for this scenario.

#### Azure Data Lake Storage

##### Explanation

Azure Data Lake Storage is a scalable and secure data lake service that is used for storing and analyzing big data. While it is optimized for big data analytics workloads, it does not offer fully managed file shares accessible via SMB or NFS protocols, making it an incorrect choice for this scenario.

##### Correct answer

#### Azure Files

##### Explanation

Azure Files offers fully managed file shares in the cloud that can be accessed via the SMB or NFS protocols. It is designed to provide a simple way to create file shares in Azure that can be used to replace or supplement traditional on-premises file servers or NAS devices, making it the correct choice for this scenario.

#### Azure Blob Storage

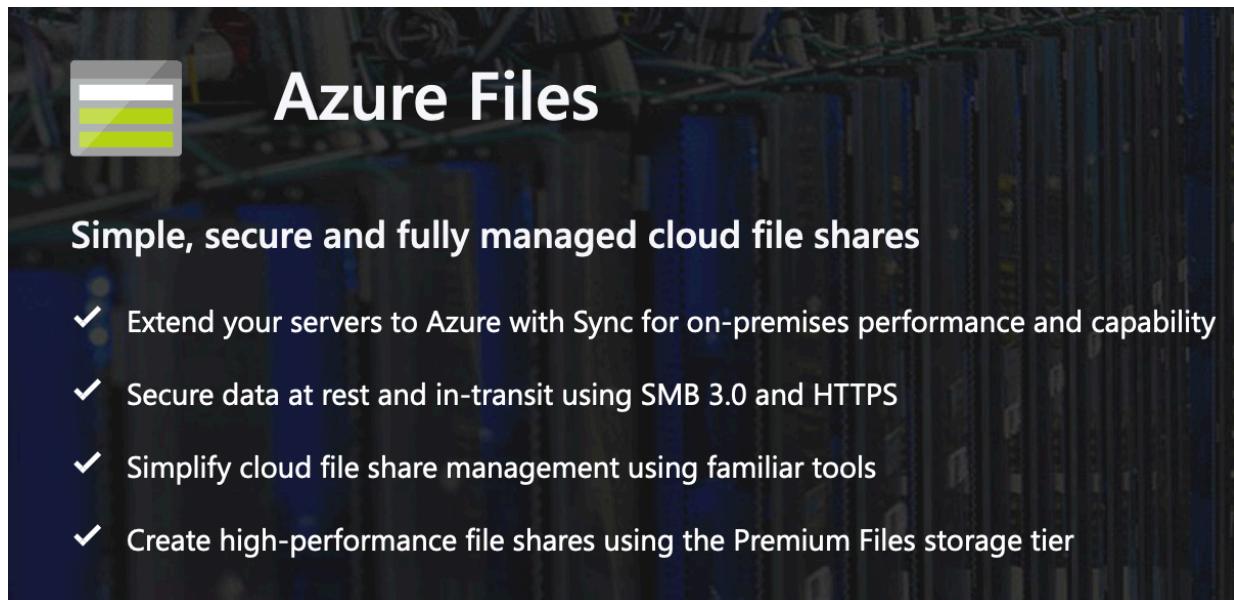
## Explanation

Azure Blob Storage is a scalable object storage service that is used for storing unstructured data like documents, images, videos, and logs. While it is a popular choice for storing large amounts of unstructured data, it does not offer fully managed file shares accessible via SMB or NFS protocols, making it an incorrect choice for this scenario.

## Overall explanation

From the official docs:

**Azure Files** is Microsoft's easy-to-use cloud file system. Azure file shares can be seamlessly used in Windows and Windows Server. To use an Azure file share with Windows, you must either mount it, which means assigning it a drive letter or mount point path, or access it via its UNC path.



Unlike other SMB shares you may have interacted with, such as those hosted on a Windows Server, Linux Samba server, or NAS device, Azure file shares do not currently support Kerberos authentication with your Active Directory (AD) or Azure Active Directory (AAD) identity.

Instead, you must access your Azure file share with the storage account key for the storage account containing your Azure file share. A storage account key is an administrator key for a storage account, including administrator permissions to all files and folders within the file share you're accessing, and for all file shares and other storage resources (blobs, queues, tables, etc) contained within your storage account.

**Reference:** <https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

## Domain

Describe Azure architecture and services

### Question 50 Skipped

**Which of the following services provides information about Azure service incidents, planned maintenance and can notify you of issues via Email, SMS and push notifications?**

#### Azure Monitor

#### Explanation

Azure Monitor is a service that provides monitoring and analytics for applications and resources in Azure. While it can help track performance and diagnose issues, it does not specifically provide information about service incidents, planned maintenance, or notifications for issues via Email, SMS, and push notifications.

#### Correct answer

#### Azure Service Health

#### Explanation

Azure Service Health is the correct choice as it specifically provides information about Azure service incidents, planned maintenance, and can notify users of issues via Email, SMS, and push notifications. It helps users stay informed about the status of Azure services they are using.

#### Azure Initiatives

#### Explanation

Azure Initiatives are sets of policies, initiatives, and definitions that help manage and enforce compliance in Azure. They are not related to providing information about

service incidents, planned maintenance, or notifications for issues via Email, SMS, and push notifications.

## Azure Trust Portal

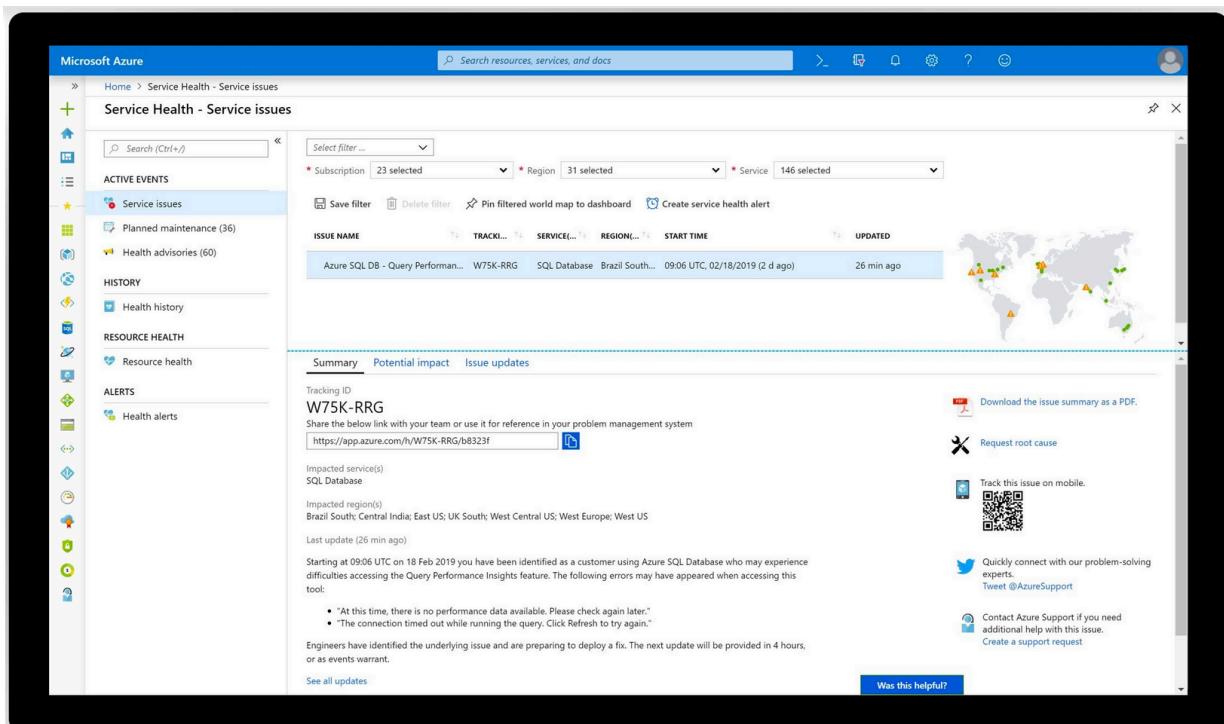
### Explanation

Azure Trust Portal is a portal that provides information about compliance, privacy, and security in Azure. It does not provide information about service incidents, planned maintenance, or notifications for issues via Email, SMS, and push notifications.

### Overall explanation

According to the official Azure docs:

**Azure Service Health** notifies you about Azure service incidents and planned maintenance so you can take action to mitigate downtime. We can configure customizable **cloud alerts** and use your personalized dashboard to analyze health issues, monitor the impact to your cloud resources, get guidance and support, and share details and updates.



Reference : <https://azure.microsoft.com/en-us/features/service-health/#features>

## Domain

Describe Azure management and governance

### Question 51 Skipped

**One of the teams in your company is looking for a solution for collecting, analyzing, and potentially taking action based on the metric and logging data from your entire Azure and on-premises environment.**

**Which of the following would you recommend?**

#### Azure Logs

##### Explanation

Azure Logs is a service that allows you to collect and store log data from various Azure resources for analysis and monitoring. While it is useful for logging, it does not provide the comprehensive solution for collecting, analyzing, and potentially taking action based on metric and logging data from the entire Azure and on-premises environment.

#### Correct answer

#### Azure Monitor

##### Explanation

Azure Monitor is the recommended solution for collecting, analyzing, and potentially taking action based on metric and logging data from the entire Azure and on-premises environment. It provides a comprehensive monitoring and analytics solution for resources in Azure and on-premises environments, allowing you to gain insights, detect issues, and take proactive actions based on the data collected.

#### Azure Insights

##### Explanation

Azure Insights is a service that provides application performance monitoring and diagnostics for applications hosted on Azure. It focuses on monitoring the performance and health of applications, rather than collecting, analyzing, and taking

action based on metric and logging data from the entire Azure and on-premises environment.

