# Microsoft Azure AZ-900 Exam Questions

**Total Questions: 460+**
**Demo Questions: 35**
**Version: Updated for 2025**

**Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner**

**For Access to the full set of Updated Questions – Visit:**
**AZ-900 Exam Dumps by Cert Empire**

# Question: 1

Which task can you perform by using Azure Advisor?

A. Integrate Active Directory and Azure Active Directory (Azure AD).

B. Estimate the costs of an Azure solution.

C. Confirm that Azure subscription security follows best practices.

D. Evaluate which on-premises resources can be migrated to Azure.

## Answer:

C

## Explanation:

Azure Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions to improve the reliability, security, performance, operational excellence, and cost-effectiveness of your Azure resources. The security recommendations are integrated with Microsoft Defender for Cloud to provide a unified view of security best practices and help you confirm that your subscription's security posture is sound.

## Why Incorrect Options are Wrong:



A. Integrating on-premises Active Directory with Azure AD is a task performed by the Azure AD Connect tool, not Azure Advisor.
B. Estimating the costs of a new Azure solution is the primary function of the Azure Pricing Calculator or the Total Cost of Ownership (TCO) Calculator.
D. Evaluating on-premises resources for migration to Azure is performed using the Azure Migrate service, which provides discovery and assessment tools.

## References:

1. Microsoft Learn. (2023). "Introduction to Azure Advisor." Microsoft Docs. In the "What is Advisor?" section, it states, "Advisor provides recommendations for Reliability, Security, Performance, Operational Excellence, and Cost." This confirms that security is a core pillar of Advisor's function.
2. Microsoft Learn. (2023). "Security recommendations in Azure Advisor." Microsoft Docs. This document specifies, "Advisor uses Microsoft Defender for Cloud to find security vulnerabilities and misconfigurations. Then, Advisor suggests solutions that will help you improve the security posture of your organization." This directly supports option C.
3. Microsoft Learn. (2023). "What is the Azure Pricing Calculator?" Microsoft Docs. This page describes the calculator as a tool to "estimate your expected monthly bill" for new deployments, which is the task described in option B.

4. Microsoft Learn. (2023). "What is Azure AD Connect?" Microsoft Docs. The "Overview" section explains that Azure AD Connect is the tool designed to meet hybrid identity goals, including synchronizing on-premises directories with Azure AD, as mentioned in option A.
5. Microsoft Learn. (2023). "About Azure Migrate." Microsoft Docs. The "Overview" section describes Azure Migrate as the central hub to "discover, assess, and migrate on-premises servers, apps, and data to the Azure cloud," which is the task in option D.

## Question: 2

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.


**Answer:**

YES

YES

YES



**Explanation:**

The General Data Protection Regulation (GDPR) is a comprehensive legal framework established by the European Union. Its primary purpose is to standardize data protection laws across all member countries, providing individuals with greater control over their personal data and defining the rules for how organizations must handle that data.

The GDPR has a broad territorial scope. According to Article 3(2), the regulation applies to organizations not established within the EU if their activities involve offering goods or services to data subjects in the EU or monitoring their behavior as far as their behavior takes place within the EU.

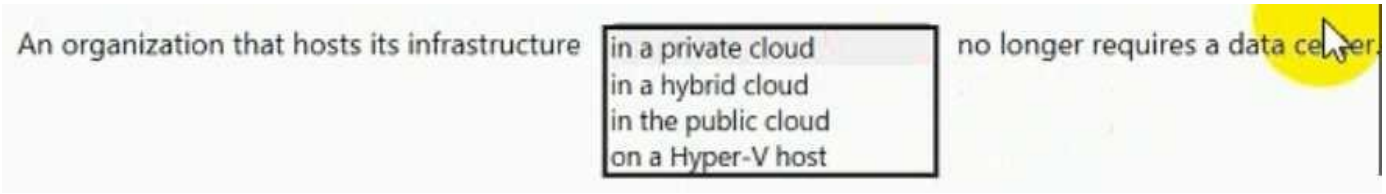
Microsoft Azure provides a platform with a wide array of security and privacy services, features, and contractual commitments that enable customers to build and manage GDPR-compliant solutions. While using Azure does not automatically confer compliance (as it is a shared responsibility), the platform provides the necessary technical controls to help organizations meet their GDPR obligations.

**References:**

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L 119/1.
Article 1, Subject-matter and objectives: "This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."
Article 3, Territorial scope: "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services... to such data subjects in the Union..."
Microsoft. (2024). Microsoft Azure Compliance Offerings. Microsoft Learn.
GDPR Section: "Azure provides a set of tools and features to help organizations meet the requirements of the GDPR... Microsoft offers data processing agreements and other contractual safeguards that support customers' GDPR compliance efforts."
Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer. https://doi.org/10.1007/978-3-319-57959-7
Chapter 3, Scope of the GDPR, Section 3.2, Territorial Scope: Discusses the extraterritorial application of the regulation to companies offering goods or services to individuals in the EU, aligning with Article 3(2).

## Question: 3

HOTSPOT To complete the sentence, select the appropriate option in the answer area.




**Answer:**

in the public cloud

**Explanation:**

An organization that moves its entire infrastructure to a public cloud offloads the responsibility of owning, managing, and maintaining the physical hardware and the facility in which it is housed. In the public cloud model, a third-party provider (e.g., AWS, Microsoft Azure, Google Cloud) owns and operates all the infrastructure components, including the data centers. The services are then delivered to the organization over the internet. This model allows an organization to completely eliminate the need for its own on-premises data center. In contrast, private clouds are often hosted on-premises, hybrid clouds involve an on-premises component, and a Hyper-V host is a physical server that would reside within a data center.



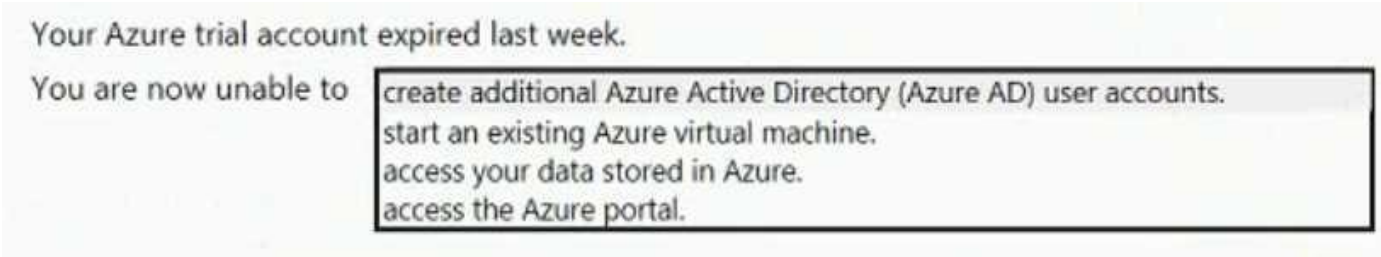
**References:**

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing (NIST Special Publication 800-145). National Institute of Standards and Technology.
Section 2, Definitions: Defines Public Cloud as: "The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider." This explicitly states the infrastructure resides at the provider's location, not the consumer's.
DOI: https://doi.org/10.6028/NIST.SP.800-145
Microsoft Azure Documentation. What is a public cloud?
Overview Section: "Public clouds are the most common type of cloud computing deployment. The cloud resources (like servers and storage) are owned and operated by a third-party cloud service provider and delivered over the Internet... With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud provider." This confirms that the provider manages the physical infrastructure, removing the need for the customer to do so.
Armbrust, M., et al. (2010). A View of Cloud Computing. Communications of the ACM, 53(4), 50-58.
Section 2.1, Defining Cloud Computing: The paper describes public cloud computing (termed

"Utility Computing") as a model where users purchase computing resources from external providers, implicitly removing the need to host those resources internally.
DOI: https://doi.org/10.1145/1721654.1721672

## Question: 4

HOTSPOT To complete the sentence, select the appropriate option in the answer area.




**Answer:**

start an existing Azure virtual machine.

**Explanation:**

When an Azure free trial account expires, the associated subscription becomes disabled. A disabled subscription prevents the use of any services that would incur costs. Virtual machines (VMs) are deallocated, and you are unable to start or manage them. While the subscription is disabled, you can still access the Azure portal to manage the subscription (e.g., upgrade to a pay-as-you-go model). For a grace period, typically 30 days, your data remains accessible before being permanently deleted. Basic Azure Active Directory (Azure AD) services, which are part of the perpetual free tier, also remain available for managing users. Therefore, the most immediate and accurate consequence is the inability to run compute resources like a VM.



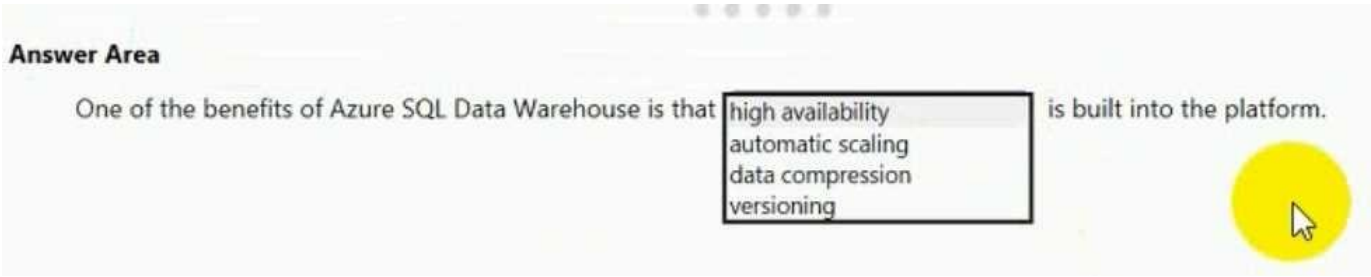
**References:**

Microsoft Azure Documentation, "Azure free account FAQ".
Section: "What happens after I use my $200 free credit or I'm at the end of 30 days?"
Content: This section explains that after the trial period, the subscription is disabled. To continue using Azure services, you must upgrade your subscription. This implicitly confirms that active services, which incur costs, will be stopped.
Microsoft Azure Documentation, "Reactivate a disabled Azure subscription".
Section: "Your subscription is disabled"
Content: This document states that for a disabled subscription (which includes an expired free trial), "Virtual machines are deallocated. Other Azure resources are not accessible... Your data is frozen and available to you if you decide to reactivate your subscription." This directly confirms that VMs are stopped and cannot be started.
Microsoft Azure Documentation, "Azure Active Directory pricing".
Section: "Free" edition.
Content: This page shows that Azure AD comes with a "Free" edition that is included with a subscription to a commercial online service like Azure. This free tier is not part of the trial's paid services and remains functional even after the trial subscription for other resources expires,

allowing for continued user account management.

