Microsoft Azure AZ-500 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-500 Exam Dumps by Cert Empire

Question: 1

You have an Azure Active Directory (Azure AD) tenant. The tenant contains users that are assigned Azure AD Premium Plan 2 licenses. You have an partner company that has a domain named The fabrikam.com domain contains a user named user'. User' has an email address of userl@tabrikam.com. You to provide User1 with to the resources in the tenant The solution must meet the following requirements: user1 must be able to sign in by using the userl@fabrikam.com credentials You must be able to grant User1 access to the resources in the tenant Administrative effort must be minimized. What should you do?

A. Create a user account for user1.

B. Create an invite for User1.

C. To the tenant add fabrikamcom as a custom domain

D. Set Enable guest self-service sign up via user flows to Yes for the tenant.

Answer:

B

Explanation:

Azure Active Directory (Azure AD) Business-to-Business (B2B) collaboration is the feature designed for this scenario. By sending an invitation to user1@fabrikam.com, a guest user object is created in your tenant. This allows User1 to authenticate using their existing Fabrikam credentials, fulfilling a key requirement. Once the invitation is accepted, this guest user object can be granted access to resources (applications, groups, etc.) within your tenant just like a native member user. This method is the most direct and requires the least administrative overhead, as you do not need to manage the user's identity, password, or domain.

Why Incorrect Options are Wrong:

A. Create a user account for user1.
This creates a new member user with a new password managed by your tenant, violating the requirement for the user to sign in with their existing credentials.
C. To the tenant add fabrikam.com as a custom domain.
This is an incorrect and high-effort action. It implies you are taking ownership of the partner's domain, which is not feasible or appropriate for collaboration.
D. Set Enable guest self-service sign up via user flows to Yes for the tenant.
This enables a broad sign-up capability for applications, which is more complex than needed. A direct invitation is the most minimal and targeted approach for a single, known partner user.

References:

1. Microsoft Documentation, Azure Active Directory B2B collaboration overview: "With Azure AD B2B, the partner uses their own identity management solution, so there's no external administrative overhead for your organization. Guest users sign in to your apps and services with their own work, school, or social identities."
Source: Microsoft Docs, "What is Azure Active Directory B2B collaboration?", Section: "Collaborate with any partner using their identities".
2. Microsoft Documentation, Add B2B collaboration users: "An admin can add a guest user to the organization in the Azure portal... The user receives an invitation email with a redemption link. The user selects the link, and then follows the prompts to sign in."
Source: Microsoft Docs, "Add Azure Active Directory B2B collaboration users in the Azure portal", Section: "Invite guest users to your directory".
3. Microsoft Documentation, Properties of a B2B guest user: "A B2B collaboration user is a user with UserType = Guest... These guest users have limited permissions in the directory, and they can be managed like any other user in your directory." This confirms that once invited, they can be granted access to resources.
Source: Microsoft Docs, "Properties of an Azure Active Directory B2B collaboration user", Section: "Key properties of the Azure AD B2B collaboration user".

Question: 2

You have an Azure Active Directory (Azure AD) tenant that contains a group named Group1 You need to ensure that the members of Group1 sign in by using passwordless authentication What should you do?

A. Configure the Microsoft Authenticator authentication method policy.

B. Configure the certificate-based authentication (CBA) policy.

C. Configure the sign-in risk policy.

D. Create a Conditional Access policy.

Answer:

A

Explanation:

To enable passwordless authentication for a specific group using the Microsoft Authenticator app, an administrator must configure the corresponding authentication method policy. This policy, found within Azure AD's authentication methods section, allows administrators to enable the feature, target specific users or groups (such as Group1), and set the "Authentication mode" to "Passwordless". This is the direct and foundational step required to allow and configure members of Group1 to register and use their phones for passwordless sign-in.

Why Incorrect Options are Wrong:

B. Configure the certificate-based authentication (CBA) policy.
This enables a different form of passwordless authentication that uses X.509 certificates, not the Microsoft Authenticator app, which is a primary method for this scenario.
C. Configure the sign-in risk policy.
This policy is part of Azure AD Identity Protection and is used to enforce controls based on the calculated risk of a sign-in, not to mandate a specific authentication method.
D. Create a Conditional Access policy.
While a Conditional Access policy can enforce the use of a passwordless method by requiring a specific authentication strength, the method itself must first be enabled and configured for the target group via its own policy.