## Azure Advisor

### Explanation

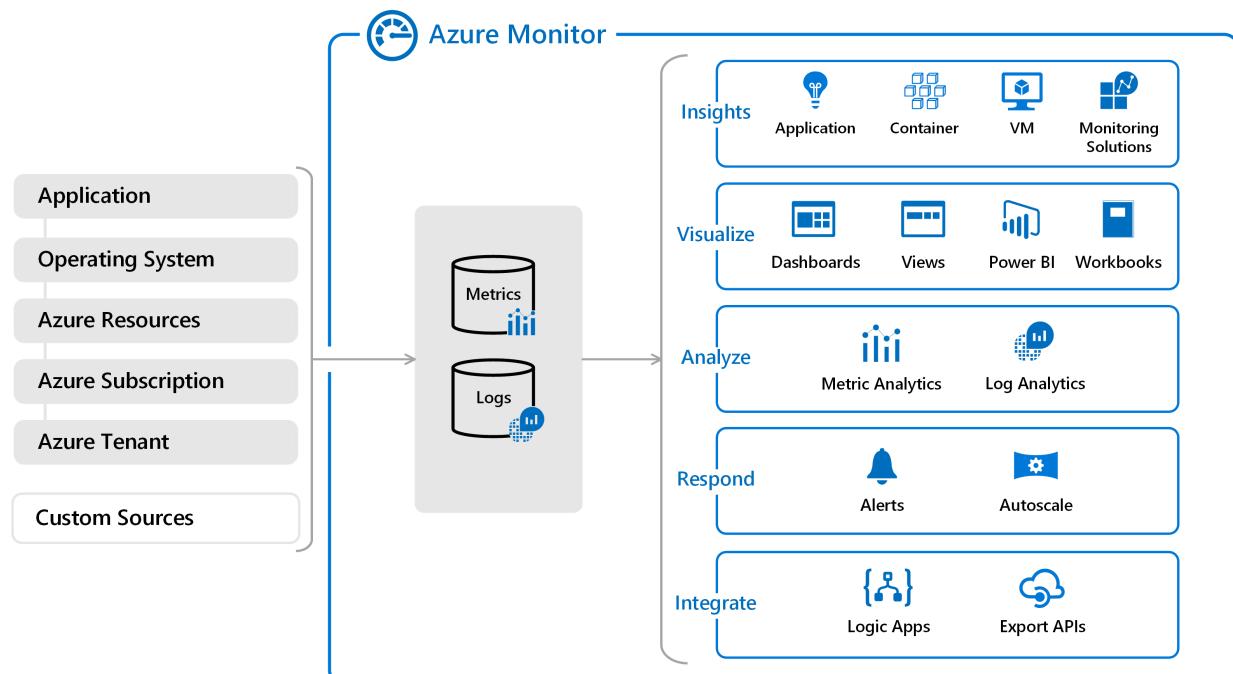
Azure Advisor is a service that provides recommendations to optimize Azure resources for high availability, security, performance, and cost. It does not focus on collecting, analyzing, and taking action based on metric and logging data from the entire Azure and on-premises environment.

### Overall explanation

#### From the Official Azure Documentation:

[Azure Monitor](#) is a platform for collecting, analyzing, visualizing, and potentially taking action based on the metric and logging data from your entire Azure and on-premises environment.

The following diagram illustrates just how comprehensive Azure Monitor is.



- On the left is a list of the sources of logging and metric data that can be collected at every layer in your application architecture, from application to operating system and network.
- In the center, you can see how the logging and metric data is stored in central repositories.

- On the right, the data is used in a number of ways. You can view real-time and historical performance across each layer of your architecture, or aggregated and detailed information. The data is displayed at different levels for different audiences. You can view high-level reports on the Azure Monitor Dashboard or create custom views by using Power BI and Kusto queries.

Additionally, you can use the data to help you react to critical events in real time, through alerts delivered to teams via SMS, email, and so on. Or you can use thresholds to trigger autoscaling functionality to scale up or down to meet the demand.

**Reference:** <https://docs.microsoft.com/en-ca/learn/modules/monitoring-fundamentals/2-identify-product-options>

## Domain

Describe Azure management and governance

### Question 52 Skipped

**You are a tech startup owner and would like to migrate your self hosted apps and services to Azure.**

**Which of the following is an advantage of the Public Cloud that you'll realize thanks to the migration?**

**Resources are not shared with others, so higher levels of control and privacy are possible.**

## Explanation

This choice is incorrect because one of the advantages of the Public Cloud, especially Azure, is that resources are shared with other users. This sharing allows for cost efficiency and scalability, but it may impact the level of control and privacy compared to a private cloud environment.

**Your organization can customize its cloud environment to meet specific business needs.**

## Explanation

This choice is incorrect because while Azure does offer customization options, the level of customization may be limited compared to a private cloud environment. Public

Cloud providers like Azure offer standardized services and configurations to ensure scalability and ease of use.

#### Correct answer

**Near unlimited scalability as on-demand resources are available to meet your business needs.**

#### Explanation

This choice is correct because one of the key advantages of the Public Cloud, such as Azure, is near unlimited scalability. Azure provides on-demand resources that can scale up or down based on your business needs, allowing you to quickly adjust resources to meet demand without the need for physical hardware provisioning.

**Peace of mind that Azure will send over hardware for you to store in your warehouse.**

#### Explanation

This choice is incorrect because Azure is a public cloud service provider that offers cloud services over the internet. Azure does not send hardware to customers for them to store in their own warehouses. Instead, Azure provides virtualized resources that are accessed and managed through the cloud platform.

#### Overall explanation

From the official docs:

The public cloud is a **shared** entity whereby multiple corporations each use a portion of the resources in the cloud. The hardware resources (servers, infrastructure etc.) are managed by the cloud provider. Multiple companies create resources such as virtual machines and virtual networks on the hardware resources.

#### Incorrect Answers:

**Resources are not shared with others, so higher levels of control and privacy are possible** - This is a characteristic of a Private Cloud.

**Your organization can customize its cloud environment to meet specific business needs** - This is also a characteristic of a Private Cloud.

**Peace of mind that Azure will send over hardware for you to store in your warehouse** - Azure stores all infrastructure on their end. You'd be storing hardware that you purchased and incur CapEx in a Private cloud setup.

**Reference:** <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds/#overview>

### Domain

Describe Azure architecture and services

### Question 53 Skipped

Yes or No:

**A resource can belong to more than one resource group.**

**Correct answer**

**No**

### Explanation

Correct. In Azure, a resource can only be associated with a single resource group. This design choice ensures that resources are organized efficiently and consistently within the Azure environment.

**Yes**

### Explanation

No, a resource in Azure can only belong to one resource group at a time. Placing a resource in multiple resource groups is not supported in Azure.

### Overall explanation

No, 1 resource = 1 resource group (very simply logic)

**From the official documentation :**

## Resource groups

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

- All the resources in your group should share the same lifecycle. You deploy, update, and delete them together. If one resource, such as a database server, needs to exist on a different deployment cycle it should be in another resource group.
- Each resource can only exist in one resource group.

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

### Domain

Describe Azure architecture and services

### Question 54 Skipped

**How can you determine the estimated monthly cost of an Azure service or resource?**

**Correct answer**

**By using the Azure Pricing Calculator**

### Explanation

Using the Azure Pricing Calculator is the correct way to determine the estimated monthly cost of an Azure service or resource. The calculator allows you to input the details of the service or resource you plan to use, such as region, type, and quantity, and provides an estimate of the monthly cost based on the current pricing information.

**By checking the current Azure Marketplace pricing**

### Explanation

Checking the current Azure Marketplace pricing can give you an idea of the pricing for different services and resources available, but it may not provide an accurate estimate of the monthly cost for a specific service or resource based on your usage requirements. The Azure Pricing Calculator is a more suitable tool for this purpose.

### **By contacting Microsoft customer support**

#### **Explanation**

Contacting Microsoft customer support is not the appropriate method to determine the estimated monthly cost of an Azure service or resource. Customer support may assist with other inquiries or issues, but they do not provide cost estimates for Azure services.

### **By analyzing the usage data of the resource**

#### **Explanation**

Analyzing the usage data of the resource may give insights into the actual usage patterns and costs incurred, but it does not provide an estimated monthly cost for an Azure service or resource. The estimated cost is based on the pricing information provided by Azure.

### **Overall explanation**

**The Azure Pricing Calculator** is a free tool that can be used to estimate the monthly cost of Azure services and resources based on factors such as region, usage, and quantity. It allows users to select specific Azure services and configurations and provides an estimated monthly cost based on the chosen parameters.

Other options:

**By contacting Microsoft customer support :** This is incorrect because contacting Microsoft customer support is not a reliable method to determine the estimated monthly cost of an Azure service or resource.

**By analyzing the usage data of the resource:** This is incorrect because analyzing the usage data of a resource can help in optimizing costs but it does not provide an estimated monthly cost.

**By checking the current Azure Marketplace pricing:** This is incorrect because checking the current Azure Marketplace pricing does not necessarily provide the estimated monthly cost of a particular service or resource.

**Reference:** <https://learn.microsoft.com/en-us/azure/cost-management-billing/understand/plan-manage-costs>

## Domain

Describe Azure management and governance

### Question 55 Skipped

**What is Microsoft Entra ID?**

**A cloud-based network security service**

#### Explanation

Microsoft Entra ID is not a cloud-based network security service. It is focused on identity and access management rather than network security.

#### Correct answer

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

#### Explanation

Microsoft Entra ID is a cloud-based identity and access management service provided by Microsoft. It helps organizations manage user identities and control access to resources in the cloud.