## Question: 5

HOTSPOT To complete the sentence, select the appropriate option in the answer area.




**Answer:**

high availability

**Explanation:**

Azure Advisor is a personalized cloud consultant that helps optimize Azure deployments by providing best practice recommendations. It analyzes resource configuration and usage telemetry across five distinct categories: Reliability (formerly High Availability), Security, Performance, Cost, and Operational Excellence. The "high availability" (now Reliability) category focuses on recommendations to ensure and improve the continuity of business-critical applications, such as suggesting zone-redundant configurations or enabling backup for virtual machines. All three options presented are valid Advisor categories, but "high availability" correctly completes the sentence as one of its core functions.

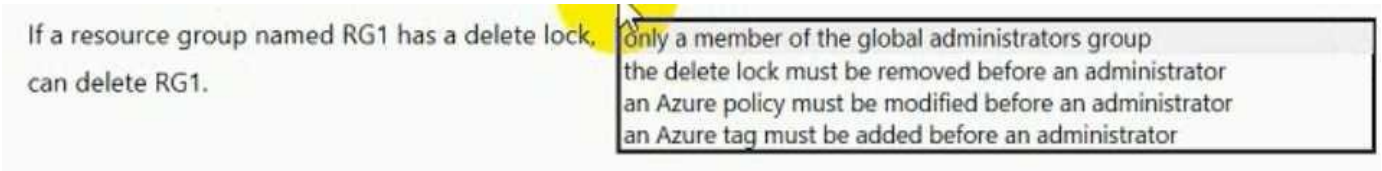


**References:**

1. Microsoft Learn, "Introduction to Azure Advisor." This official documentation outlines the five categories of recommendations. It explicitly states, "Reliability (formerly called High Availability): To ensure and improve the continuity of your business-critical applications."
Source: https://learn.microsoft.com/en-us/azure/advisor/advisor-overview, Section: "Recommendations in Advisor".
2. Microsoft Learn, AZ-900 Learning Path, "Describe features and tools in Azure for governance and compliance." This courseware for the AZ-900 exam details the function of Azure Advisor.
Source: https://learn.microsoft.com/en-us/training/modules/describe-features-tools-azure-for-governance-compliance/4-describe-azure-advisor, Section: "Advisor recommendations". The text confirms, "The Reliability category was formerly known as High Availability."

## Question: 6

HOTSPOT To complete the sentence, select the appropriate option in the answer area.




**Answer:**

the delete lock must be removed before an administrator

**Explanation:**

An Azure delete lock (CanNotDelete) on a resource group prevents all users from deleting it, regardless of their role-based access control (RBAC) permissions. This includes users with Owner or Global Administrator roles. The lock provides a layer of protection against accidental deletion that supersedes user permissions. To delete the resource group, a user with the appropriate permissions (specifically, the Microsoft.Authorization/locks/* action, which is part of the Owner and User Access Administrator built-in roles) must first explicitly remove the delete lock. Only after the lock is removed can the resource group be deleted.

**References:**



Microsoft Learn (Official Azure Documentation):
Document: Lock resources to prevent unexpected changes
Section: "How locks are applied" and "Who can create or delete locks"
Quote/Concept: "Locks apply to all users and roles..... CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource. To delete a locked resource, you must first remove the lock..... To create or delete management locks, you must have access to Microsoft.Authorization/locks/* actions. Of the built-in roles, only Owner and User Access Administrator are granted those actions." This confirms that the lock must be removed first by an authorized user.

# Question: 7

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| You can nest resource groups. | ○ | ○ |
| An Azure virtual machine can be in multiple resource groups. | ○ | ○ |

## Answer:

No

No

## Explanation:

Azure resource groups are flat containers used to manage the lifecycle of related resources for an Azure solution. They cannot be nested within one another.

Furthermore, every Azure resource, including a virtual machine, must exist in one and only one resource group at any given time. While a resource can be moved from one resource group to another, it cannot simultaneously be a member of multiple groups. This single-parent structure is a fundamental principle of Azure Resource Manager (ARM) for consistent management, billing, and access control.



## References:

Microsoft Azure Documentation. (n.d.). Azure Resource Manager overview. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview
In the "Resource groups" section, the documentation states, "Every resource must exist in one and only one resource group." and "Resource groups can't be nested." This directly refutes both statements in the question.
Microsoft Azure Documentation. (n.d.). What are Azure resource groups?. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal#what-are-resource-groups
Under the "Resource group considerations" heading, it notes: "Resources can only exist in one resource group." This confirms the second statement is false.

# Question: 8

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| Azure resources can only access other resources in the same resource group. | ○ | ○ |
| If you delete a resource group, all the resources in the resource group will be deleted. | ○ | ○ |

## Answer:

Statement 1: No

Statement 2: Yes

## Explanation:

Statement 1: Azure resources can only access other resources in the same resource group.

This statement is No. A resource group is a logical container for management, billing, and lifecycle purposes, not a security or access boundary. Azure resources can interact with resources in different resource groups, different subscriptions, or even different Azure Active Directory tenants, provided that appropriate networking, identity, and access control (e.g., Role-Based Access Control - RBAC) configurations are in place. For example, a virtual machine in one resource group can connect to a SQL database in another.



Statement 2: If you delete a resource group, all the resources in the resource group will be deleted.

This statement is Yes. A core feature of Azure Resource Manager is lifecycle management. When you delete a resource group, you are instructing Azure to delete all the resources contained within it. This action is recursive and, by default, will remove all associated components. While certain conditions like resource locks can prevent the deletion of a resource group until the lock is removed, the fundamental behavior of deleting a group is to delete its contents.

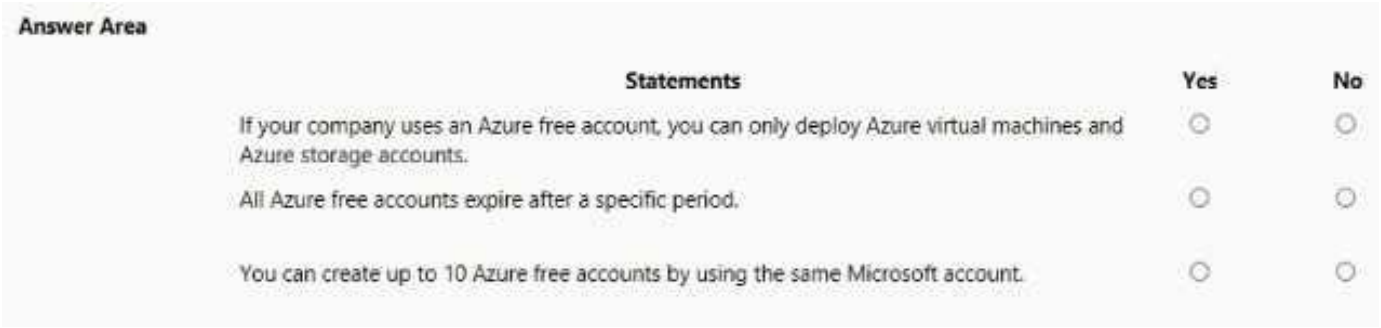
## References:

Microsoft Corporation. (2024). What is Azure Resource Manager? Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview. Supporting evidence for Statement 1: In the "Terminology" section, it is stated, "The resource group stores metadata about the resources... Placing resources in the same resource group is for

logical grouping. It doesn't affect how the resources can interact with each other."
Microsoft Corporation. (2024). Manage Azure resource groups by using the Azure portal. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal#delete-resource-group.
Supporting evidence for Statement 2: The section "Delete resource group" explicitly states, "When you delete a resource group, you delete all of the resources in it."

# Question: 9

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE Each correct selection is worth one point.




**Answer:**

Statement 1: No

Statement 2: Yes

Statement 3: No

**Explanation:**



If your company uses an Azure free account, you can only deploy Azure virtual machines and Azure storage accounts. (No) The Azure free account provides access to a wide variety of services, not just virtual machines and storage. It includes a $200 credit to use on most Azure services for the first 30 days, 12 months of popular free services, and access to over 55 services that are always free up to specified limits.

All Azure free accounts expire after a specific period. (Yes) The promotional benefits of the Azure free account are time-limited. The $200 credit expires after 30 days, and the access to popular services for free expires after 12 months. After this period, the user must upgrade to a pay-as-you-go subscription to continue using services that are not in the "always free" category. Therefore, the "free account" as a promotional offer expires.

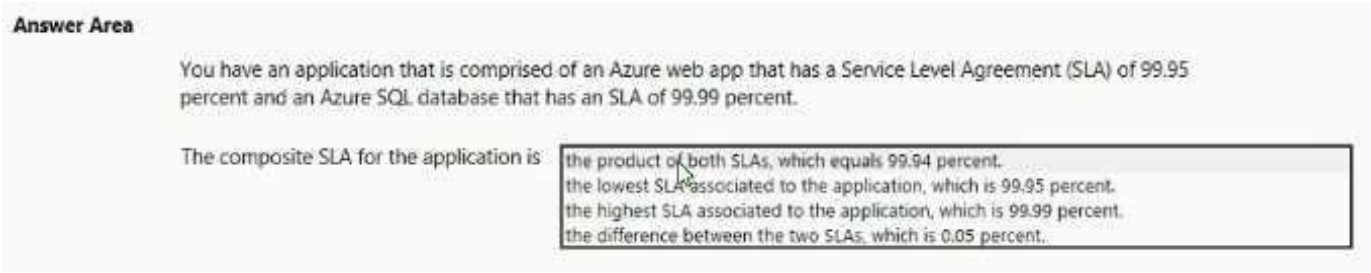
You can create up to 10 Azure free accounts by using the same Microsoft account. (No) The Azure free account offer is strictly limited to one per new customer. This is enforced by verifying a unique credit card, phone number, and email address (Microsoft account). Attempting to create multiple free accounts with the same information is not permitted by the terms of service.