References:

1. Microsoft Entra documentation, "Enable passwordless sign-in with Microsoft Authenticator": This document outlines the precise steps. In the "Enable the passwordless authentication method" section, it states: "Browse to Protection Authentication methods Policies. Under Microsoft Authenticator, choose the following options: ... Target - All users or Select users.....For users in the target group(s), set Authentication mode to Passwordless." This directly corresponds

to option A.
Source: Microsoft Learn, learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-authentication-passwordless-phone
2. Microsoft Entra documentation, "Manage authentication methods for Azure AD": This document explains the role of authentication method policies. It states, "You can manage the authentication methods used in your Azure AD tenant from the Authentication methods policy... The policy has settings for each method that let you control how it's used." This confirms that the method policy is the correct place for this configuration.
Source: Microsoft Learn, learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods-manage
3. Microsoft Entra documentation, "Conditional Access: Authentication strength": This source clarifies the role of Conditional Access, which is to require a certain level of authentication. It states, "Authentication strength allows administrators to specify which combination of authentication methods can be used to access a resource." This shows it's an enforcement tool, secondary to enabling the method itself as described in option A.
Source: Microsoft Learn, learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-authentication-strengths

Question: 3

HOTSPOT You have an Azure subscription that contains a user named User1 and a storage account named storage 1. The storage1 account contains the resources shown in the following table:

Name	Type
container1	Container
folder1	File share
table1	Table

User1 is assigned the following roles for storage1:

• Storage Blob Data Reader

• Storage Table Data Contributor

• Storage File Data SMB Share Reader

Statements	Yes	No
On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.	○	○
On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure Active Directory (Azure AD) credentials, he can delete the files in folder1.	○	○
On October 1, 2022, User1 can delete the rows in table1 by using SAS1.	○	○

Answer:

Statement 1: On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.

• Correct Answer: Yes

Statement 2: On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure Active Directory (Azure AD) credentials, he can delete the files in folder1.

• Correct Answer: No

Statement 3: On October 1, 2022, User1 can delete the rows in table1 by using SAS1.

• Correct Answer: Yes

Explanation:

(Yes) The first statement is correct. A Shared Access Signature (SAS) token's permissions are independent of a user's RBAC roles. Since the SAS1 token is configured to allow Delete permissions on the File service and is valid on October 1, 2022, it can be used to delete files in the folder1 file share.

(No) The second statement is incorrect. When using Azure AD credentials to map a drive, permissions are governed by the user's assigned RBAC roles. User1 has the Storage File Data SMB Share Reader role, which only grants read access. To delete files, a role with write/delete permissions, such as Storage File Data SMB Share Contributor, would be required.

(Yes) The third statement is correct. Similar to the first statement, the permissions granted by SAS1 are key. The SAS token allows Delete permissions for the Table service and is valid on the specified date. Therefore, it can be used to delete rows (entities) from table1.

References:

Microsoft Documentation, "Grant limited access to Azure Storage resources using shared access signatures (SAS)": This document specifies the permissions available for a service SAS. For the File service, the d permission allows for the deletion of a file. For the Table service, the d permission allows for the deletion of an entity. This supports the reasoning for statements 1 and 3.

Microsoft Documentation, "Assign share-level permissions": This document outlines the built-in RBAC roles for Azure Files. It explicitly states that the Storage File Data SMB Share Reader role provides "read access to files and directories in Azure file shares." It does not include delete permissions, which supports the reasoning for statement 2.
Microsoft Documentation, "Authorize access to tables using Azure Active Directory": This resource details the RBAC roles for Table storage. It lists the Storage Table Data Contributor role, which User1 has, granting read, write, and delete permissions via Azure AD. However, statement 3 specifically asks about access using SAS1, making the SAS token's permissions the deciding factor.

Question: 4

You have an Azure subscription that contains a web app named App1. Users must be able to select between a Google identity or a Microsoft identity when authenticating to App1. You need to add Google as an identity provider in Azure AD. Which two pieces of information should you configure? Each correct answer presents part of the solution.