**A cloud-based application deployment service**

#### Explanation

Microsoft Entra ID is not a cloud-based application deployment service. It is primarily focused on identity and access management, not on deploying applications to the cloud.

## A cloud-based storage solution

### Explanation

Microsoft Entra ID is not a cloud-based storage solution. It is specifically designed for managing user identities and access to resources, rather than storing data.

### Overall explanation

Microsoft Entra ID is an integrated cloud identity and access solution, and a leader in the market for managing directories, enabling access to applications, and protecting identities.

**Reference:** <https://www.microsoft.com/en-ca/security/business/identity-access/microsoft-entra-id>

### Domain

Describe Azure architecture and services

## Question 56 Skipped

**Which of the following displays personalized recommendations for all your subscriptions, and you can use filters to select recommendations for specific subscriptions, resource groups, or services?**

### Azure Arc

### Explanation

Azure Arc is a tool that extends Azure management and services to any infrastructure, including on-premises, multi-cloud, and edge environments. It does not provide personalized recommendations or the ability to filter recommendations for specific subscriptions, resource groups, or services like Azure Advisor does.

### Azure Monitor

### Explanation

Azure Monitor is not the correct choice for this scenario. While Azure Monitor provides monitoring and insights into your Azure resources, it does not specifically offer personalized recommendations or the ability to filter recommendations for specific subscriptions, resource groups, or services.

## Azure Service Health

### Explanation

Azure Service Health focuses on providing information about the health of Azure services and regions, including ongoing incidents and planned maintenance. It does not offer personalized recommendations or the ability to filter recommendations for specific subscriptions, resource groups, or services.

**Correct answer**

## Azure Advisor

### Explanation

Azure Advisor is the correct choice as it provides personalized recommendations for all your subscriptions. It allows you to use filters to select recommendations for specific subscriptions, resource groups, or services, making it a versatile tool for optimizing your Azure resources.

## Overall explanation

### From the Official Azure Documentation:

[Azure Advisor](#) evaluates your Azure resources and makes recommendations to help improve reliability, security, and performance, achieve operational excellence, and reduce costs. Advisor is designed to help you save time on cloud optimization. The recommendation service includes suggested actions you can take right away, postpone, or dismiss.

The recommendations are available via the Azure portal and the API, and you can set up notifications to alert you to new recommendations.

When you're in the Azure portal, the **Advisor** dashboard displays personalized recommendations for all your subscriptions, and you can use filters to select recommendations for specific subscriptions, resource groups, or services.

**Reference:** <https://docs.microsoft.com/en-ca/learn/modules/monitoring-fundamentals/2-identify-product-options>

## Domain

Describe Azure management and governance

### Question 57 Skipped

An organization would like to create a web app to allow its employees to enter their vacation / time-off details and then store that information in a backend storage solution. They have noted that Python is their preferred language.

As the lead consultant, which service would you recommend?

#### Azure Functions

##### Explanation

Azure Functions are serverless compute services that allow you to run event-triggered code without managing servers. While they can be used for specific tasks or functions within an application, they may not be the best choice for hosting a complete web app with user input and backend storage requirements.

##### Correct answer

#### Azure App Service

##### Explanation

Azure App Service is the most suitable option for hosting web applications like the one described in the question. It supports multiple programming languages, including Python, and provides a fully managed platform for building, deploying, and scaling web apps without managing the underlying infrastructure.

#### Azure Cosmos DB

##### Explanation

Azure Cosmos DB is a globally distributed, multi-model database service that may be overkill for the requirements of a simple web app to store vacation/time-off details.

While it provides scalability and high availability for data storage, it may introduce unnecessary complexity and cost for this scenario.

## Azure Kubernetes

### Explanation

Azure Kubernetes is a container orchestration service that may be more complex than necessary for a simple web app like the one described. While it can be used to deploy and manage containerized applications, it may not be the most straightforward solution for a Python-based web app with basic functionality.

### Overall explanation

From the official Azure docs:

**Azure App Service** is an HTTP-based service for hosting web applications, REST APIs, and mobile back ends. You can develop in your favorite language, be it .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python. Applications run and scale with ease on both Windows and [Linux](#)-based environments.



Mobile Apps



API Apps



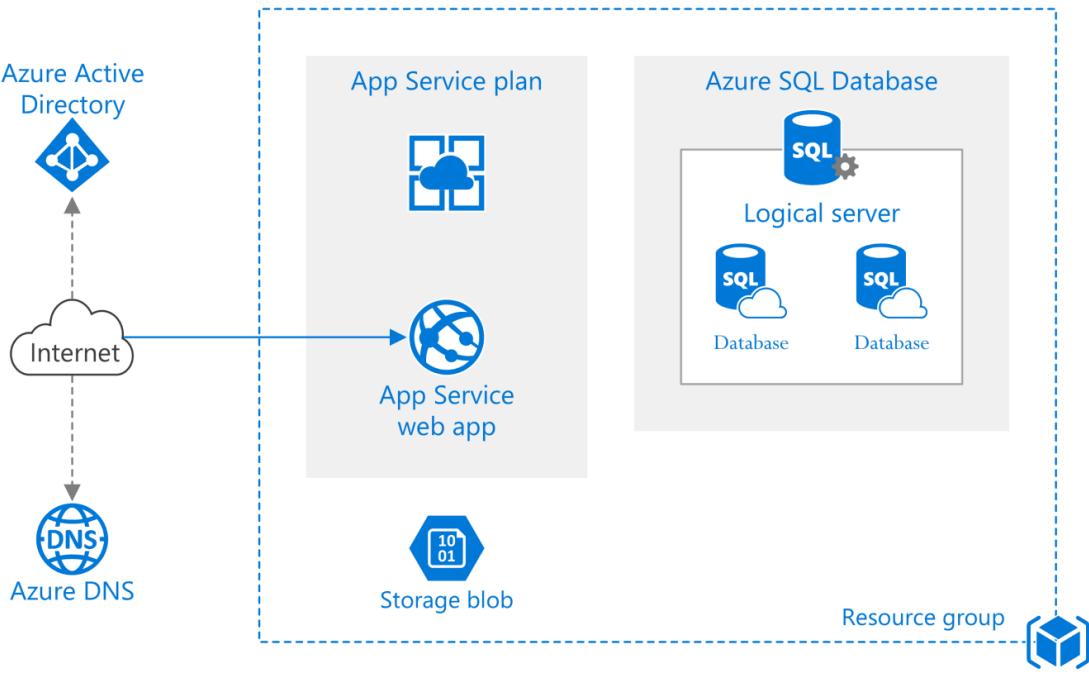
Web Apps



Function Apps



**It is also possible to scale apps on an enterprise grade platform:**



**Reference :** <https://docs.microsoft.com/en-us/azure/app-service/overview>

## Domain

Describe Azure architecture and services

### Question 58 Skipped

**When assigning Azure role-based access control (Azure RBAC) at the management group level, which of the following occurs?**

**Correct answer**

**Permissions are inherited by all sub-management groups, subscriptions, resource groups, and resources under the management group.**

## Explanation

When Azure RBAC is assigned at the management group level, the permissions are inherited by all sub-management groups, subscriptions, resource groups, and resources under the management group. This allows for consistent access control across all resources within the hierarchy.

## **Permissions are restricted to the management group level only.**

### **Explanation**

Permissions assigned at the management group level are not restricted to that level only. They are inherited by all resources under the management group, including subscriptions, resource groups, and individual resources.

## **Permissions are assigned individually for each subscription under the management group.**

### **Explanation**

Permissions are not assigned individually for each subscription under the management group when Azure RBAC is applied at the management group level. Instead, the permissions are inherited by all resources under the management group, including subscriptions.

## **Permissions apply only to the resources within the management group.**

### **Explanation**

Contrary to this choice, permissions assigned at the management group level do not apply only to the resources within the management group. They are inherited by all resources under the management group, providing a broader scope of access control.

## **Overall explanation**

Permissions are inherited by **all** sub-management groups, subscriptions, resource groups, and resources under the management group.

When you assign Azure role-based access control (Azure RBAC) at the management group level, the permissions are inherited by all sub-management groups, subscriptions, resource groups, and resources under the management group. This approach simplifies access management and helps maintain consistency across the organization.

**Reference:** <https://learn.microsoft.com/en-us/training/modules/describe-core-architectural-components-of-azure/6-describe-azure-management-infrastructure>

## Domain

Describe Azure management and governance

### Question 59 Skipped

Yes or No:

**We get total control of the underlying Operating System when working with Platform As a Service (PaaS) solutions.**

**Correct answer**

**No**

#### Explanation

In Platform As a Service (PaaS) solutions, the cloud provider manages the underlying Operating System, providing a fully managed platform for deploying and running applications. Users do not have direct access or control over the Operating System, as it is abstracted to simplify application development and deployment.

**Yes**

#### Explanation

When working with Platform As a Service (PaaS) solutions, the underlying Operating System is abstracted and managed by the cloud provider. Users do not have direct control over the Operating System, as the focus is on deploying and managing applications rather than managing the infrastructure.