**References:**

Microsoft Azure Official Documentation. (n.d.). Azure free account FAQ. Microsoft.
Relevant Sections: "What is included in the Azure free account?", "What happens when the 12 months are over?", and "Who is eligible for the Azure free account?".
Content: The documentation explicitly lists the three components of the free offer (credit, 12-month services, always-free services). It confirms the expiration of the credit (30 days) and the popular services (12 months). It also states, "The offer is limited to one Azure free account per new customer and cannot be combined with any other offers".

# Question: 10

HOTSPOT To complete the sentence, select the appropriate option in the answer area.




## Answer:

The product of both SLAs, which equals 99.94 percent.

## Explanation:

The composite Service Level Agreement (SLA) for an application composed of multiple dependent services is calculated by multiplying the SLAs of the individual components. For the system to be available, both the Azure web app and the Azure SQL database must be available. The probability of both independent events occurring is the product of their individual probabilities.

The calculation is as follows: SLAcomposite=SLAWebApptimesSLASQLDatabase

SLAcomposite=99.95 SLAcomposite=0.9995times0.9999 SLAcomposite=0.99940005 SLAcompositeapprox99.94

This result demonstrates that the composite SLA is always lower than the lowest individual SLA of its constituent components.

## References:

Microsoft Azure Documentation: The official Azure Architecture Center documentation explicitly defines how to calculate composite SLAs for applications with multiple services.
Source: Microsoft Learn, Azure Architecture Center, "Composite SLAs".
Reference: In the section "Composite SLAs," the document states, "The composite SLA is calculated by multiplying the individual SLAs... For example, if you have a web app with a 99.95 percent SLA and a database with a 99.99 percent SLA, the composite SLA is: 99.95% 99.99% = 99.94%".
Academic Publication on System Reliability: The principle of calculating the total reliability of a system with components in a series (where all must function for the system to function) is a foundational concept in reliability engineering.
Source: Rausand, M., & Hyland, A. (2004). System Reliability Theory: Models, Statistical Methods, and Applications (2nd ed.). Wiley.

Reference: Chapter 3, Section 3.2, "Series Structures". This section establishes that for a series system with n independent components, the system reliability, Rs(t), is the product of the individual component reliabilities: Rs(t)=
prodi=1
n
Ri(t). The SLA is a measure of availability, which is a form of reliability.
DOI: https://doi.org/10.1002/0471667254

# Question: 11

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.


## Answer:

Statement 1: No

Statement 2: No

Statement 3: No

## Explanation:



Availability zones can be implemented in all Azure regions.

• No. Azure Availability Zones are physically separate locations within an Azure region. While the number of regions supporting them is continuously growing, they are not available in all Azure regions. Service availability is dependent on the specific region.

Only virtual machines that run Windows Server can be created in availability zones.

• No. Azure Availability Zones support a wide range of services and operating systems. This includes virtual machines running various distributions of Linux in addition to Windows Server.

Availability zones are used to replicate data and applications to multiple regions.

• No. This statement describes geo-redundancy or cross-region replication. Availability Zones are used for high availability and redundancy within a single Azure region to protect against datacenter-level failures. Replicating across regions is a different disaster recovery strategy.

**References:**

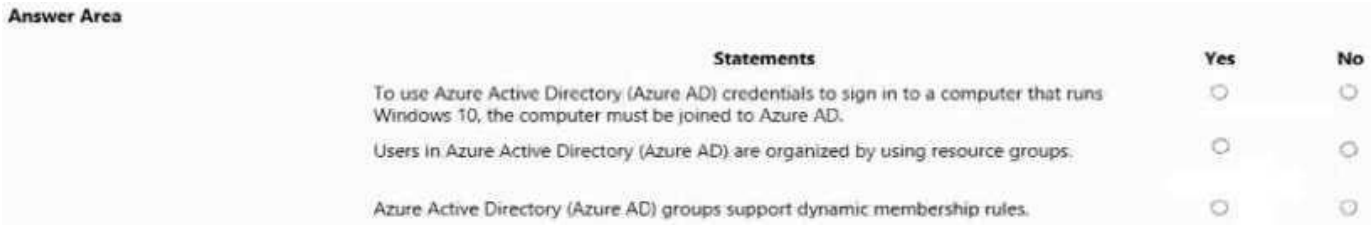
Microsoft Azure Documentation, "Azure regions and availability zones." This document explicitly lists which regions support Availability Zones, demonstrating they are not universally available. It states, "Regions that support Availability Zones are listed below." which is followed by a specific subset of all Azure regions.

Microsoft Azure Documentation, "What are availability zones?" This page defines Availability Zones as "...unique physical locations within an Azure region," which directly contradicts the claim that they are used for replication to multiple regions. The document contrasts this with regional pairs, which are used for cross-region replication.

Microsoft Azure Documentation, "Create a Linux virtual machine in the Azure portal." This tutorial, along with its Windows counterpart, provides step-by-step instructions for deploying VMs. In the "Basics" tab of the creation process, the "Availability options" dropdown allows selecting an "Availability zone" for both Linux and Windows virtual machines, confirming that support is not exclusive to Windows Server.

# Question: 12

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise select No. NOTE: Each correct selection is worth one point.




**Answer:**

Yes

No

Yes

**Explanation:**

Statement 1 is TRUE. For a user to sign in to a Windows 10/11 device using their Azure AD account (e.g., user@domain.com), the device must have an identity in Azure AD. This is achieved through Azure AD Join or Hybrid Azure AD Join. This process links the device to the Azure AD tenant, enabling management and single sign-on with Azure AD credentials.



Statement 2 is FALSE. Resource groups are management containers in Azure Resource Manager (ARM) used to group Azure resources like virtual machines, storage, and databases. They are not used to organize identity objects like users or groups within Azure AD. Users in Azure AD are organized within the directory tenant itself and can be managed using security groups, Microsoft 365 groups, or administrative units.

Statement 3 is TRUE. Azure AD groups support both assigned (manual) and dynamic membership. With a dynamic group, administrators can define rules based on user or device attributes (such as department, location, or device OS). Azure AD automatically adds or removes members from the group if their attributes change to match or no longer match the rule, which simplifies group management.

**References:**

Azure AD Joined Devices:
Microsoft Learn. (2024). Azure AD joined devices. In Azure Active Directory Documentation. Retrieved from

https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join. See the "Overview" section which states, "Azure AD join allows users to sign in to their devices using their work or school Azure AD accounts."

Azure Resource Groups:

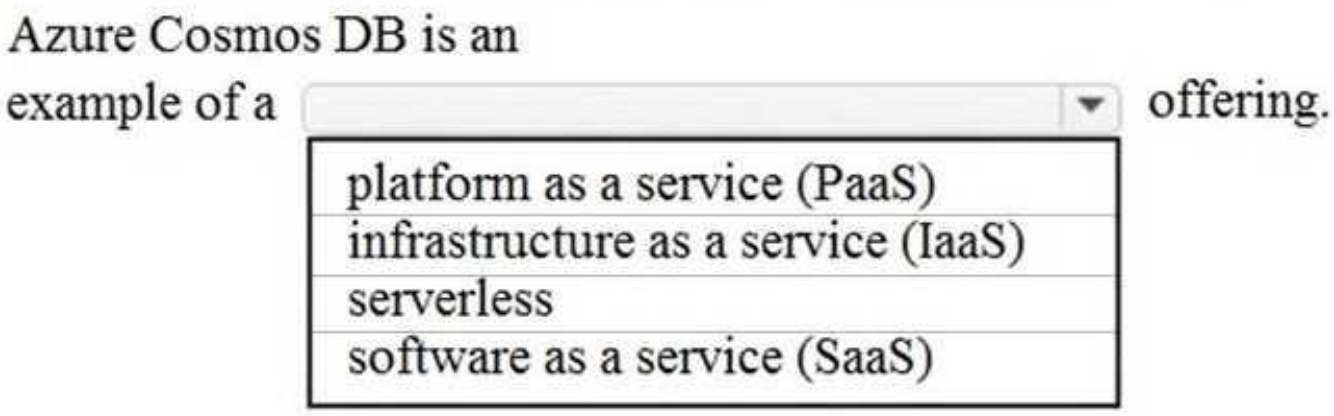
Microsoft Learn. (2024). What is Azure Resource Manager?. In Azure Documentation. Retrieved from https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview. See the "Terminology" section, which defines a resource group as "A container that holds related resources for an Azure solution." It does not mention Azure AD users as a type of resource for this container.

Dynamic Membership Rules:

Microsoft Learn. (2024). Dynamic membership rules for groups in Azure Active Directory. In Azure Active Directory Documentation. Retrieved from https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership. See the "Overview" section, which states, "You can create attribute-based rules to enable dynamic membership for a group in Azure Active Directory (Azure AD)."

## Question: 13

HOTSPOT To complete the sentence, select the appropriate option in the answer area.




**Answer:**

platform as a service (PaaS)

**Explanation:**

Azure Cosmos DB is a fully managed, globally distributed, multi-model database service. In the cloud computing service model, this falls under Platform as a Service (PaaS). The provider (Microsoft) manages the underlying infrastructure, including servers, networking, storage, operating systems, and the database software itself. The consumer interacts with the service to store and manage data for their applications without needing to manage the platform's foundation. While Cosmos DB offers a serverless consumption model, its fundamental classification as a service type is PaaS, as it provides a complete platform for database operations.