A. a tenant name

B. a tenant ID

C. the endpoint URL Of an application

D. a client ID

E. a client secret

Answer:

D, E

Explanation:

To federate Azure Active Directory (Azure AD) with Google for user authentication, you must register your application with Google's identity platform. This is done through the Google API Console. During this registration process, Google provides two critical pieces of information: a Client ID and a Client Secret.

The Client ID is a public identifier for your application. The Client Secret is a confidential value known only to your application and Google. Both are required in the Azure AD identity provider configuration to establish a secure OAuth 2.0 trust relationship, allowing Azure AD to delegate authentication requests to Google and securely receive identity tokens.

Why Incorrect Options are Wrong:

A. A tenant name is the domain name for your Azure AD instance (e.g., contoso.onmicrosoft.com) and is not part of the Google federation configuration.

B. A tenant ID is the unique identifier (GUID) for your Azure AD tenant and is not a value provided by or configured for Google federation.

C. The endpoint URL, specifically the redirect URI, is a value from Azure AD that you configure in the Google API Console, not a value you receive from Google to configure in Azure.

References:

1. Microsoft Learn: Add Google as an identity provider for B2B guest users. In "Step 3: Configure Google federation in Azure AD," the instructions state: "In the Client ID box, paste the client ID you copied earlier. In the Client secret box, paste the client secret you copied earlier." This confirms that the Client ID and Client Secret obtained from Google are the required configuration

values.

2. Microsoft Learn: Tutorial: Add an identity provider to your Azure Active Directory B2C tenant. In the section "Configure Google as an identity provider," the steps require you to "Enter the Client ID of the Google application that you created earlier" and "Enter the Client secret that you recorded." This demonstrates the same requirement for Azure AD B2C scenarios.

Question: 5

You have an Azure key vault named Vault1 that stores the resources shown in following table.

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?

A. Key1 Only

B. Cert1 only

C. Key1 and Secret1 only

D. Key1 and Cert1 only

E. Secret1 and Cert1 only

F. Key1, Secret1, and Cert1

Answer:

C

Explanation:

Azure Key Vault provides a specific, configurable feature named "rotation policy" for both keys and secrets. For keys, the rotation policy automates the generation of a new key version at a scheduled time or after a specific duration. For secrets, the rotation policy integrates with Azure Event Grid and automation services (like Azure Functions or Logic Apps) to manage the lifecycle of credentials such as database connection strings.
While certificates have automated renewal capabilities, this is configured within the certificate's "Issuance Policy" through "Lifetime Actions," which is a distinct mechanism from the feature explicitly named "rotation policy" that applies to keys and secrets.

Why Incorrect Options are Wrong:

A. Key1 Only: This is incorrect because secrets also support a configurable rotation policy.
B. Cert1 only: This is incorrect. Certificates use an "Issuance Policy" for renewal, not a "rotation policy," and both keys and secrets support rotation policies.
D. Key1 and Cert1 only: This is incorrect because the feature for certificates is named "Issuance Policy," not "rotation policy," and secrets do support rotation.
E. Secret1 and Cert1 only: This is incorrect because keys support a rotation policy, and the

feature for certificates is named differently.

F. Key1, Secret1, and Cert1: This is incorrect because the specific "rotation policy" feature, by name and implementation, applies to keys and secrets, not certificates.

References:

1. Microsoft Documentation - Configure key auto-rotation in Azure Key Vault: "Azure Key Vault automates the rotation of keys in a key vault. When you configure a key rotation policy, you can customize the rotation frequency." (Section: "Key rotation policy")
2. Microsoft Documentation - Configure secret auto-rotation in Azure Key Vault: "Azure Key Vault automates the rotation of secrets for databases or services that use a username and password for authentication... You can set a rotation policy on a secret to schedule rotation..." (Section: "Secret rotation policy")
3. Microsoft Documentation - Tutorial: Configure certificate auto-rotation in Key Vault: "To configure certificate auto-rotation... 3. Select the Issuance Policy tab... 4. Set the Lifetime Action Type to Automatically renew at a given percentage lifetime." (Section: "Create a certificate in Key Vault") This reference demonstrates that certificate lifecycle management uses an "Issuance Policy" and "Lifetime Actions," distinguishing it from the "rotation policy" of keys and secrets.

Question: 6

You have an Azure subscription that contains a You need to grant user1 access to blob1. The solution must ensure that the access expires after six days. What should you use?