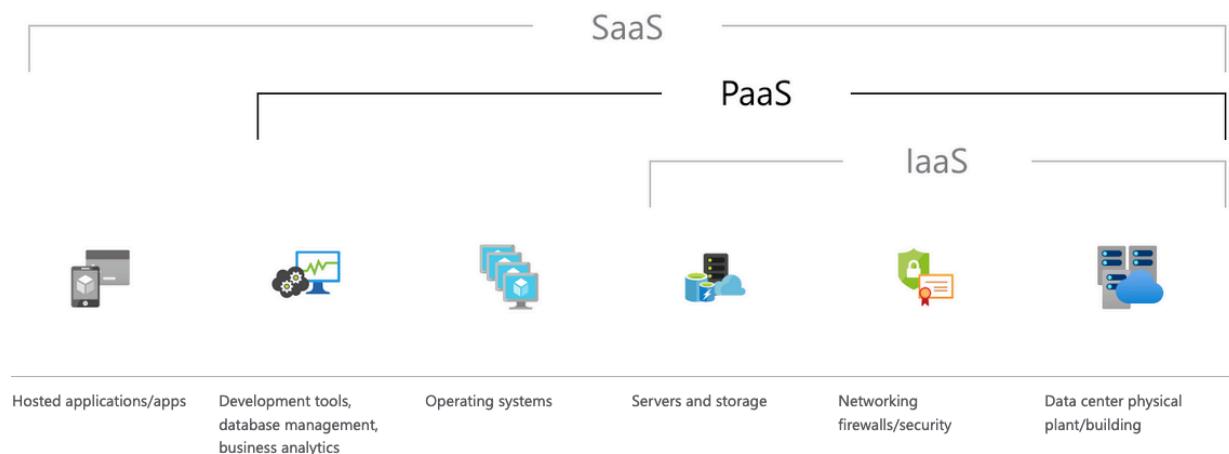
#### Overall explanation

**From the official Azure documentation:**

**Platform as a service (PaaS)** is a complete development and deployment environment in the cloud, with resources that enable you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications. You purchase the resources you need from a [cloud service provider](#) on a pay-as-you-go basis and access them over a secure Internet connection.

Like [IaaS](#), 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.

PaaS allows you to avoid the expense and complexity of buying and managing software licenses, the underlying application infrastructure and middleware, container orchestrators such as [Kubernetes](#), or the development tools and other resources. You manage the applications and services you develop, and the cloud service provider **typically manages everything else**.



A great image to reference for such concepts -

[\(Important\)](https://www.redhat.com/en/topics/cloud-computing/iaas-vs-paas-vs-saas)

**Reference:** <https://azure.microsoft.com/en-us/overview/what-is-paas/>

## Domain

Describe Cloud Concepts

## Question 60 Skipped

**Yes or No:**

**Your company has explored some of the services in Azure Public preview. One of the architects working in your team has advised to deploy mission critical services/applications to these services. Are they correct?**

**Yes**

### **Explanation**

Deploying mission critical services or applications to services in Azure Public preview is not recommended. Services in preview may still be undergoing testing and development, and there could be potential issues or changes that could impact the stability and reliability of the services. It is advisable to wait until the services are generally available before deploying mission critical workloads to ensure a more stable and supported environment.

**Correct answer**

**No**

### **Explanation**

The architect advising against deploying mission critical services or applications to services in Azure Public preview is correct. It is important to prioritize stability, reliability, and support when deploying critical workloads. Waiting for services to be generally available ensures a more mature and tested environment, reducing the risk of potential issues or changes impacting the performance of mission critical applications.

### **Overall explanation**

According to the official documentation, it is important to note that the services offered in public preview are **excluded from the Service Level Agreements (SLAs)**. **It is therefore not a good idea to deploy production environments on resources / services that are in preview (public or private).**

Azure may include preview, beta, or other pre-release features, services, software, or regions offered by Microsoft to obtain customer feedback ("Previews"). Previews are made available to you on the condition that you agree to these terms of use, which supplement [your agreement](#) governing use of Azure.

PREVIEWS ARE PROVIDED "AS-IS," "WITH ALL FAULTS," AND "AS AVAILABLE," AND ARE EXCLUDED FROM THE SERVICE LEVEL AGREEMENTS AND LIMITED WARRANTY.

Previews may not be covered by customer support. Previews may be subject to reduced or different security, compliance and privacy commitments, as further explained in the [Microsoft Online Services Privacy Statement](#), [Microsoft Azure Trust Center](#), the [Online Services Terms](#), and any additional notices provided with the Preview. Customers should not use Previews to process Personal Data or other data that is subject to heightened compliance requirements. Certain named Previews may also be subject to additional terms set forth below, if any. We may change or discontinue Previews at any time without notice. We also may choose not to release a Preview into "General Availability."

**Reference :** <https://azure.microsoft.com/en-ca/support/legal/preview-supplemental-terms/>

**Domain**

### Question 61 Skipped

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

#### 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. Since you want to move your existing app to Azure and be relieved of manual administration and maintenance, SaaS may not provide the level of control and customization you require.

##### 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 and environment for developers to build, deploy, and manage applications without the complexity of infrastructure management. This would allow you to focus on developing and running your app without worrying about the underlying infrastructure.

#### Infrastructure as a Service (IaaS)

##### Explanation

Infrastructure as a Service (IaaS) involves renting virtualized hardware resources over the internet. While IaaS provides more control over the infrastructure compared to PaaS, it still requires manual administration and maintenance, which is something you want to avoid. Therefore, IaaS may not be the best choice for your use case.

## Database as a Service (DaaS)

### Explanation

Database as a Service (DaaS) is a cloud service model that provides database management and maintenance. While DaaS can be beneficial for offloading database management tasks, it may not address all the manual administration and maintenance requirements for your entire application. Therefore, DaaS may not be the most suitable option for your use case of moving your app to Azure and reducing manual tasks.

### Overall explanation

Platform as a service (PaaS) is a complete development and deployment environment in the cloud, with resources that enable you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications. You purchase the resources you need from a cloud service provider on a pay-as-you-go basis and access them over a secure Internet connection.

Like [IaaS](#), 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.

**PaaS allows you to avoid the expense and complexity of buying and managing software licenses, the underlying application infrastructure and middleware, container orchestrators such as [Kubernetes](#), or the development tools and other resources. You manage the applications and services you develop, and the cloud service provider typically manages everything else.**

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

### Domain

Describe Cloud Concepts

### Question 62 Skipped

**Yes or No: Permissions are by default inherited by all resources residing in a resource group.**

**No**

**Explanation**

No explanation is provided for this choice since it is not the correct answer.

**Correct answer**

**Yes**

**Explanation**

Yes, permissions are by default inherited by all resources residing in a resource group in Azure. This means that when you assign permissions to a resource group, all resources within that group inherit those permissions unless explicitly overridden at the resource level.

**Overall explanation**

**From the official docs:**

A resource group can be used to scope access control for administrative actions. By default, permissions set at the resource level **are inherited** by the resources in the resource group.

More info about resources :

# Resource groups

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

- All the resources in your resource group should share the same lifecycle. You deploy, update, and delete them together. If one resource, such as a server, needs to exist on a different deployment cycle it should be in another resource group.
- Each resource can exist in only one resource group.
- You can add or remove a resource to a resource group at any time.
- You can move a resource from one resource group to another group. For more information, see [Move resources to new resource group or subscription](#).
- The resources in a resource group can be located in different regions than the resource group.
- When you create a resource group, you need to provide a location for that resource group.

You may be wondering, "Why does a resource group need a location? And, if the resources can have different locations than the resource group, why does the resource group location matter at all?"

The resource group stores metadata about the resources. When you specify a location for the resource group, you're specifying where that metadata is stored. For compliance reasons, you may need to ensure that your data is stored in a particular region.

If a resource group's region is temporarily unavailable, you can't update resources in the resource group because the metadata is unavailable. The resources in other regions will still function as expected, but you can't update them. This condition doesn't apply to global resources like Azure Content Delivery Network, Azure DNS, Azure Traffic Manager, and Azure Front Door.

For more information about building reliable applications, see [Designing reliable Azure applications](#).

- A resource group can be used to scope access control for administrative actions. To manage a resource group, you can assign [Azure Policies](#), [Azure roles](#), or [resource locks](#).
- You can [apply tags](#) to a resource group. The resources in the resource group don't inherit those tags.
- A resource can connect to resources in other resource groups. This scenario is common when the two resources are related but don't share the same lifecycle. For example, you can have a web app that connects to a database in a different resource group.
- When you delete a resource group, all resources in the resource group are also deleted. For information about how Azure Resource Manager orchestrates those deletions, see [Azure Resource Manager resource group and resource deletion](#).

**References:** <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview>

## Domain

Describe Azure architecture and services

## Question 63 Skipped

**Yes or No:**

**It is possible to deploy Azure resources through a Tablet by using Bash in the Azure Cloud Shell.**

**Correct answer**

**Yes**

### **Explanation**

Yes, it is possible to deploy Azure resources through a Tablet by using Bash in the Azure Cloud Shell. The Azure Cloud Shell provides a browser-based shell experience that enables access to Azure resources from virtually anywhere, including tablets. Users can use the Bash environment within the Cloud Shell to manage Azure resources, run scripts, and execute commands to deploy and manage resources in Azure.