**References:**

Microsoft Azure Documentation, "What is Platform as a service (PaaS)?", Microsoft Corp. This document categorizes services that allow for the development, testing, and deployment of software applications as PaaS. It explicitly includes "Databases" and "Business analytics" as common PaaS scenarios, which directly applies to Azure Cosmos DB as a managed database service.

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing (Special Publication 800-145). National Institute of Standards and Technology, U.S. Department of Commerce. On page 2, PaaS is defined as the capability for the consumer to "deploy onto the cloud infrastructure consumer-created or acquired applications... The consumer does not manage or control the underlying cloud infrastructure... but has control over the deployed applications." This definition perfectly describes the user's interaction with Azure Cosmos DB. Available at: https://doi.org/10.6028/NIST.SP.800-145

Armbrust, M., et al. (2010). "A View of Cloud Computing." Communications of the ACM, 53(4),

50-58. In Section 2.1, "Classes of Utility Computing," the authors describe Platform-as-a-Service offerings as providing higher-level abstractions, including database services, which contrasts with IaaS's lower-level resource provisioning. Azure Cosmos DB fits this description of a higher-level, abstracted database platform. https://doi.org/10.1145/1721654.1721672

## Question: 14

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

| Statements | Yes | No |
|---|---|---|
| Building a data center infrastructure is an example of operational expenditure (OpEx) costs. | ◯ | ◯ |
| Monthly salaries for technical personnel are an example of operational expenditure (OpEx) costs. | ◯ | ◯ |
| Leasing software is an example of operational expenditure (OpEx) costs. | ◯ | ◯ |

**Answer:**

No



Yes

Yes

**Explanation:**

Capital Expenditure (CapEx) is the upfront spending on physical infrastructure which will be used over an extended period. Operational Expenditure (OpEx) is the ongoing, recurring cost for services or products as they are consumed.

Building a data center is a significant, one-time investment in a physical asset, which is a classic example of CapEx.

Conversely, monthly salaries and software leases (or subscriptions) are recurring, day-to-day business costs. They are consumed immediately and paid on a regular basis, making them clear examples of OpEx.

**References:**

Microsoft Learn. (n.d.). Describe capital expenditure (CapEx) and operational expenditure (OpEx). Microsoft Azure Fundamentals: Describe cloud concepts. Retrieved from Microsoft's official documentation.
This document explicitly states: "CapEx is an upfront spending of money on physical infrastructure... OpEx is spending on products and services as needed... Examples of OpEx include... employee salaries."
Brealy, R. A., Myers, S. C., & Allen, F. (2020). Principles of Corporate Finance (13th ed.). McGraw-Hill Education.
Chapter 6, Section 6.1: This chapter defines investment decisions (CapEx) as acquiring long-lived assets, contrasting them with operational costs (OpEx) like salaries and recurring service payments which are expensed in the period they are incurred.
Patel, P., Ranabahu, A. H., & Sheth, A. P. (2009). Service Level Agreement in Cloud Computing. In Proceedings of the 2009 IEEE International Conference on Web Services (pp. 1-8).
Section 2.B: This paper discusses the economic model of cloud computing, highlighting the shift from a CapEx model (buying and building your own hardware/data centers) to an OpEx model (paying a monthly bill for resources, akin to leasing or subscribing).
https://doi.org/10.1109/ICWS.2009.110

## Question: 15

This question requires that you evaluate the underlined text to determine if it is correct. An Availability Zone in Azure has physically separate locations across two continents. Instructions: Review the underlined text. If it makes the statement correct, select "No change is needed." If the statement is incorrect, select the answer choice that makes the statement correct.

A. No change is needed.

B. within a single Azure region

C. within multiple Azure regions

D. within a single Azure datacenter

**Answer:**

B

**Explanation:**

The original statement is incorrect. Azure Availability Zones are physically separate locations within a single Azure region. Each Availability Zone is composed of one or more datacenters with independent power, cooling, and networking. This design provides high availability and protects applications and data from datacenter-level failures. A single Azure region is a set of datacenters deployed within a latency-defined perimeter and does not span continents; therefore, its constituent Availability Zones are also confined to that single geographic region.



**Why Incorrect Options are Wrong:**

A. No change is needed.
The original statement is factually incorrect. Availability Zones are components of a single region, which is located in one geographic area, not across continents.
C. within multiple Azure regions
This describes a multi-region architecture or region pairs, which is a different concept for disaster recovery. An Availability Zone exists only within one region.
D. within a single Azure datacenter
This is incorrect because an Availability Zone is made up of one or more datacenters. The purpose is to have separation between datacenters, not within one.

**References:**

1. Microsoft Learn. (2024). Regions and Availability Zones in Azure. "Core concepts - Azure". Retrieved from https://learn.microsoft.com/en-us/azure/availability-zones/az-overview#availability-zones.
Section: Availability Zones: "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." This directly supports the correct answer (B) and refutes options A and D.

2. Microsoft Learn. (2024). Describe core architectural components of Azure. "Azure Fundamentals: Describe core Azure concepts". Retrieved from https://learn.microsoft.com/en-us/training/modules/describe-core-architectural-components-of-azure/3-describe-regions-availability-zones.

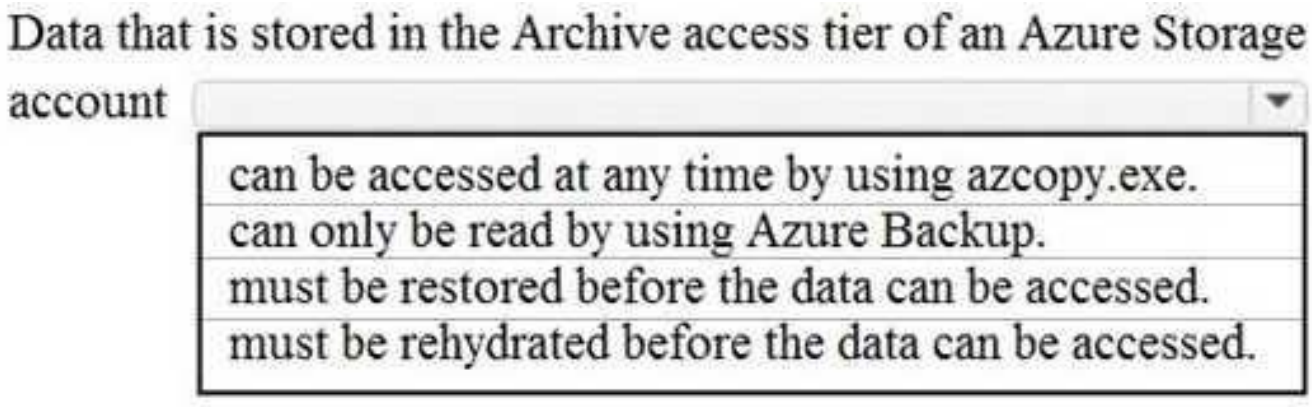
Section: What are Availability Zones?: "Availability Zones are physically separate datacenters within an Azure region." This statement explicitly confirms that Availability Zones are contained within a single region.

3. Microsoft Azure Documentation. (2023). Azure resiliency. "White papers". Retrieved from https://azure.microsoft.com/en-us/resources/azure-resiliency/.

Page 5, Section: Azure Regions: "An Availability Zone is a physically separate location within an Azure region...". This white paper reinforces the hierarchical relationship where zones are subsets of a region, invalidating the idea they could span regions or continents (options A and C).

## Question: 16

HOTSPOT To complete the sentence, select the appropriate option in the answer area.




**Answer:**

must be rehydrated before the data can be accessed.

**Explanation:**

Data in the Azure Archive access tier is stored offline, providing the lowest storage cost but with the highest data retrieval costs and latency. To access a blob in the Archive tier, it must first be moved to an online tier (either Hot or Cool). This process is known as rehydration. Rehydration is an asynchronous operation that can take several hours to complete, depending on the priority specified (Standard or High). Once the blob is rehydrated to an online tier, it can be read or modified.



**References:**

Microsoft Azure Documentation, "Azure Blob storage access tiers - Hot, Cool, and Archive."
Reference: Under the "Archive tier" section, it states, "To read data in the Archive tier, you must first change the tier of the blob to Hot or Cool. This process is known as rehydration and can take hours to complete."
Microsoft Azure Documentation, "Blob rehydration from the Archive tier."
Reference: The introduction paragraph explicitly states, "While a blob is in the Archive access tier, it's considered offline and can't be read or modified. To read or modify data in an archived blob, you must first rehydrate it to an online tier, either the hot or cool tier."

## Question: 17

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

| Statements | Yes | No |
|---|---|---|
| All the Azure resources deployed to a resource group must use the same Azure region. | ○ | ○ |
| If you assign a tag to a resource group, all the Azure resources in that resource group are assigned to the same tag. | ○ | ○ |
| If you assign permissions for a user to manage a resource group, the user can manage all the Azure resources in that resource group. | ○ | ○ |

**Answer:**

No

No

Yes

**Explanation:**

A resource group is a logical container, and its own location only determines where the metadata for that group is stored. The resources within the group can be in any Azure region, they do not need to match the resource group's location. This allows for grouping logically related resources that may be distributed geographically for performance or redundancy.

Tags applied at the resource group level are not automatically inherited by the resources within that group. Each resource must be tagged explicitly, either manually or through an Azure Policy, to

have the same tag as its parent resource group.

Azure Role-Based Access Control (RBAC) permissions are inherited down the hierarchy. When you grant a user permissions (e.g., the Contributor role) at the scope of a resource group, those permissions apply to all the resources contained within that group.