A. a shared access policy

B. a shared access signature (SAS)

C. role-based access control (RBAC)

D. a managed identity

Answer:

B

Explanation:

A Shared Access Signature (SAS) is the most appropriate solution for providing temporary, delegated access to a specific resource in Azure Storage. A SAS is a URI that includes a token containing a set of query parameters. These parameters define the permissions granted (e.g., read, write), the resource being accessed (in this case, blob1), and a validity interval, including a mandatory expiry time. This allows you to grant user1 access to blob1 that automatically expires after the specified six-day period, meeting all the requirements of the scenario precisely.

Why Incorrect Options are Wrong:

A. a shared access policy: A shared access policy is defined on a container to manage a group of SAS tokens, but it does not directly grant access itself. A SAS is still required.
C. role-based access control (RBAC): RBAC grants permissions to identities (users, groups) but does not natively provide a simple, time-bound expiry mechanism. This would grant persistent access until manually revoked.
D. a managed identity: A managed identity is an identity for an Azure resource (like a VM or Function App) to authenticate to other services, not for granting access to an external user.

References:

1. Microsoft Documentation, "Grant limited access to Azure Storage resources using shared access signatures (SAS)": "A shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control over how a client can access your data. For example: ... How long the SAS is valid, including the start time and the expiry time." This document explicitly details the use of an expiry time as a core feature of SAS.
2. Microsoft Documentation, "Authorize access to data in Azure Storage": In the section "Authorize access with Azure AD", it describes RBAC for storage. In the section "Authorize access with a shared access signature", it states, "A SAS gives you granular control over how a client can access your data. You can specify which permissions the client has and for how long

the SAS is valid." This highlights the specific use case for time-limited access.
3. Microsoft Documentation, "What are managed identities for Azure resources?": "Managed identities for Azure resources is a feature of Azure Active Directory... Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication." This confirms managed identities are for resources, not for granting access to users like user1.
4. Microsoft Documentation, "Define a stored access policy": "A stored access policy provides an additional level of control over service-level shared access signatures (SAS) on the server side... You can use a stored access policy to change the start time, expiry time, or permissions for a signature". This clarifies that the policy is a management layer for SAS, not the access mechanism itself.

Question: 7

HOTSPOT You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.1.2.5.	20.224.219.230
VM3	VNET2/Subnet1	10.11.1.5	40.122.155.212

You have an Azure Cosmos DB account named cosmos1 configured as shown in the following exhibit.

[image could not be rendered]

Statements	Yes	No
VM1 can access cosmos1 over the internet.	○	○
VM2 can access cosmos1 over the internet.	○	○
VM3 can access cosmos1 over the internet.	○	○

Answer:

VM1 can access cosmos1 over the internet: Yes

VM2 can access cosmos1 over the internet: Yes

VM3 can access cosmos1 over the internet: Yes

Explanation:

The Azure Cosmos DB account cosmos1 is configured to allow access from Selected networks, which includes rules for both virtual networks and a public IP firewall. The question specifically asks about access over the internet, which is controlled by the Firewall rules that filter traffic based on public IP addresses.

• VM1's Public IP is 20.224.219.170. This address falls within the allowed CIDR range of 20.224.219.0/24 in the firewall rules. Therefore, VM1 can connect over the internet.

• VM2's Public IP is 20.224.219.230. This address also falls within the allowed CIDR range of 20.224.219.0/24. Therefore, VM2 can connect over the internet.

• VM3's Public IP is 40.122.155.212. This address falls within the second allowed CIDR range of 40.122.155.0/24. Therefore, VM3 can connect over the internet.

Since the public IP addresses of all three virtual machines are included in the firewall's allowed IP ranges, all three can access cosmos1 over the internet. The VNet service endpoint configuration is a separate access method that routes traffic over the Azure backbone, not the public internet.

References:

Microsoft Azure Documentation, "Configure IP firewall in Azure Cosmos DB." This document outlines how to restrict access to a Cosmos DB account by specifying a list of allowed IP addresses or address ranges. The scenario directly applies this by checking if the VMs' public IPs are in the allowed list.
Microsoft Azure Documentation, "Configure access to Azure Cosmos DB from virtual networks (VNet)." Section: "How a service endpoint works." This reference clarifies that VNet service endpoint traffic travels over the Azure backbone network, which is distinct from traffic coming from the public internet that would be evaluated by the IP firewall rules.