**No**

### **Overall explanation**

From the official docs:

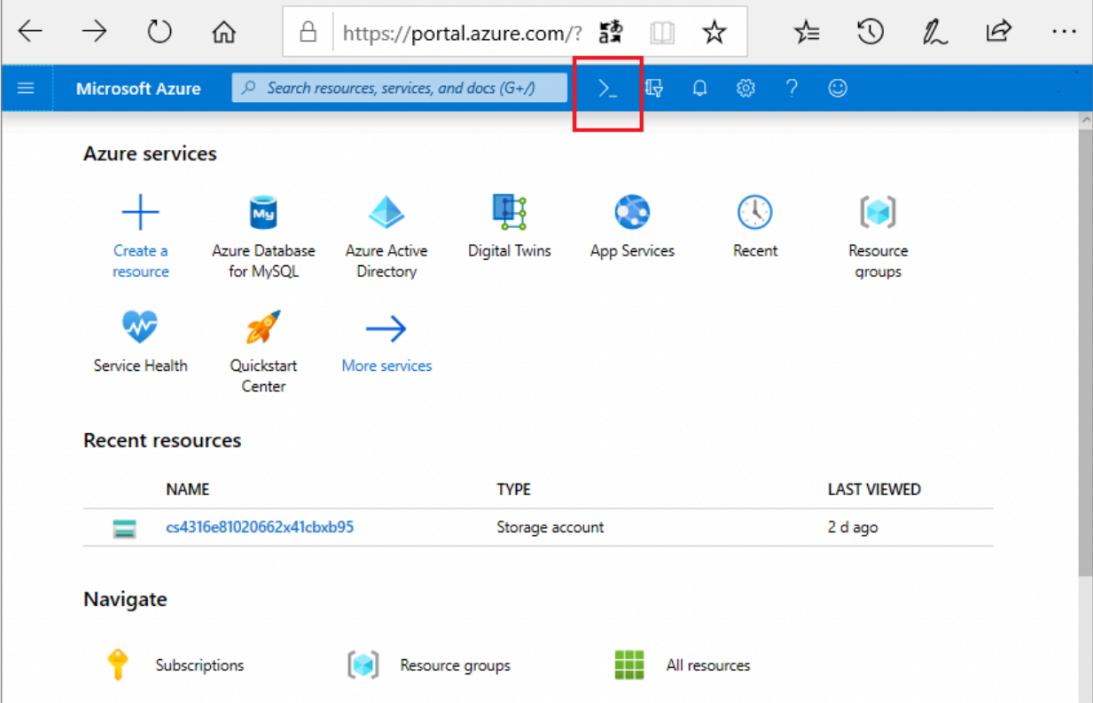
Azure Cloud Shell is an interactive, authenticated, **browser-accessible (the key to everything since all you need is a browser and the OS doesn't matter)** shell for managing Azure resources. It provides the flexibility of choosing the shell experience that best suits the way you work, **either Bash or PowerShell**.

All you need is a **browser** on your Tablet, and then:

# Choice of preferred shell experience

Users can choose between Bash or PowerShell.

1. Select Cloud Shell.

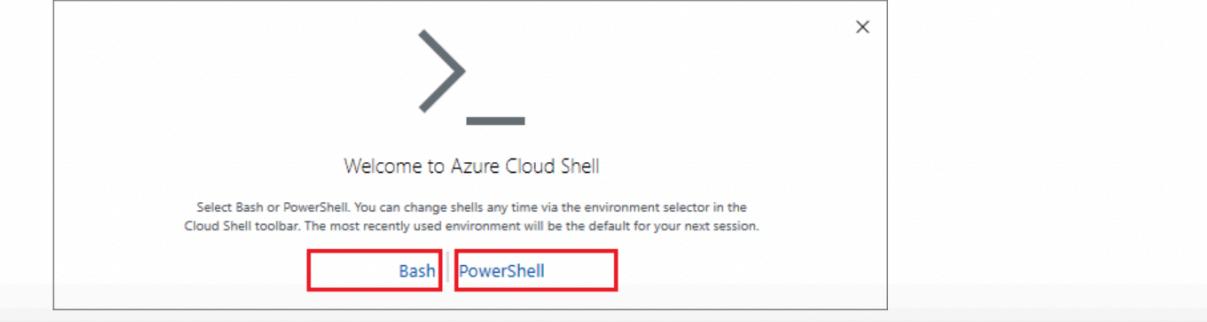


The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with various icons and a search bar. To the right of the search bar is a small icon of a terminal window with a right-pointing arrow, which is the Cloud Shell icon. This icon is highlighted with a red box. Below the header, there's a section titled "Azure services" with several service icons like Create a resource, Azure Database for MySQL, and App Services. Further down is a "Recent resources" table:

NAME	TYPE	LAST VIEWED
cs4316e81020662x41cxb95	Storage account	2 d ago

At the bottom, there's a "Navigate" section with links for Subscriptions, Resource groups, and All resources.

2. Select Bash or PowerShell.



The screenshot shows the Azure Cloud Shell welcome screen. It features a large "Welcome to Azure Cloud Shell" message with a large right-pointing arrow icon above it. Below the message, there's a note: "Select Bash or PowerShell. You can change shells any time via the environment selector in the Cloud Shell toolbar. The most recently used environment will be the default for your next session." At the bottom, there are two buttons: "Bash" and "PowerShell", both of which are highlighted with red boxes.

**Reference:** <https://docs.microsoft.com/en-us/azure/cloud-shell/quickstart>  
<https://docs.microsoft.com/en-us/azure/cloud-shell/overview>

## Domain

Describe Azure management and governance

## Question 64 Skipped

**Which of the following actions can help you reduce your Azure costs?**

**Increasing the number of virtual machines deployed**

## Explanation

Increasing the number of virtual machines deployed will actually lead to higher Azure costs as you will be paying for more resources. It is important to right-size your resources and only deploy the necessary number of virtual machines to avoid unnecessary expenses.

#### Correct answer

### Reducing the amount of data transferred between Azure regions

#### Explanation

Reducing the amount of data transferred between Azure regions can help lower costs as data transfer fees can add up quickly. By optimizing your data transfer patterns and minimizing unnecessary data movement, you can effectively reduce your Azure costs.

### Keeping all virtual machines running 24/7

#### Explanation

Keeping all virtual machines running 24/7 will result in higher costs as you will be paying for the compute resources continuously. It is recommended to utilize cost-saving measures such as scheduling virtual machines to shut down during off-peak hours or using auto-scaling to adjust resources based on demand.

### Enabling automatic scaling for all virtual machines

#### Explanation

Enabling automatic scaling for all virtual machines can help optimize costs by automatically adjusting the number of virtual machines based on demand. This ensures that you are only paying for the resources you need at any given time, reducing costs associated with over-provisioning.

#### Overall explanation

Reducing the amount of data transferred between Azure regions can help reduce costs by minimizing data egress charges.

#### Other options:

- **Deploying more virtual machines:** This can actually increase costs if they are not utilized efficiently.
- **Enabling automatic scaling:** This can help optimize resource usage and reduce costs, but it depends on the specific workload and usage patterns.
- **Keeping virtual machines running 24/7:** This can result in unnecessary costs, especially if they are not utilized all the time. It is recommended to use automation to start and stop VMs based on usage patterns.

**Reference:** <https://learn.microsoft.com/en-us/azure/cost-management-billing/cost-management-billing-overview>

## Domain

Describe Azure management and governance

### Question 65 Skipped

**What is the default maximum capacity for storage accounts?**

**Correct answer**

**5 PiB**

## Explanation

The default maximum capacity for storage accounts in Microsoft Azure is 5 PiB (Pebibytes). This capacity allows for storing a large amount of data within the storage account without the need for additional configuration or scaling.

**750 TiB**

## Explanation

The default maximum capacity for storage accounts in Microsoft Azure is not 750 TiB. The correct default maximum capacity is 5 PiB, which offers a much larger storage capacity for storing data within the storage account.

## 2 PiB

### Explanation

The default maximum capacity for storage accounts in Microsoft Azure is not 2 PiB. The correct default maximum capacity is 5 PiB, which provides a larger storage capacity for data storage and management.

## 400 TB

### Explanation

The default maximum capacity for storage accounts in Microsoft Azure is not 400 TB. The correct default maximum capacity is 5 PiB, which is significantly larger than 400 TB.

### Overall explanation

Referring to the official Azure docs:

#### **The maximum storage account capacity currently is : 5PiB**

\*These might change with time so if you feel it has changed, inform me through message or in the Q/A section, I'll highly appreciate it :)

## Scale targets for standard storage accounts

The following table describes default limits for Azure general-purpose v1, v2, Blob storage, block blob storage, and Data Lake Storage Gen2 enabled storage accounts. The *ingress* limit refers to all data that is sent to a storage account. The *egress* limit refers to all data that is received from a storage account.

Resource	Limit
Number of storage accounts per region per subscription, including standard, premium, and Data Lake Storage Gen2 enabled storage accounts. <sup>3</sup>	250
Maximum storage account capacity	5 PiB <sup>1</sup>

**Reference :** <https://docs.microsoft.com/en-us/azure/storage/common/scalability-targets-standard-account>

## Domain

Describe Azure architecture and services

### Question 66 Skipped

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

Would you agree with this implementation?

**Correct answer**

**No**

**Yes**

## Explanation

Azure App Service is a PaaS offering for hosting web applications, while Azure Virtual Machines are IaaS offerings for running virtualized servers. Also, this combination may introduce unnecessary complexity and management overhead for a simple POC.

## Overall explanation

An Azure App Service is a **PaaS** (Platform as a Service) example so this is not an issue.

However, Azure Virtual machines fall under the category of **IaaS** (Infrastructure as a Service) service since you're renting infrastructure. Therefore, we would disagree with this decision.

## References:

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

## Domain

Describe Cloud Concepts

### Question 67 Skipped

You can significantly reduce costs (up-to 72%) as compared to pay-as-you-go pricing by \_\_\_\_\_.

#### Using the free tier

##### Explanation

While using the free tier can help you avoid certain costs for limited usage, it may not provide the same level of cost reduction as using Reserved Instances, which offer deeper discounts for committed usage over a longer period.

#### Provisioning a lot of resources

##### Explanation

Provisioning a lot of resources may actually increase costs as you would be paying for resources that are not being fully utilized. It is important to right-size your resources to avoid unnecessary expenses.

#### Not using a lot of resources

##### Explanation

Not using a lot of resources can help reduce costs to some extent, but it may not provide the same level of cost savings as using Reserved Instances, which offer discounted rates for committed usage. It is important to optimize resource usage and consider cost-saving options like Reserved Instances for significant cost reduction.