**References:**

Microsoft Azure Documentation (Resource Group Location):
Microsoft Learn. (n.d.). Azure Resource Manager overview. In Azure documentation. Retrieved from https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview
Reference Section: Under the "Resource groups" section, the documentation states, "The resource group stores metadata about the resources... The location of the resource group can be different than the location of resources."
Microsoft Azure Documentation (Tag Inheritance):
Microsoft Learn. (n.d.). Use tags to organize your Azure resources and management hierarchy. In Azure documentation. Retrieved from https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources
Reference Section: Under the "Inheritance" section, it explicitly states, "Tags applied to the resource group are not inherited by the resources in that resource group."
Microsoft Azure Documentation (RBAC Inheritance):
Microsoft Learn. (n.d.). What is Azure role-based access control (RBAC)?. In Azure documentation. Retrieved from https://learn.microsoft.com/en-us/azure/role-based-access-control/overview
Reference Section: Under the "Scope" section, the documentation explains, "When you assign a role at a parent scope, those permissions are inherited by the child scopes... If you assign the Contributor role to a user at the resource group scope, they can manage all resources in the resource group."

# Question: 18

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

| Statements | Yes | No |
|---|---|---|
| Each Azure subscription can contain multiple account administrators. | ○ | ○ |
| Each Azure subscription can be managed by using a Microsoft account only. | ○ | ○ |
| An Azure resource group contains multiple Azure subscriptions. | ○ | ○ |

**Answer:**

No

No

No

**Explanation:**

Each Azure subscription can contain multiple account administrators.

• This is incorrect. An Azure subscription is tied to a single Azure account, and each account has only one Account Administrator. This role is the billing owner of the subscriptions within that account. While other administrative roles, such as Co-Administrator or Azure RBAC roles (like Owner), can be assigned to multiple users, the Account Administrator role is unique and singular.

Each Azure subscription can be managed by using a Microsoft account only.

• This is incorrect. Azure subscriptions are managed via identities within a Microsoft Entra ID (formerly Azure Active Directory) tenant. These identities can be work or school accounts (native to Microsoft Entra ID) or personal Microsoft accounts (e.g., outlook.com). Management is not restricted to only one type of account.

An Azure resource group contains multiple Azure subscriptions.

• This is incorrect. The hierarchy is reversed. An Azure subscription is a container for multiple resource groups. A resource group must exist within a single subscription and serves as a logical container for resources (like virtual machines, storage accounts, etc.) that are deployed within that subscription. A resource group cannot contain a subscription.

**References:**

Microsoft Documentation: "Azure classic subscription administrator roles, Azure RBAC roles, and Microsoft Entra roles".
Reference: Under the "Azure classic subscription administrator roles" section, it explicitly states, "There is one Account Administrator per Azure account." This document details the different administrative roles and their scopes.
Microsoft Documentation: "Azure fundamental concepts".
Reference: In the section "Azure resource hierarchy," the documentation clarifies the structure: Management groups Subscriptions Resource groups Resources. This confirms that resource groups are contained within subscriptions, not the other way around.
Microsoft Learn: "Describe Microsoft Entra ID".
Reference: This module explains that Microsoft Entra ID provides identity services and supports various identity types, including "work or school accounts" and "Microsoft accounts," which can be used to access Azure resources, disproving the claim that only Microsoft accounts can be used.

## Question: 19

DRAG DROP Match the Azure Services service to the correct descriptions. Instructions: To answer, drag the appropriate service from the column on the left to its description on the right. Each service may be used once, more than once, or not at all. NOTE: Each correct match is worth one point


### Answer:

Analyze security log files from Azure virtual machines: Azure Sentinel

Display the secure score for an Azure subscription: Azure Security Center



Store passwords for use by Azure Function applications: Azure Key Vault

### Explanation:

Azure Sentinel is Microsoft's cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution. Its primary function is to collect and analyze vast amounts of security data and logs from sources like Azure virtual machines to detect, investigate, and respond to threats.

Azure Security Center (now Microsoft Defender for Cloud) is a tool for security posture management. A key feature is the secure score, which assesses your Azure subscriptions against security recommendations and provides a numerical score to help you understand and improve your security posture.

Azure Key Vault is a cloud service designed to securely store and manage secrets, keys, and certificates. It is the appropriate service for an Azure Function application to store passwords or connection strings, avoiding the insecure practice of hardcoding them in the application's source code.

**References:**

Microsoft Learn Microsoft Sentinel Documentation. "What is Microsoft Sentinel?". This document states, "Microsoft Sentinel is a scalable, cloud-native solution that provides... Security information and event management (SIEM)... Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds." This confirms its role in analyzing log files from sources like VMs.

Microsoft Learn Microsoft Defender for Cloud Documentation. "Secure score in Microsoft Defender for Cloud." This official documentation explicitly details the function: "Microsoft Defender for Cloud continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level." This directly links the service to displaying a secure score.

Microsoft Learn Azure Key Vault Documentation. "About Azure Key Vault." The overview states, "Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys." This supports its use for storing passwords for applications like Azure Functions.

## Question: 20

Your company has a Software Assurance agreement that includes Microsoft SQL Server licenses You plan to deploy SQL Server on Azure virtual machines. What should you do to minimize licensing costs for the deployment?

A. Use Azure reservations.

B. Use Azure Hybrid Benefit

C. Deallocate the virtual machines during off hours.

D. Configure Azure Cost Management budgets.

**Answer:**

B

**Explanation:**

Azure Hybrid Benefit is a licensing program specifically designed for customers who have existing on-premises licenses with active Software Assurance (SA). It allows them to use these licenses for workloads running in Azure. For SQL Server on Azure Virtual Machines, applying the Hybrid Benefit means the customer only pays for the base compute infrastructure costs, effectively waiving the cost of the SQL Server license itself on the VM. This directly leverages the company's existing SA agreement to minimize licensing costs for the new cloud deployment, making it the most appropriate and cost-effective solution described.



**Why Incorrect Options are Wrong:**

A. Use Azure reservations.
Azure Reservations provide discounts on compute costs (the virtual machine infrastructure) by committing to a term, not on the SQL Server software licensing costs.
C. Deallocate the virtual machines during off hours.
This strategy reduces compute costs by stopping the VM but does not reduce the hourly rate of the SQL Server license when the VM is running.
D. Configure Azure Cost Management budgets.
This is a tool for monitoring and alerting on spending. It does not actively reduce costs; it only helps in tracking them against a defined budget.

**References:**

1. Microsoft Learn, AZ-900: Describe Azure cost management and Service Level Agreements. "Describe Azure Hybrid Benefit" section. This module explicitly states, "The Azure Hybrid Benefit is a licensing benefit that helps you to significantly reduce the costs of running your workloads in the cloud. It works by letting you use your on-premises Software Assurance-enabled Windows Server and SQL Server licenses on Azure."

2. Microsoft Azure Documentation, "Azure Hybrid Benefit for SQL Server on Azure Virtual Machines." Under the "Overview" section, it details, "Azure Hybrid Benefit is a licensing benefit that helps you to bring your on-premises core-based SQL Server licenses with active Software Assurance to Azure." It further clarifies that this benefit applies to SQL Server on Azure VMs.
3. Microsoft Learn, AZ-900: Describe factors that can affect costs in Azure. The "Reservations" section explains that reservations offer discounted prices on certain Azure services for a one- or three-year term, focusing on compute and other resource costs, not bring-your-own-license scenarios.

## Question: 21

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

A. Application security groups only

B. IP Addressess only

C. Service Tags only

D. IP Addresses, Service tags and Application security groups

### Answer:

D

### Explanation:

An Azure Network Security Group (NSG) inbound security rule filters network traffic destined for Azure resources. To define the origin of this traffic, the 'source' property of the rule can be configured with several options for maximum flexibility. These options include specific IP addresses or CIDR blocks, pre-defined Service Tags which represent groups of IP prefixes for specific Azure services (e.g., Storage, Sql), and Application Security Groups (ASGs), which allow you to group virtual machines and define network policies based on those logical groupings. Using all three provides granular control over network access.



### Why Incorrect Options are Wrong:

A. Incorrect. While Application Security Groups are a valid source, they are not the exclusive option; IP addresses and Service Tags are also permissible sources.
B. Incorrect. While IP addresses are a valid source, they are not the only option; Service Tags and Application Security Groups can also be used.
C. Incorrect. While Service Tags are a valid source, they are not the only option; IP addresses and Application Security Groups are also valid sources.

### References:

1. Microsoft Learn. (2024). Network security groups. Under the section "Security rules," the documentation states for Source and Destination: "Any, IP Addresses/CIDR block, service tag, or application security group."
2. Microsoft Learn. (2023). AZ-900: Describe core Azure concepts - Describe Azure network security groups. In the section "How do network security groups work?", the text specifies that a rule's source and destination "Can be an IP address, a CIDR block, a service tag, or an application security group."
3. Microsoft Learn. (2024). Virtual network service tags. Under the section "Service tags for network security groups," it explicitly states, "You can use service tags in your network security group inbound and outbound rules."

## Question: 22

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

| Statements | Yes | No |
|---|---|---|
| Azure China is operated by Microsoft. | ○ | ○ |
| Azure Government is operated by Microsoft. | ○ | ○ |
| Azure Government is available only to US government agencies and their partners. | ○ | ○ |

**Answer:**

No

Yes



Yes

**Explanation:**

Azure China is a sovereign cloud service that is physically isolated within mainland China. To comply with Chinese regulations, it is operated by a local partner, Shanghai Blue Cloud Technology Co., Ltd. (21Vianet), not directly by Microsoft. Microsoft provides the technology, but 21Vianet operates the datacenters.

Conversely, Azure Government is a sovereign cloud for the United States, which is directly operated by Microsoft. The services are managed by screened U.S. personnel. Its use is restricted to eligible U.S. government entities (federal, state, local, tribal) and their partners who handle controlled data, ensuring compliance with strict government security and compliance requirements.