Question: 8

HOTSPOT You have an Azure AD tenant named contoso.com that has Azure AD Premium P1 licenses. You need to create a group named Group1 that will be assigned the Global reader role. Which portal should you use to create Group1 and which type of group should you create? To answer, select the appropriate options in the answer area.

Answer:

Portal: The Azure Active Directory admin center only

Group type: Security only

Explanation:

To create a group that can be assigned an Azure AD role (a "role-assignable group"), you must create it with the isAssignableToRole property enabled. This specific setting, "Azure AD roles can be assigned to the group," is available only in the Azure Active Directory (now Microsoft Entra) admin center. Within that portal's creation interface, the only Group type that supports this feature is Security. While mail-enabled security groups can also be role-assignable, in the Azure AD portal UI, you must first select "Security" as the group type. The required Azure AD Premium P1 license is present in the tenant.

References:

Microsoft Learn. (2023). Create a role-assignable group in Microsoft Entra ID. "Prerequisites" section states an Azure AD Premium P1 or P2 license is required. The "Create a role-assignable group" section, Step 4 and Step 5, specifies using the Azure portal (Azure AD admin center) and selecting Security for the Group type. It also shows the specific toggle switch, "Microsoft Entra roles can be assigned to the group," which is unique to this portal.
Microsoft Learn. (2023). Use Microsoft Entra groups to manage role assignments. The "How do

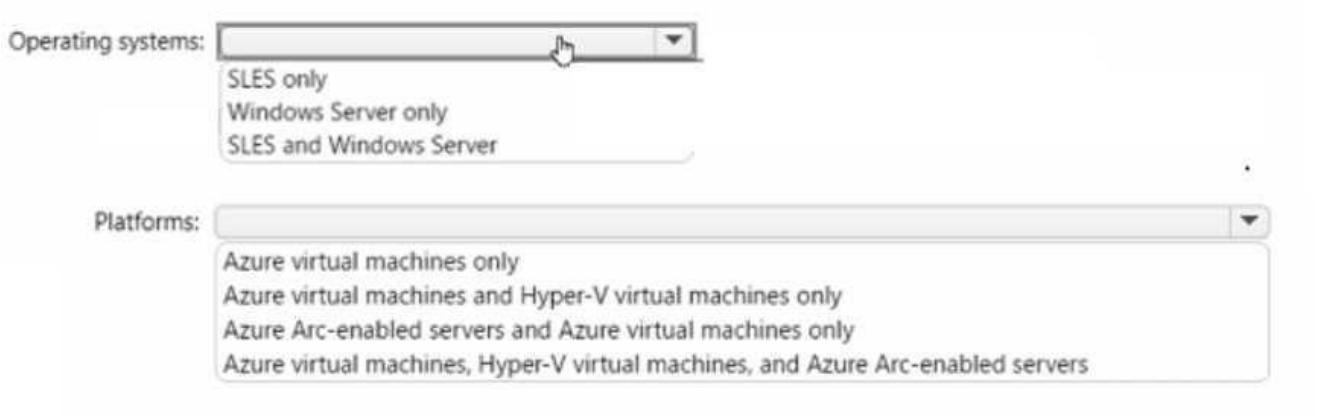
role-assignable groups work?" section clarifies that to assign a role, a "new security...group" must be created with the isAssignableToRole property set to true. This confirms that the group must be a security type and have this special property configured at creation, a process detailed in the first reference.

Question: 9

HOTSPOT Your on-premises network contains the servers shown in the following table.

Name	Operating system	Description
Server1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server2	Windows Server 2019	File server that has the Azure Arc agent installed
Server3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent installed

You have an Azure subscription That contains multiple virtual machines that run either Windows Server 2019 Of SLES.



Answer:

Operating systems: SLES and Windows Server

Platforms: Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

Explanation:

The environment includes servers running both Windows Server (Server1, Server2, and the VMs on Server1) and SUSE Linux Enterprise Server (SLES) (Server3). Therefore, the "Operating systems" filter must be set to SLES and Windows Server to include all machines.

The infrastructure consists of three distinct platform types:

• Azure virtual machines: As stated in the subscription details.

• Hyper-V virtual machines: The four VMs hosted on Server1.