Correct answer

## Using Reserved Instances

### Explanation

Using Reserved Instances allows you to commit to a specific amount of usage for a one- or three-year term, which can result in significant cost savings compared to pay-as-you-go pricing. This option provides a discounted rate for the committed usage.

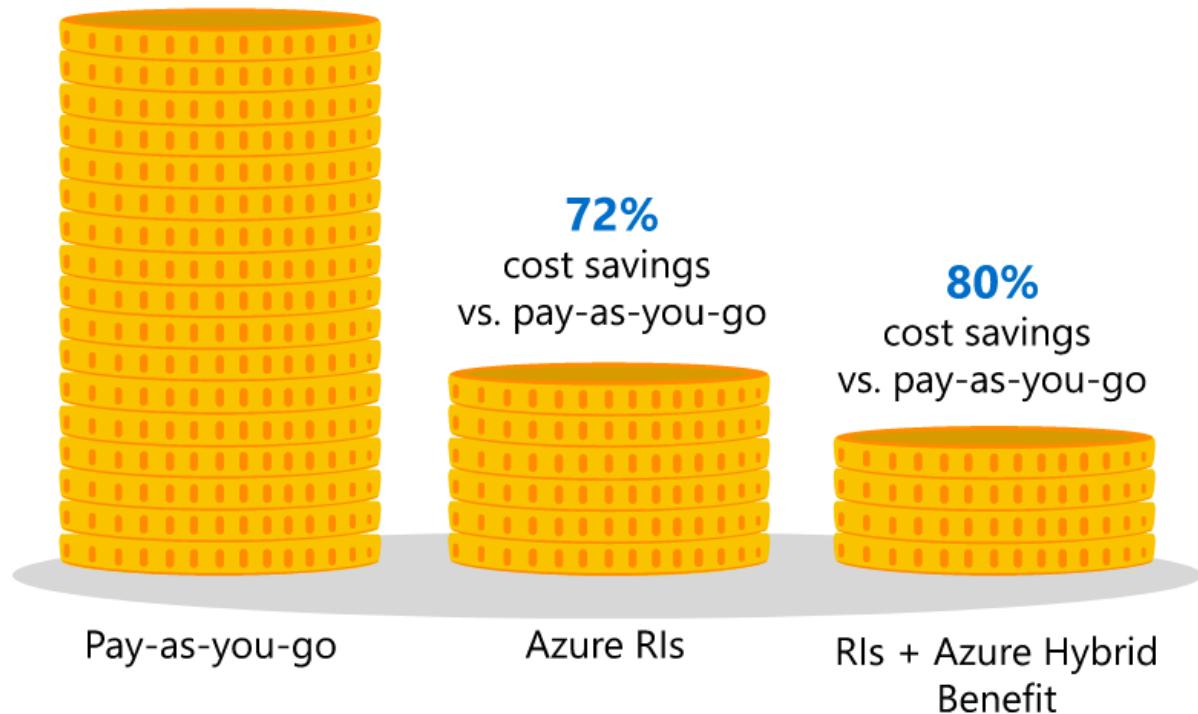
### Overall explanation

You can significantly reduce costs — **up to 72 percent** compared to pay-as-you-go prices—with

one-year or three-year terms on Windows and Linux virtual machines (VMs). When you combine the cost savings gained from **Azure RIs (reserved instances)** with the added value of the Azure Hybrid Benefit, you can save up to 80 percent\*\*.

It is possible to lower your total cost of ownership by combining Azure Reserved Instances with pay-as-you-go prices to manage costs across predictable and variable workloads. In many cases, you can further reduce your costs with reserved instance size flexibility.

Save up to **80%** with RIs and Azure Hybrid Benefit



**Reference :** <https://azure.microsoft.com/en-us/pricing/reserved-vm-instances/>

## Domain

Describe Azure management and governance

### Question 68 Skipped

**True or False: Resources don't inherit the tags you apply to a resource group or a subscription.**

#### Correct answer

**True**

#### Explanation

True. Resources in Azure do not automatically inherit the tags applied to a resource group or subscription. Tags must be explicitly applied to each individual resource to ensure consistent tagging across all resources within a resource group or subscription.

**False**

#### Explanation

False. Resources in Azure do not inherit tags from a resource group or subscription by default. Each resource must have tags applied individually to ensure proper tagging and organization within Azure.

## Overall explanation

From the official docs :

Yes, this is true. Resources **don't** inherit the tags you apply to a resource group or a subscription. To apply tags from a subscription or resource group to the resources, see [Azure Policies - tags](#).

**Reference:** <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal#tag-resource-groups>

## Domain

Describe Azure management and governance

### Question 69 Skipped

**You've been asked by senior management to prepare a presentation describing not only the benefits, but also the estimated cost savings you can realize by migrating your workloads to Azure. As the lead architect, which service would you use for these calculations?**

**Correct answer**

**Azure TCO calculator**

## Explanation

The Azure TCO (Total Cost of Ownership) calculator is specifically designed to help organizations estimate the cost savings and benefits of migrating their workloads to Azure. It provides a detailed breakdown of the costs associated with running workloads on-premises versus in the cloud, allowing you to make informed decisions about migration.

**Azure Advisor**

## Explanation

Azure Advisor is a service that provides personalized recommendations to help you optimize your Azure resources for performance, security, and cost. While it can help you make cost-effective decisions about your Azure resources, it is not the primary tool for calculating the estimated cost savings of migrating workloads to Azure.

**Azure Cost Management**

## Explanation

Azure Cost Management is a service that helps you track and optimize your Azure spending. While it provides valuable insights into your current usage and costs, it is

not specifically designed for calculating the estimated cost savings of migrating workloads to Azure.

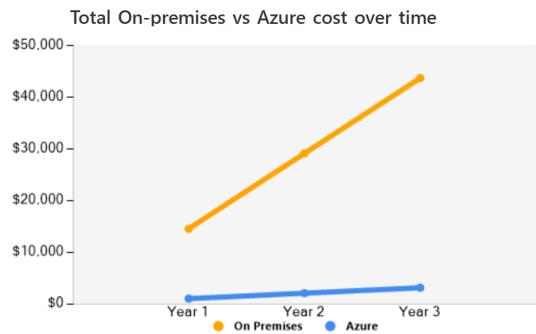
## Azure Monitor

### Explanation

Azure Monitor is a service that helps you monitor the performance and availability of your applications and services running on Azure. While it provides valuable insights into the health of your resources, it is not designed for calculating cost savings or estimating the financial benefits of migrating workloads to Azure.

### Overall explanation

For users wishing to adopt cloud services, Azure provides a web-based TCO Calculator. You can use this calculator to estimate the **costs of migrating your data and applications to Azure and predict potential savings**.



Your estimated cost savings could be as much as

**\$40,617 (93%)**

over 3 year(s) with Microsoft Azure

Estimated cost savings over 3 year(s) by category

Compute	\$25,087
Data center	\$5,094
Networking	\$7,715
Storage	\$1,741
- IT labor	\$980

#### On-premises cost breakdown summary

Category	Costs
Compute	\$26,651
Hardware	\$23,282
Software	\$2,315
Electricity	\$1,054
Data center	\$5,094
Networking	\$7,715
Storage	\$2,662
IT labor	\$1,654
<b>Total</b>	<b>\$43,776</b>

#### Azure cost breakdown summary

Category	Web direct cost	1 Year Reserved VM	3 Year Reserved VM
Compute	\$4,216	\$2,521	\$1,564
Data center	\$0	\$0	\$0
Networking	\$0	\$0	\$0
Storage	\$921	\$921	\$921
IT labor	\$674	\$674	\$674
<b>Total</b>	<b>\$5,812</b>	<b>\$4,116</b>	<b>\$3,160</b>

Reference: <https://azure.microsoft.com/en-in/pricing/tco/calculator/>

## Domain

Describe Azure management and governance

### Question 70 Skipped

**A startup is developing a mobile application that experiences unpredictable traffic spikes. Which cloud pricing model would best accommodate these fluctuations while minimizing costs?**

#### Spot instances

##### Explanation

Spot instances offer significant cost savings compared to on-demand instances but are not suitable for a startup with unpredictable traffic spikes. Spot instances can be interrupted by the cloud provider if the market price exceeds the bid price, potentially causing disruptions during peak traffic periods.

#### Dedicated hosts

##### Explanation

Dedicated hosts provide physical servers dedicated to a single customer, which may not be cost-effective for a startup with unpredictable traffic spikes. Dedicated hosts require a fixed commitment and may not offer the flexibility needed to scale resources based on fluctuating demand, potentially leading to higher costs.

#### Correct answer

#### Pay-as-you-go

##### Explanation

The pay-as-you-go pricing model allows the startup to only pay for the resources they use, making it ideal for unpredictable traffic spikes. This model provides flexibility to scale resources up or down based on demand, helping to minimize costs during low-traffic periods.

## Reserved instances

### Explanation

Reserved instances require a commitment to a specific amount of resources for a fixed term, which may not be suitable for a startup experiencing unpredictable traffic spikes. While reserved instances offer cost savings for steady workloads, they may not be cost-effective during fluctuating traffic patterns.

### Overall explanation

**Pay-as-you-go** offers the highest flexibility to adjust resource usage based on demand. As the startup experiences unpredictable traffic spikes, they can easily scale up resources when needed and pay only for what they use.

**Reference:** <https://azure.microsoft.com/en-us/pricing/purchase-options/pay-as-you-go>

### Domain

Describe Cloud Concepts

### Question 71 Skipped

For industries that work with highly sensitive data, such as banking, finance, government, and healthcare, \_\_\_\_\_ cloud may be their best cloud option.