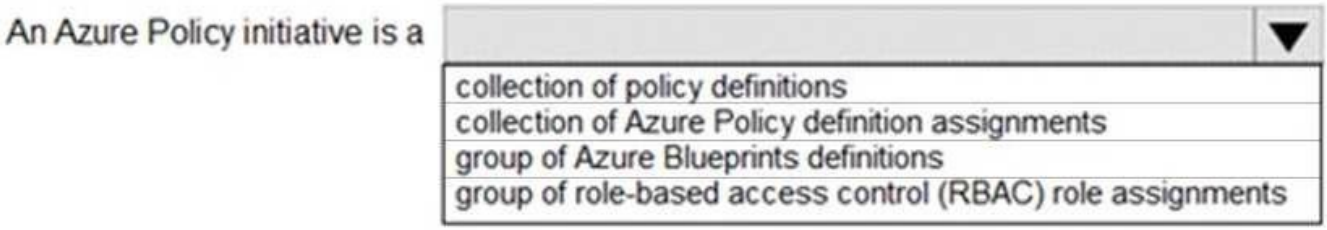
**References:**

Microsoft Azure Documentation. "Azure in China." This document explicitly states, "Microsoft Azure operated by 21Vianet (Azure China) is a physically separated instance of cloud services located in China. It's independently operated and transacted by Shanghai Blue Cloud Technology

Co., Ltd. ('21Vianet')."
Microsoft Azure Documentation. "What is Azure Government?" This resource clarifies, "Azure Government is a mission-critical cloud, operated by screened US persons..." and details its physical and network isolation from non-US government deployments.
Microsoft Learn. "Compare Azure Government and global Azure." Under the "Who can use Azure Government?" section, it specifies, "Azure Government is available to U.S. government (federal, state, and local) entities, and their partners who hold and process controlled data."

# Question: 23

HOTSPOT To complete the sentence, select the appropriate option in the answer area.




**Answer:**

collection of policy definitions

**Explanation:**

An Azure Policy initiative is a collection of policy definitions that are grouped together to help achieve a single, overarching goal. This approach simplifies the management of policies by allowing a set of related policies to be managed and assigned as a single item. For example, an organization might create a security initiative that includes multiple policy definitions, such as enforcing encryption, requiring specific network configurations, and auditing resource tags. This initiative can then be assigned to a subscription or management group to enforce all the contained policies at once.

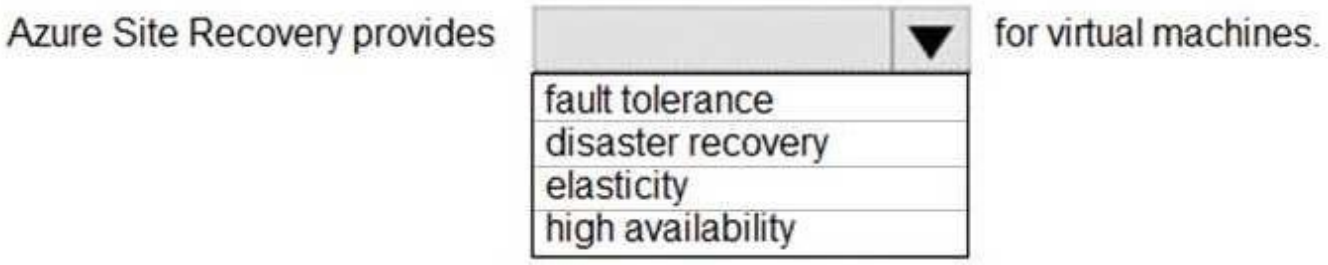


**References:**

Microsoft Azure Documentation, "Overview of Azure Policy":
Section: What is Azure Policy? Initiative definition
Content: "An initiative definition is a collection of policy definitions that are tailored towards achieving a singular overarching goal... For example, you could create an initiative with a goal to monitor your organization's compliance with the PCI DSS standard."
Microsoft Azure Documentation, "Azure Policy initiative definition structure":
Section: Initiative definition
Content: "An initiative definition is used to group several policy definitions to simplify assignments and management because you work with a group as a single item."

## Question: 24

HOTSPOT To complete the sentence, select the appropriate option in the answer area.




**Answer:**

disaster recovery

**Explanation:**

Azure Site Recovery is a native Disaster Recovery as a Service (DRaaS) offering. Its core purpose is to ensure business continuity by replicating workloads from a primary site to a secondary location. In the event of a disaster or major outage at the primary site, an organization can fail over to the secondary location to quickly resume operations.

While high availability and fault tolerance focus on preventing downtime from component failures within a single location (e.g., using redundant hardware or availability zones), disaster recovery specifically addresses site-level failures. Elasticity refers to the ability to scale resources up or down, which is a different cloud capability.

**References:**

Microsoft Corporation. "About Site Recovery." Microsoft Learn. Accessed September 11, 2025.
Reference Details: In the "Overview" section, the document states, "Azure Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there." This directly defines the service's role as a disaster recovery solution.
Microsoft Corporation. "High availability and disaster recovery for IaaS apps." Microsoft Learn. Accessed September 11, 2025.
Reference Details: This documentation explicitly distinguishes the concepts. It describes High Availability as measures taken within a region (e.g., Availability Sets, Availability Zones) to handle localized hardware failures, while describing Disaster Recovery as the process of "recovering from a catastrophic loss" by failing over to a different geographic region, which is the primary use case for Azure Site Recovery.

## Question: 25

To which cloud models can you deploy physical servers?

A. private cloud and hybrid cloud only

B. private cloud only

C. private cloud, hybrid cloud and public cloud

D. hybrid cloud only

### Answer:

A

### Explanation:

A private cloud is a cloud computing environment dedicated to a single organization. When hosted on-premises, the organization is responsible for purchasing, deploying, and managing its own physical servers and infrastructure. A hybrid cloud combines a private cloud with a public cloud. Consequently, an organization can deploy physical servers within the private cloud component of its hybrid cloud architecture. In a public cloud model, the cloud provider owns and manages all physical hardware; customers provision virtual resources on the provider's infrastructure and do not deploy their own physical servers.



### Why Incorrect Options are Wrong:

B. private cloud only: This is incorrect because a hybrid cloud, by definition, includes a private cloud component where an organization can deploy its physical servers.
C. private cloud, hybrid cloud and public cloud: This is incorrect because in a public cloud model, the cloud provider owns and manages the physical infrastructure. Customers cannot deploy their own physical servers into a public cloud provider's datacenter.
D. hybrid cloud only: This is incorrect because a standalone private cloud is a common model where an organization deploys and manages its own physical servers.

### References:

1. Microsoft Learn. "Describe cloud service types." AZ-900: Describe cloud concepts. Microsoft, n.d. In the section "What is a private cloud?", it states, "A private cloud may be hosted from your on-site datacenter. It can also be hosted by a third-party service provider." An on-site datacenter explicitly involves deploying physical servers. In the section "What is a public cloud?", it clarifies, "...you have no local hardware to manage or keep up-to-date; everything runs on your cloud provider's hardware."
2. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing (Special Publication 800-145). National Institute of Standards and Technology.
Section: 3. Deployment Models, Private cloud: "The cloud infrastructure is provisioned for

exclusive use by a single organization... It may be owned, managed, and operated by the organization... and it may exist on or off premises." The on-premises model requires the organization to deploy physical servers.
Section: 3. Deployment Models, Hybrid cloud: "The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public)..." This confirms a hybrid cloud contains a private component.

## Question: 26

In which type of cloud model are all the hardware resources owned by a third-party and shared between multiple tenants?

A. private

B. hybrid

C. public

### Answer:

C

### Explanation:

A public cloud is a deployment model where a third-party provider owns and operates all hardware resources, such as servers and storage, and delivers them over the internet. These resources are provisioned in a multi-tenant environment, meaning they are shared among multiple, distinct organizations or "tenants." This model offers economies of scale and a pay-as-you-go pricing structure, as customers only pay for the resources they consume. The defining characteristics are third-party ownership and shared infrastructure.

### Why Incorrect Options are Wrong:



A. private: In a private cloud, computing resources are used exclusively by a single business or organization and are not shared with other tenants.
B. hybrid: A hybrid cloud is a combination of public and private clouds, not a distinct model solely defined by shared, third-party-owned hardware.

### References:

1. Microsoft Learn. (2024). Describe the different types of cloud models. In "AZ-900: Describe cloud concepts". "The public cloud is defined as computing services offered by third-party providers over the public Internet, making them available to anyone who wants to use or purchase them. They may be free or sold on-demand, allowing customers to pay only per usage for the CPU cycles, storage, or bandwidth they consume..... In a public cloud, you share the same hardware, storage, and network devices with other organizations or cloud "tenants.""
Source: Microsoft Learn, Module "Describe cloud concepts", Unit "Describe the different types of cloud models".
2. Microsoft Learn. (2024). What is a Private Cloud?. Microsoft Azure Documentation. "A private cloud consists of computing resources used exclusively by one business or organization. In a private cloud, the services and infrastructure are always maintained on a private network, and the hardware and software are dedicated solely to your organization."
Source: Microsoft Azure, "Cloud computing concepts" section.

3. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing (Special Publication 800-145). National Institute of Standards and Technology.
Section: "3. Deployment Models", Page 3. "Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider."

## Question: 27

DRAG DROP Match the cloud model to the correct advantage. Instructions: To answer, drag the appropriate cloud model from the column on the left to its advantage on the right. Each cloud model may be used once, more than once, or not at all. NOTE: Each correct match is worth one point

| Cloud model | Work Area | |
|---|---|---|
| Hybrid Cloud | | No required capital expenditure. |
| Private Cloud | | Provides complete control over security. |
| Public Cloud | | Provides a choice to use on-premises or cloud-based resources. |

**Answer:**

No required capital expenditure: Public Cloud

Provides complete control over security: Private Cloud

Provides a choice to use on-premises or cloud-based resources: Hybrid Cloud

**Explanation:**



The correct pairings are based on the fundamental characteristics of each cloud deployment model.

• Public Cloud: Resources are owned and operated by a third-party provider and delivered over the internet. This model eliminates capital expenditure (CapEx) for purchasing hardware and shifts costs to an operational expenditure (OpEx) model, where you pay only for what you consume.

• Private Cloud: The computing infrastructure is dedicated to a single organization. Because the organization manages and controls the entire environment, it can implement and maintain its own specific security policies, offering a high degree of control.