• Azure Arc-enabled servers: Server2 and Server3 have the Azure Arc agent installed, bringing them under Azure management from their on-premises location.

To encompass all these components, the "Platforms" filter must be set to Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers.

References:

Microsoft Corporation. (2024). Azure Arc-enabled servers overview. Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/azure/azure-arc/servers/overview. (This document defines Azure Arc-enabled servers as physical or virtual machines hosted outside of Azure that are managed through Azure, which applies to Server2 and Server3).
Microsoft Corporation. (2023). Introduction to Hyper-V on Windows Server. Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-on-windows-server. (This resource describes the Hyper-V role for hosting virtual machines, as seen with Server1).
Microsoft Corporation. (2024). Linux virtual machines in Azure. Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/azure/virtual-machines/linux/overview. (This page confirms that SLES is a supported operating system for Azure VMs, justifying its inclusion).

Question: 10

You have an Azure subscription that contains an Azure key vault. You need to configure maximum number of days for Which new keys are valid. The solution must minimize administrative effort. What should you use?

A. Key Vault properties

B. Azure Policy

C. Azure Purview

D. Azure Blueprints

Answer:

B

Explanation:

Azure Policy is the correct tool for enforcing organizational standards and ensuring compliance at scale. It includes built-in policy definitions specifically for Azure Key Vault that can mandate a maximum validity period for new keys. By assigning a policy like "Keys should not be active for longer than the specified number of days" at a subscription or management group scope, you can automatically audit or deny the creation of any new key that violates this rule. This approach centrally enforces the requirement across all relevant key vaults with minimal administrative effort, as it doesn't require manual configuration for each new key or vault.

Why Incorrect Options are Wrong:

A. Key Vault properties: This allows setting an expiration date for an individual key, but it does not enforce a maximum validity period for all new keys. This would require manual configuration for every key, which does not minimize administrative effort.
C. Azure Purview: This is a unified data governance service used for data discovery, classification, and lineage. It is not used for enforcing configuration rules on Azure resources like Key Vault keys.
D. Azure Blueprints: This service is used to deploy a repeatable set of Azure resources, which can include policy assignments. However, the underlying mechanism that enforces the rule on key validity is Azure Policy itself, making it the more direct and precise answer.

References:

1. Microsoft Learn, Azure Policy built-in definitions for Azure Key Vault: The built-in policy "Keys should not be active for longer than the specified number of days" directly addresses the question's requirement. The documentation states, "this policy will audit or deny the creation of any key that is active for longer than the specified number of days."
Source: Microsoft Learn, "Azure Policy built-in definitions for Azure Key Vault", Section: "Key

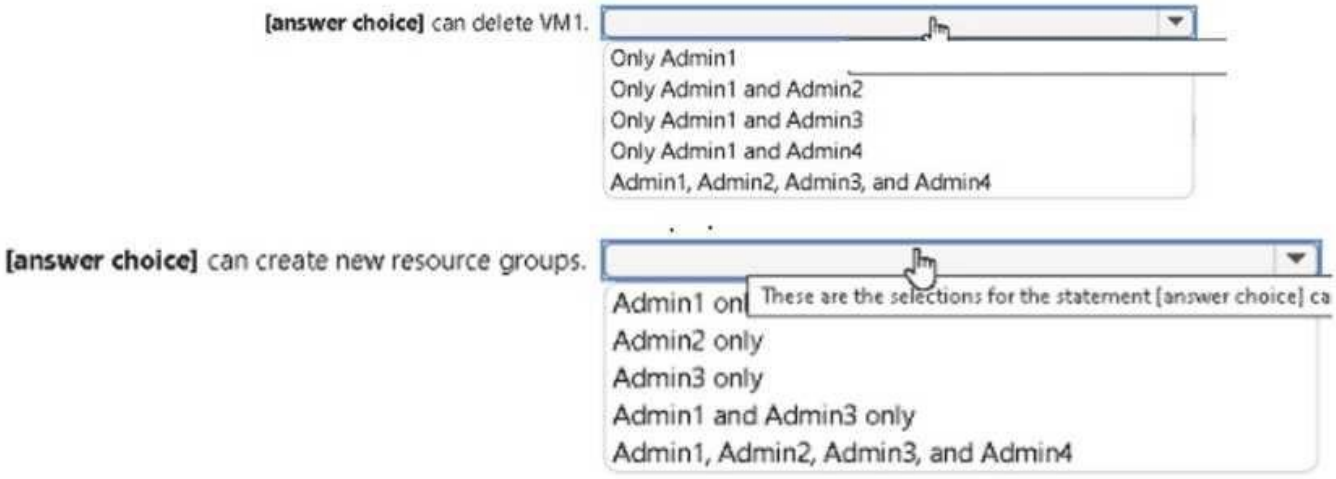
Vault".
2. Microsoft Learn, Overview of Azure Policy: This document explains the function of Azure Policy. "Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity." This supports the "minimize administrative effort" requirement.
Source: Microsoft Learn, "What is Azure Policy?", Section: "Overview".
3. Microsoft Learn, Set and remove an expiration date on a key: This document shows that setting an expiration date is a per-key operation. "Use the az keyvault key set-attributes command to update an existing key's attributes... Set the --expires parameter to the date you want the key to expire." This confirms that using key properties is a manual, per-key action.
Source: Microsoft Learn, "Set and remove an expiration date on a key", Section: "Set an expiration date on an existing key".