**Private**

**Correct answer**

**Hybrid**

### Explanation

Hybrid cloud combines the benefits of both private and public cloud models, allowing organizations to leverage the scalability and cost-effectiveness of public cloud services while maintaining sensitive data and critical workloads on-premises or in a private cloud environment. This hybrid approach provides flexibility, security, and

compliance for industries like banking, finance, government, and healthcare that require a balance between security and agility.

## Public

### Overall explanation

#### From the official docs:

For industries that work with highly sensitive data, such as banking, finance, government, and healthcare, hybrid may be their best cloud option. For example, some regulated industries require certain types of data to be stored on-premises while allowing less sensitive data to be stored on the cloud. In this kind of hybrid cloud architecture, organizations gain the flexibility of the public cloud for less regulated computing tasks, while still meeting their industry requirements.

**Reference:** <https://azure.microsoft.com/en-gb/overview/what-is-hybrid-cloud-computing/>

## Domain

Describe Cloud Concepts

### Question 72 Skipped

**During live telecasts of football matches, streaming platforms sometimes experience massive spikes in viewerships and users visiting their websites when a goal is scored. Which of the following would be beneficial to deal with such expected demand of resources?**

## Virtual Machines

### Explanation

Virtual Machines require manual provisioning, configuration, and scaling, which may not be efficient for handling unexpected spikes in resource demand during live events. They are not as agile or cost-effective as serverless computing for handling fluctuating workloads.

## Containers

### Explanation

Containers provide a lightweight, portable, and scalable solution for deploying applications. While they can help with resource management and scalability, they may not be the most efficient option for handling sudden spikes in demand during live events like football matches.

## Kubernetes

### Explanation

Kubernetes is a container orchestration tool that helps automate the deployment, scaling, and management of containerized applications. While it can improve resource utilization and scalability, it may not be the most suitable choice for handling unpredictable spikes in viewership during live events.

### Correct answer

## Serverless Computing

### Explanation

Serverless Computing allows developers to focus on writing code without worrying about managing servers or infrastructure. It automatically scales based on demand, making it an ideal choice for handling sudden spikes in viewership during live telecasts of football matches.

### Overall explanation

**Serverless computing** enables developers to build applications faster by eliminating the need for them to manage infrastructure. With serverless applications, the cloud service provider automatically provisions, scales, and manages the infrastructure required to run the code.

While understanding the definition of serverless computing, it's important to note that servers are still running the code. The serverless name comes from the fact that the tasks associated with infrastructure provisioning and management are invisible to the developer. This approach enables developers to increase their focus on the **business logic and deliver more value to the core of the business (IMPORTANT)**. Serverless

computing helps teams increase their productivity and bring products to market faster, and it allows organizations to better optimize resources and stay focused on innovation.

### Top benefits of serverless computing



#### No infrastructure management

Using fully managed services enables developers to avoid administrative tasks and focus on core business logic. With a serverless platform, you simply deploy your code, and it runs with high availability.



#### Dynamic scalability

With serverless computing, the infrastructure dynamically scales up and down within seconds to match the demands of any workload.



#### Faster time to market

Serverless applications reduce the operations dependencies on each development cycle, increasing development teams' agility to deliver more functionality in less time.



#### More efficient use of resources

Shifting to serverless technologies helps organizations reduce TCO and reallocate resources to accelerate the pace of innovation.

**Reference :** <https://azure.microsoft.com/en-us/overview/serverless-computing/>

### Domain

Describe Cloud Concepts

### Question 73 Skipped

\_\_\_\_\_ is an agreement with Microsoft to use one or more Microsoft cloud platforms or services, for which charges accrue based on either a per-user license fee or on cloud-based resource consumption.

#### A License

#### Explanation

A License typically refers to the permission to use a specific software or service. While licenses are important for accessing and using Microsoft products, they do not specifically represent an agreement with Microsoft for cloud platform or service usage as described in the question.

#### A Resource Group

#### Explanation

A Resource Group is a logical container that holds related resources for an Azure solution. While it is an important concept in Azure for organizing and managing resources, it is not directly related to an agreement with Microsoft for cloud platform or service usage.

#### **Correct answer**

### **A Subscription**

#### **Explanation**

A Subscription is the correct choice as it refers to an agreement with Microsoft to use their cloud platforms or services. Charges for the subscription can be based on a per-user license fee or on cloud-based resource consumption, making it the appropriate option for this scenario.

### **A User Account**

#### **Explanation**

A User Account is an identity created for a user to access Azure services. While user accounts are essential for managing access and permissions within Azure, they do not represent an agreement with Microsoft for cloud platform or service usage.

#### **Overall explanation**

According to the official docs -

# Subscriptions

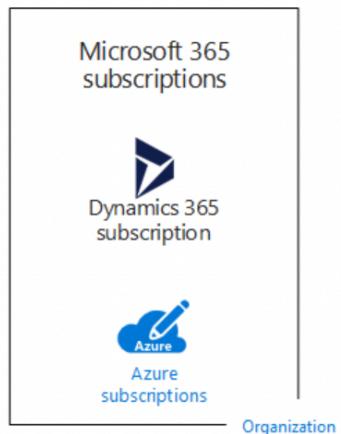
A subscription is an agreement with Microsoft to use one or more Microsoft cloud platforms or services, for which charges accrue based on either a per-user license fee or on cloud-based resource consumption.

- Microsoft's Software as a Service (SaaS)-based cloud offerings (Microsoft 365 and Dynamics 365) charge per-user license fees.
- Microsoft's Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud offerings (Azure) charge based on cloud resource consumption.

You can also use a trial subscription, but the subscription expires after a specific amount of time or consumption charges. You can convert a trial subscription to a paid subscription.

Organizations can have multiple subscriptions for Microsoft's cloud offerings. Figure 1 shows a single organization that has multiple Microsoft 365 subscriptions, a Dynamics 365 subscription, and multiple Azure subscriptions.

Figure 1: Example of multiple subscriptions for an organization



## References:

<https://docs.microsoft.com/en-us/office365/enterprise/subscriptions-licenses-accounts-and-tenants-for-microsoft-cloud-offerings>

## Domain

Describe Azure architecture and services

## Question 74 Skipped

**When computing and processing demand increases beyond an on-premises datacenter's capabilities, businesses can easily use the \_\_\_\_\_ cloud to instantly scale capacity up or down to handle excess capacity.**

## Private

## Explanation

Private clouds, on the other hand, are dedicated cloud environments that are typically used by a single organization. While private clouds offer control and customization options, they do not provide the same level of instant scalability as public clouds. Businesses using a private cloud may face limitations when trying to quickly scale their capacity to handle excess demand beyond the capabilities of their on-premises datacenter.

#### Correct answer

**Public**

#### Explanation

Public cloud services provide businesses with the ability to instantly scale their computing and processing capacity up or down based on demand. This scalability is achieved by leveraging the resources and infrastructure of a third-party cloud service provider, allowing businesses to quickly adapt to changing workload requirements without the need for additional on-premises hardware or infrastructure investments.

#### Overall explanation

##### From the official docs:

When computing and processing demand increases beyond an on-premises datacenter's capabilities, businesses can use the cloud to instantly scale capacity up or down to handle excess capacity. It also allows them to avoid the time and cost of purchasing, installing, and maintaining new servers that they may not always need.

**Reference:** <https://azure.microsoft.com/en-gb/overview/what-is-hybrid-cloud-computing/>

#### Domain

Describe Cloud Concepts

#### Question 75 Skipped

**What is the primary purpose of Microsoft Purview in Azure?**

**To offer a suite of security services for protecting virtual machines.**

**Explanation**

Microsoft Purview does not primarily offer a suite of security services for protecting virtual machines. Its main focus is on data governance and management, rather than virtual machine security.

**To enable real-time analytics and monitoring for Azure resources.**

**Explanation**

While Microsoft Purview may offer some capabilities for analytics and monitoring, its primary purpose is not to enable real-time analytics and monitoring for Azure resources. It is more focused on data governance and management.

**To provide a cloud-based development platform for building and deploying applications.**

**Explanation**

Microsoft Purview is not primarily focused on providing a cloud-based development platform for building and deploying applications. Its main purpose lies in data management and governance across various environments.

**Correct answer**

**To manage and govern data across on-premises, multi-cloud, and SaaS environments.**

**Explanation**

This choice is correct. Microsoft Purview is designed to manage and govern data across on-premises, multi-cloud, and SaaS environments. It provides organizations with a unified view of their data estate and helps ensure compliance and data security.

**Overall explanation**

**Microsoft Purview** is designed to help organizations manage, discover, classify, and govern data across a variety of sources, including on-premises, multi-cloud, and

software-as-a-service (SaaS) environments. It provides a unified data governance solution to ensure data security, compliance, and data-driven insights.

**Reference:** <https://azure.microsoft.com/en-ca/products/purview>

## Domain

Describe Azure management and governance

### Question 76 Skipped

**A customer is using a Platform as a Service (PaaS) model to develop a web application. Which of the following security responsibilities typically falls on the Cloud Service Provider (CSP)?**

Correct answer

**Protecting the underlying infrastructure**

#### Explanation

Protecting the underlying infrastructure, such as servers, networks, and storage, is a security responsibility that typically falls on the Cloud Service Provider (CSP). The CSP is responsible for ensuring the security and compliance of the infrastructure that hosts the web application.

**All of the these**

#### Explanation

"All of these" is not the correct choice because securing the application code and managing user identities and access controls are typically the responsibilities of the customer or developer. Protecting the underlying infrastructure is a security responsibility that falls on the Cloud Service Provider (CSP).

**Securing the application code**

#### Explanation

Securing the application code is typically the responsibility of the customer or the developer who creates the web application. The Cloud Service Provider (CSP) is not

responsible for securing the code itself, but rather for providing a secure infrastructure for the application to run on.