• Hybrid Cloud: This model integrates a private cloud (or on-premises infrastructure) with a public cloud. This combination allows organizations the flexibility to place workloads in the most appropriate environment, giving them a choice between using their own resources or cloud-based resources.

**References:**

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing (Special Publication 800-145). National Institute of Standards and Technology.
Public Cloud (Section 2): "The cloud infrastructure is provisioned for open use by the general public... It is owned, managed, and operated by a business, academic, or government organization, or some combination of them." This provider-owned model is the basis for eliminating customer capital expenditure.
Private Cloud (Section 2): "The cloud infrastructure is provisioned for exclusive use by a single organization... It may be owned, managed, and operated by the organization, a third party, or some combination of them..." This exclusivity provides the foundation for complete control over security.
Hybrid Cloud (Section 2): "The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public)..." This composition is what provides the choice of using on-premises or cloud resources.
DOI: https://doi.org/10.6028/NIST.SP.800-145
Microsoft Azure Documentation. What are public, private, and hybrid clouds?
Public Cloud: "With a public cloud, you don't have to purchase any hardware or software... you trade capital expenses for operational expenses."
Private Cloud: "...services and infrastructure are maintained on a private network...This single-tenant environment means that the hardware, and software are dedicated solely to your organization. A private cloud offers the highest levels of control and security."
Hybrid Cloud: "Hybrid clouds combine on-premises infrastructure-or a private cloud-with a public cloud. Hybrid clouds allow data and apps to move between the two environments."

## Question: 28

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

A. Azure Advisor

B. Azure Service Health

C. Azure Monitor

D. Azure Network Watcher

### Answer:

C

### Explanation:

Azure Monitor is the comprehensive solution for collecting, analyzing, and acting on telemetry from your Azure and on-premises environments. It includes the Azure Activity Log, which records all subscription-level events, such as an administrator stopping a virtual machine (the 'Deallocate Virtual Machine' operation). You can create alert rules in Azure Monitor that are triggered by specific Activity Log events. This allows you to automatically send a notification or take an automated action when a VM is stopped by an administrator.



### Why Incorrect Options are Wrong:

A. Azure Advisor: This service provides recommendations to optimize Azure resources for cost, security, and performance. It does not provide real-time event monitoring or alerting for administrative actions.
B. Azure Service Health: This service monitors the health of the Azure platform and services, not the state of your individual resources or administrative actions performed on them.
D. Azure Network Watcher: This is a suite of tools for monitoring and diagnosing network-related issues within your Azure virtual networks. It does not monitor the operational state of virtual machines.

### References:

1. Microsoft Learn. "Overview of Azure Monitor." Azure Monitor Documentation. This document states, "Azure Monitor helps you maximize the availability and performance of your applications and services. It delivers a comprehensive solution for collecting, analyzing, and acting on telemetry..." and lists "Respond to critical situations with alerts."
2. Microsoft Learn. "Create, view, and manage activity log alerts by using Azure Monitor." Azure Monitor Documentation. This guide details the process: "Activity log alerts are alerts that activate when a new activity log event occurs that matches the conditions specified in the alert... For example, you can receive an alert when a user deletes a virtual machine in your subscription."

The action of stopping a VM is a similar administrative event.

3. Microsoft Learn. "Introduction to Azure Advisor." Azure Advisor Documentation. This source clarifies Advisor's role: "Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments."

4. Microsoft Learn. "What is Azure Service Health?" Azure Service Health Documentation. This document explains, "Azure Service Health is a suite of experiences that provide personalized guidance and support when issues with Azure services affect you."

# Question: 29

You have an Azure environment. You need to create a new Azure virtual machine from a tablet that runs the Android operating system. What are three possible solutions? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Use Bash in Azure Cloud Shell.

B. Use PowerShell in Azure Cloud Shell.

C. Use the PowerApps portal.

D. Use the Security & Compliance admin center.

E. Use the Azure portal.

**Answer:**

A, B, E

**Explanation:**

The requirement is to create an Azure virtual machine from an Android tablet. This necessitates using tools that are accessible through a web browser or a dedicated mobile application.
1. Azure portal (E): A web-based, unified console that provides a graphical user interface (GUI) to provision and manage Azure resources. It is accessible from any modern web browser, including those on an Android tablet.
2. Azure Cloud Shell (A, B): An interactive, authenticated, browser-accessible shell for managing Azure resources. It provides the flexibility of choosing between Bash (with the Azure CLI) and PowerShell, both of which can be used to create virtual machines via command-line instructions. Since Cloud Shell runs in a browser, it is fully functional on an Android tablet.

**Why Incorrect Options are Wrong:**

C. Use the PowerApps portal.
The PowerApps portal is used for creating and managing low-code business applications, not for direct Azure infrastructure deployment like creating a VM.
D. Use the Security & Compliance admin center.
This is a Microsoft 365 portal for managing security and compliance features; it cannot be used to create or manage Azure infrastructure resources.

**References:**

1. Azure portal: Microsoft Learn. (2023). What is the Azure portal? "The Azure portal is a web-based, unified console that provides an alternative to command-line tools... You can manage your Azure subscription using a graphical user interface..... You can access the portal from any modern browser on any device."

Source: Microsoft Learn, "Describe the core architectural components of Azure," Module: "Describe Azure management and governance," Unit: "What is the Azure portal?"
2. Azure Cloud Shell (Bash & PowerShell): Microsoft Learn. (2023). Overview of Azure Cloud Shell. "Azure Cloud Shell is an interactive, authenticated, browser-accessible shell for managing Azure resources. It provides the flexibility of choosing the shell experience that best suits the way you work, either Bash or PowerShell."
Source: Microsoft Learn, "Azure Cloud Shell overview."
3. Creating a VM with Azure Tools: Microsoft Learn. (2023). Create a Windows virtual machine in Azure. This document details the methods for creating a VM using the Azure portal, Azure PowerShell, and Azure CLI, confirming all three are valid management tools for this task.
Source: Microsoft Learn, "Quickstart: Create a Windows virtual machine in the Azure portal." (This page also links to the PowerShell and CLI quickstarts).

## Question: 30

You plan to deploy several Azure virtual machines. You need to ensure that the services running on the virtual machines are available if a single data center fails. Solution: You deploy the virtual machines to a scale set. Does this meet the goal?

A. Yes

B. No

### Answer:

B

### Explanation:

A Virtual Machine Scale Set (VMSS) is a compute resource used to deploy and manage a set of identical virtual machines. While a VMSS can be configured to provide high availability across data centers by distributing instances across multiple Availability Zones, this is not its default or only configuration. A scale set can also be deployed within a single Availability Zone. If the scale set is deployed to a single zone and that zone (representing one or more data centers) fails, the entire application becomes unavailable. Therefore, simply deploying to a scale set is insufficient to meet the goal; it must be explicitly configured to be zone-redundant.



### Why Incorrect Options are Wrong:

A. Yes: This is incorrect because the solution is incomplete. Deploying to a scale set does not automatically guarantee protection against a data center failure unless it is specifically configured to span multiple Availability Zones.

### References:

1. Microsoft Learn. (2023). What are Virtual Machine Scale Sets? - In the "High availability and scale sets" section, it states, "To provide high availability, you can use Availability Zones to automatically distribute VM instances in a scale set... across multiple datacenters." This highlights that using Availability Zones is a specific configuration for achieving this goal.
2. Microsoft Learn. (2023). Regions and Availability Zones in Azure. - The "Availability Zones" section defines them as "unique physical locations within an Azure region" designed to protect applications and data from datacenter failures. This establishes the correct mechanism for meeting the requirement.
3. Microsoft Learn. (2023). Create a Virtual Machine Scale Set that uses Availability Zones. - The document's overview explicitly states, "To protect your virtual machine scale sets from datacenter-level failures, you can create a scale set across Availability Zones." This confirms that creating a scale set alone is not enough; it must be configured to use zones.
4. Microsoft Learn. (2024). AZ-900: Describe core Azure architectural components. - The module

on "Describe Azure regions, availability zones, and region pairs" explains that Availability Zones are the feature used to ensure services remain available during datacenter failures.

## Question: 31

Your company is planning a deployment using Azure Database for PostgreSQL. The deployment should meet the following requirements: - Up to 10 TB storage - Azure Premium Storage - Point-in-time-restore for up to 35 days You need to select the appropriate deployment and pricing tier to meet these requirements and minimize costs. What should you select?

A. Azure Database for PostgreSQL Single Server Memory Optimized tier

B. Azure Database for PostgreSQL Hyperscale (Citus)

C. Azure Database for PostgreSQL Single Server General Purpose tier

D. Azure Database for PostgreSQL Single Server Basic tier

### Answer:

C

### Explanation:

The General Purpose tier for Azure Database for PostgreSQL - Single Server is the most appropriate and cost-effective choice. It meets all specified requirements: it supports storage up to 16 TB (exceeding the 10 TB need), utilizes high-performance storage, and allows for a point-in-time restore backup retention period of up to 35 days. Compared to the Memory Optimized tier, it offers a balanced compute and memory configuration at a lower cost, which aligns with the goal of cost minimization since no memory-intensive workload was specified. The Hyperscale (Citus) option is designed for larger, distributed workloads and would be significantly more expensive.



### Why Incorrect Options are Wrong:

A. Azure Database for PostgreSQL Single Server Memory Optimized tier: This tier meets the technical requirements but is more expensive than the General Purpose tier and is designed for memory-intensive workloads, which were not specified.
B. Azure Database for PostgreSQL Hyperscale (Citus): This is a scale-out deployment option for massively parallel workloads, making it unnecessarily complex and more costly for the specified 10 TB requirement.
D. Azure Database for PostgreSQL Single Server Basic tier: This tier does not meet the storage requirement, as it is limited to a maximum of 1 TB of storage.

### References:

1. Microsoft Documentation, "Pricing tiers in Azure Database for PostgreSQL - Single Server": This document outlines the specifications for each tier.
Section: "Basic pricing tier": "Max Storage: 1 TB". This confirms why option D is incorrect.
Section: "General Purpose and Memory Optimized pricing tiers": "Max Storage: 16 TB". This

confirms that both General Purpose and Memory Optimized tiers meet the storage requirement. It also describes General Purpose as suitable for "most business workloads" and Memory Optimized for "high-performance database workloads," indicating a cost and performance difference.

2. Microsoft Documentation, "Backup and restore in Azure Database for PostgreSQL - Single Server": This document details the backup capabilities.

Section: "Backup retention": "Backups are retained for a period you specify, between 7 and 35 days. The default retention period is seven days. You can set the retention period... for all tiers (Basic, General Purpose, and Memory Optimized)." This confirms all single-server tiers meet the 35-day restore requirement.

3. Microsoft Documentation, "What is Azure Database for PostgreSQL?": This document describes the different deployment options.

Section: "Azure Database for PostgreSQL - Hyperscale (Citus)": Describes this option as one that "horizontally scales queries across multiple machines using sharding," which is intended for workloads approaching or exceeding 100 GB of data, indicating it is for larger-scale needs than Single Server. This supports why option B is not the most cost-effective choice.

## Question: 32

Your company uses management groups to manage resources in your Azure tenant more efficiently. User1 should be able to assign access and assign policies to management groups. You need to determine to which role-based access control (RBAC) role User1 should be added. Your solution should follow the principle of least privilege. To which role should you add User1?

A. Owner

B. User Access Administrator

C. Management Group Contributor

D. Contributor

### Answer:

B

### Explanation:

The User Access Administrator role is the most appropriate choice as it adheres to the principle of least privilege. This role grants permissions to manage user access and policy assignments for resources within the scope it is assigned. Specifically, it includes the Microsoft.Authorization/ permission, which allows a user to create and manage both role assignments ("assign access") and policy assignments. It does not grant broad permissions to create, modify, or delete the resources themselves, unlike the Owner or Contributor roles. This provides the exact capabilities required by User1 without granting unnecessary privileges.



### Why Incorrect Options are Wrong:

A. Owner: This role violates the principle of least privilege by granting full control over all resources and their access, which is more than the required permissions.
C. Management Group Contributor: This role allows for managing management groups and subscriptions but crucially lacks the permission to assign access (manage role assignments) to other users.
D. Contributor: This role can manage resources but cannot assign access to other users or groups, failing to meet a primary requirement of the task.
---

### References:

1. Microsoft Learn. (2023). Azure built-in roles.
Section: "User Access Administrator"
Content: "Lets you manage user access to Azure resources." The role's permissions include Microsoft.Authorization/, which covers both role assignments and policy assignments.
Section: "Owner" and "Contributor"

Content: The documentation explicitly states that the Contributor role "does not allow you to assign roles in Azure RBAC," while the Owner role has "full access to manage all resources," making it overly permissive.
2. Microsoft Learn. (2023). What are Azure management groups?
Section: "Azure custom RBAC roles for management groups"
Content: This document explains how RBAC roles, including built-in ones like User Access Administrator, can be applied at the management group scope to control access and policy for all subscriptions within that group.
3. Microsoft Learn. (2023). Best practices for Azure RBAC.
Section: "Only grant the access users need"
Content: This section details the principle of least privilege, stating, "It's a best practice to grant users the least privilege to get their work done. Avoid assigning broader roles at broader scopes even if it initially seems more convenient." This supports selecting User Access Administrator over Owner.

## Question: 33

A team has an Azure Cosmos DB account. A solution needs to be in place to generate an alert from Azure Log Analytics when a query request charge exceeds 40 units more than 10 times during a 10- minute window. Which of the following would you recommend? (Choose two)

A. Create a search query to identify when the requestCharges exceeds 10.

B. Configure a period of 10 and a frequency of 10.

C. Create a search query to identify when the requestCharges exceeds

D. Create a search query to identify when the durations exceeds 10.

### Answer:

B, C

### Explanation:

To meet the requirement, you must create a log alert rule in Azure Monitor. This process involves two key configurations. First, you need a Kusto Query Language (KQL) search query to filter the diagnostic logs for the specific condition. The requirement is to identify when the "request charge exceeds 40 units," which translates to a query where requestCharges 40. Second, you must configure the alert logic's time parameters. The "10-minute window" directly corresponds to the Period setting in the alert rule. Setting both the Period and Frequency to 10 minutes ensures the query evaluates the last 10 minutes of data every 10 minutes, which is the standard configuration for this type of windowed alert.



### Why Incorrect Options are Wrong:

A. The specified request charge threshold in the requirement is 40, not 10.
D. The alert condition is based on the request charge (requestCharges), not the query execution time (durations).

### References:

1. Microsoft Learn, Azure Cosmos DB Documentation. "Monitor Azure Cosmos DB data by using diagnostic settings in Azure". This document details the fields available in Azure Cosmos DB diagnostic logs, confirming that requestCharge represents the Request Units (RUs) consumed. The query must filter on this value.
2. Microsoft Learn, Azure Monitor Documentation. "Create or edit an alert rule". In the "Configure alert logic" section, it explains the Period and Frequency settings. Period is defined as "The time range over which to evaluate the collected data," which corresponds to the "10-minute window" in the question.
3. Microsoft Learn, Azure Monitor Documentation. "Log alerts in Azure Monitor". This article describes the components of a log alert rule, including the "Condition," which consists of the log

query and the measurement settings (e.g., period, frequency, threshold). This confirms that both a correct query and time configuration are necessary.

# Question: 34

Which service provides network traffic filtering across multiple Azure subscriptions and virtual networks?

A. Azure Firewall

B. an application security group

C. Azure DDoS protection

D. a network security group (NSG)

**Answer:**

A

**Explanation:**

Azure Firewall is a managed, cloud-based network security service designed to protect Azure Virtual Network resources. A key feature is its ability to provide centralized network traffic filtering and policy enforcement. It can be deployed in a central virtual network (a hub-and-spoke model) to govern and log traffic for spoke virtual networks, which can reside in the same or different subscriptions. This centralized control model directly addresses the requirement of filtering traffic across multiple subscriptions and virtual networks, making it the correct service for this scenario.



**Why Incorrect Options are Wrong:**

B. an application security group: Application security groups (ASGs) are used to group VMs within a single virtual network to simplify rule creation in a Network Security Group (NSG); they do not operate across V-Nets.
C. Azure DDoS protection: This service is specifically designed to mitigate Distributed Denial of Service (DDoS) attacks, not for general, user-defined network traffic filtering based on custom rules.
D. a network security group (NSG): An NSG provides traffic filtering for resources within a single virtual network. It cannot be applied centrally to filter traffic across multiple virtual networks or subscriptions.

**References:**

1. Microsoft Azure Documentation. "What is Azure Firewall?" Microsoft Learn. "You can create, enforce, and log application and network connectivity policies across subscriptions and virtual networks." This statement directly confirms that Azure Firewall is designed for this purpose. Source: https://learn.microsoft.com/en-us/azure/firewall/overview, Introduction section, Paragraph 2.
2. Microsoft Azure Documentation. "Azure Firewall Manager." Microsoft Learn. "Azure Firewall Manager is a security management service that provides central security policy and route

management for cloud-based security perimeters." This highlights its role in centralized management across different network topologies.
Source: https://learn.microsoft.com/en-us/azure/firewall-manager/overview, Introduction section, Paragraph 1.
3. Microsoft Azure Documentation. "Network security groups." Microsoft Learn. "You can associate a network security group to, or disassociate a network security group from: Network interface... Subnet..." This shows an NSG's scope is limited to components within a single virtual network.
Source: https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview, "Associate a network security group" section.
4. Microsoft Azure Documentation. "Application security groups." Microsoft Learn. "All network interfaces assigned to an application security group must exist in the same virtual network that the first network interface assigned to the application security group is in." This confirms ASGs are scoped to a single VNet.
Source: https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups, "Application security groups" section, Constraints paragraph.

## Question: 35

A company is planning on deploying a stateless based application based on microservices using the Azure Service Fabric service. You need to design the infrastructure that would be required in the Azure Service Fabric service. Which of the following should you consider? (Choose two)

A. The network connectivity

B. The number of node types in the cluster

C. The properties for each node type

D. The service tier

### Answer:

B, C

### Explanation:

When designing the infrastructure for an Azure Service Fabric cluster, two fundamental considerations are the node types and their specific properties. A node type maps to an underlying Virtual Machine Scale Set. You must decide on the number of node types required (e.g., one for front-end services and another for back-end services). For each node type, you must then define its properties, which include the VM size (SKU), the number of instances (nodes), the durability tier, and the reliability tier. These choices directly determine the cluster's capacity, performance, and fault tolerance.



### Why Incorrect Options are Wrong:

A. The network connectivity is a general Azure infrastructure consideration, not a specific design choice within the Service Fabric cluster itself.
D. Azure Service Fabric does not have a "service tier" in the same way as services like Azure SQL Database. It uses reliability and durability tiers for its node types.

### References:

1. Microsoft Azure Documentation, "Service Fabric cluster capacity planning considerations." This document explicitly states, "A key part of planning for any Service Fabric production deployment is cluster capacity planning. Key considerations include... The number of node types and their properties." It further details that properties include durability, reliability, and VM SKU. Source: learn.microsoft.com/en-us/azure/service-fabric/service-fabric-cluster-capacity-planning, Section: "Key capacity planning considerations".
2. Microsoft Azure Documentation, "Azure Service Fabric node types and virtual machine scale sets." This page clarifies the relationship between node types and the underlying infrastructure. It states, "Each node type that is defined in a Service Fabric cluster is set up as a separate virtual machine scale set... For each node type, you can independently scale it up or down... and have

different capacity metrics." This confirms that defining the number of node types (B) and their properties (C) are core design tasks.
Source: learn.microsoft.com/en-us/azure/service-fabric/service-fabric-cluster-nodetypes, Section: "Node types and virtual machine scale sets".