## Managing user identities and access controls

### Explanation

Managing user identities and access controls is a shared responsibility between the customer and the Cloud Service Provider (CSP). While the CSP may provide tools and services for managing user identities and access controls, the customer is ultimately responsible for configuring and monitoring these settings for their specific application.

### Overall explanation

In PaaS, the **CSP** manages the infrastructure, including the underlying hardware, networking, and operating system. However, the customer is responsible for the security of the application code, data, and user management.

**Reference:** <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

### Domain

Describe Cloud Concepts

### Question 77 Skipped

**Which of the following can you use to implement strict governance and ensure that the right people have access to the right resources, and only when they need it?**

### Microsoft Sentinel

### Explanation

Microsoft Sentinel is a security information and event management (SIEM) tool that provides intelligent security analytics and threat detection across the enterprise. While it helps in monitoring and responding to security threats, it is not specifically designed for implementing strict governance and access control policies.

**Correct answer**

## **Microsoft Entra ID**

### **Explanation**

Microsoft Entra ID is a solution that enables organizations to implement strict governance by providing identity and access management capabilities. It ensures that the right people have access to the right resources at the right time, making it a suitable choice for enforcing access control policies.

## **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. While it enhances security for accessing virtual machines, it is not specifically designed for implementing strict governance and access control policies across the organization.

## **Microsoft Defender for Cloud**

### **Explanation**

Microsoft Defender for Cloud is a cloud workload protection platform that helps organizations secure their cloud resources and workloads. While it offers security features, it is not primarily focused on implementing strict governance and access control policies like Microsoft Entra ID.

### **Overall explanation**

#### **From the official docs:**

[Microsoft Entra](#) is an enterprise identity service that provides single sign-on, multifactor authentication, and conditional access to guard against 99.9 percent of cybersecurity attacks.



SSO simplifies access to your apps from anywhere



Conditional access and multifactor authentication help secure data



A single identity control plane grants full visibility and control of your environment



Governance ensures the right people have access to the right resources, and only when they need it

**Microsoft Defender for Cloud** - is a solution for cloud security posture management (CSPM) and cloud workload protection (CWP) that finds weak spots across cloud configurations, helps strengthen the overall security posture of environments, and can protect workloads across multicloud and hybrid environments from evolving threats.

**Azure Bastion** - is a fully managed service that provides more secure and seamless Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH) access to virtual machines (VMs) without any exposure through public IP addresses.

**Microsoft Sentinel** - is a birds-eye view across the enterprise. It puts the cloud and large-scale intelligence from decades of Microsoft security experience to work. Make your threat detection and response smarter and faster with artificial intelligence (AI).

Reference: <https://azure.microsoft.com/en-ca/services/active-directory/#features>

## Domain

Describe Azure architecture and services

### Question 78 Skipped

#### Which of the following statements is accurate?

If you want to migrate a website that is hosted On-Prem presently to Azure, one of the clear benefits is the Pay-As-You-Go Pricing that comes with Azure.

**This is not true, we first need to pay to transfer all the website data to Azure**

#### Explanation

This explanation is incorrect as the statement in Choice A is accurate. While there may be costs associated with transferring website data to Azure, the Pay-As-You-Go Pricing model refers to the pricing structure once the website is hosted on Azure, not the initial data transfer.

#### **Correct answer**

**The given statement is correct.**

#### **Explanation**

The statement is accurate because one of the benefits of migrating a website from an On-Prem environment to Azure is the Pay-As-You-Go Pricing model, which allows you to pay only for the resources you use, providing cost-efficiency and flexibility.

**This is not true. You need a VPN to complete the migration which will cost a lot.**

#### **Explanation**

This explanation is incorrect as the statement in Choice A is accurate. While setting up a VPN may be necessary for secure communication during migration, it is not a requirement for the Pay-As-You-Go Pricing model that Azure offers.

**This is not true, a website hosted on Azure will be costlier as its charged by the second.**

#### **Explanation**

This explanation is incorrect as the statement in Choice A is accurate. Azure's Pay-As-You-Go Pricing model is designed to provide cost-effective pricing based on actual usage, which can be more cost-efficient compared to traditional hosting models.

#### **Overall explanation**

When planning to migrate a website to Azure, the Pay As you Go pricing model is a big advantage. You can even use Azure Websites to accomplish this.

Azure Websites is offered in four tiers: **Free, Shared (Preview), Basic and Standard**.

- **Websites Shared (Preview):** The price for the Shared tier during preview is **\$0.013** per hour per website instance (~\$10/month). This price reflects a 33% preview discount.

- **Websites Basic and Standard:** The Basic and Standard tiers offer multiple instance sizes as well as scaling to meet changing capacity needs starting from \$56 for a Basic (Single Small instance) and \$75 for a Standard ( Single small instance)

For more details on features per price tier , click [here](#).

### Incorrect Answers:

- You do not need a VPN for Azure web sites.
- You do not pay to transfer data into Azure web sites.
- You are not charged by the second.

### Domain

Describe Azure management and governance

### Question 79 Skipped

#### When should you scale 'out' your deployment?

##### Correct answer

**When you need additional Virtual Machines / compute to speed up your application**

##### Explanation

Scaling out by adding additional Virtual Machines or compute resources is the correct choice when you need to increase the capacity of your deployment to handle higher traffic or workload. This approach helps speed up your application by distributing the workload across multiple instances.

**When you need to reduce your cost of operation**

##### Explanation

Scaling out may not necessarily reduce the cost of operation, as adding more Virtual Machines or compute resources can increase operational costs. The primary goal of

scaling out is to improve performance and handle increased workload efficiently.

### **When you want to reduce the unused capacity of your system**

#### **Explanation**

Scaling out is not typically done to reduce the unused capacity of your system. It is more focused on increasing capacity to handle higher demand and improve performance. If you want to reduce unused capacity, you may consider scaling in or optimizing resource allocation.

### **When you need a stronger CPU to make your application run faster**

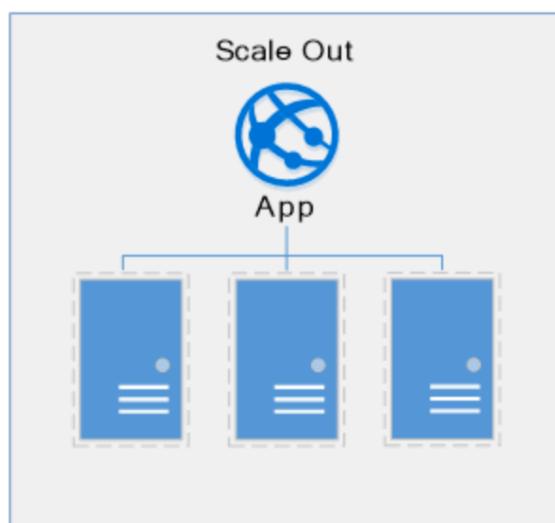
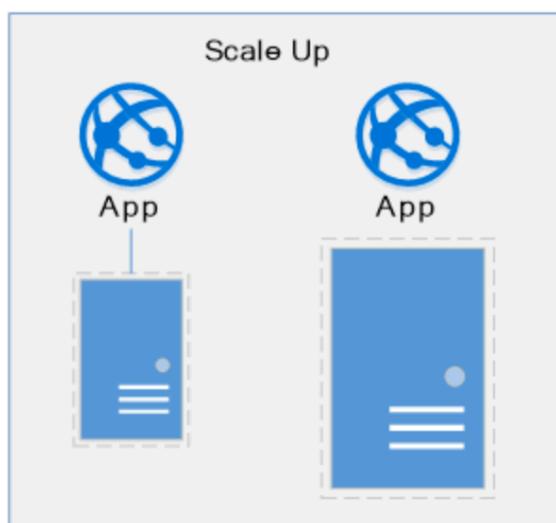
#### **Explanation**

Scaling out your deployment involves adding more instances of the application to handle increased workload, rather than increasing the power of a single instance. This approach helps distribute the load across multiple instances, improving performance and scalability.

## **Overall explanation**

### **Scale Out**

A scale out operation is the equivalent of creating multiple copies of your web site and adding a load balancer to distribute the demand between them. When you scale out a web site in Azure, there is no need to configure load balancing separately since this is already provided by the platform



**References :** <https://www.azurebarry.com/how-to-autoscale-azure-app-services-cloud-services/>

## Domain

Describe Cloud Concepts

### Question 80 Skipped

Yes or No:

**Data in an Azure storage account is replicated 3 times in the primary region.**

**Correct answer**

**Yes**

#### Explanation

Yes, data in an Azure storage account is replicated 3 times in the primary region by default. This ensures high durability and availability of the data stored in Azure storage accounts.

**No**

#### Overall explanation

Azure Storage always stores **multiple** copies of your data so that it is protected from planned and unplanned events, including transient hardware failures, network or power outages, and massive natural disasters. Redundancy ensures that your storage account meets the [Service-Level Agreement \(SLA\) for Azure Storage](#) even in the face of failures.

**See below:**

# Redundancy in the primary region

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

- **Locally redundant storage (LRS)** copies your data synchronously three times within a single physical location in the primary region. LRS is the least expensive replication option, but is not recommended for applications requiring high availability.
- **Zone-redundant storage (ZRS)** copies your data synchronously across three Azure availability zones in the primary region. For applications requiring high availability, Microsoft recommends using ZRS in the primary region, and also replicating to a secondary region.

## Locally-redundant storage

Locally redundant storage (LRS) replicates your data three times within a single physical location in the primary region. LRS provides at least 99.99999999% (11 nines) durability of objects over a given year.

**Reference :** <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy>

## Domain

Describe Azure architecture and services

[Back to result overview](#)

[Scroll back to top](#)