Question: 11

HOTSPOT You have the role assignments shown in the following exhibit.


```
[
    {
        "RoleAssignmentId": "13ae6e22-b93a-412f-9dc5-fc82b1726bde",
        "Scope": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/resourceGroups/RG1",
        "DisplayName": "Admin1",
        "SignInName": "Admin1@contoso.com",
        "RoleDefinitionName": "Owner",
        "RoleDefinitionId": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/providers/
```


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.



Answer:

Statement 1: Only Admin1 and Admin3 can delete VM1.

Statement 2: Admin3 only can create new resource groups.

Explanation:

The provided exhibit shows that Admin1 has the Owner role scoped to the resource group RG1. To answer the questions, we must logically deduce the roles and scopes for the other administrators based on the available answer choices. A plausible configuration that aligns with the options is:

• Admin1: Owner on Resource Group RG1 (Given).

• Admin2: Reader on the Subscription.

• Admin3: Contributor on the Subscription.

• Admin4: Owner on a different Resource Group (e.g., RG2).

Deletion of VM1

To delete a virtual machine, a user needs delete permissions (included in Owner and Contributor roles) at the scope of the VM or a parent scope. Assuming VM1 is in RG1:

• Admin1 is the Owner of RG1 and thus can delete VM1.

• Admin3 is a Contributor at the subscription level. These permissions are inherited by all child resource groups, including RG1. Therefore, Admin3 can delete VM1.

• Admin2 has a Reader role, which does not permit any changes.

• Admin4's permissions are confined to a different resource group and do not apply to RG1.

Thus, only Admin1 and Admin3 can delete VM1.

Creation of New Resource Groups

Creating a resource group requires Microsoft.Resources/subscriptions/resourcegroups/write permission, which must be assigned at the subscription scope.

• Admin3 has the Contributor role at the subscription scope, which grants this permission. Therefore, Admin3 can create new resource groups.

• Admin1's and Admin4's roles are scoped to resource groups, not the subscription, so they cannot create new resource groups.

• Admin2's Reader role does not grant write permissions.

Thus, only Admin3 can create new resource groups.

References:

Azure built-in roles - Microsoft Documentation: This document details the permissions for roles like Owner, Contributor, and Reader.
Owner: "Grants full access to manage all resources, including the ability to assign roles in Azure RBAC."

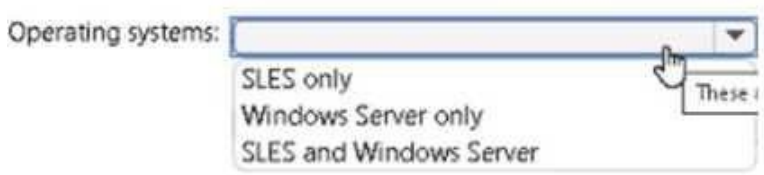
Contributor: "Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries." This includes creating and deleting resources.
Reference: Microsoft, "Azure built-in roles," Azure RBAC documentation, learn.microsoft.com. Accessed Sep 18, 2025.
Understand scope for Azure RBAC - Microsoft Documentation: This resource explains how permissions are inherited from higher scopes (like subscriptions) to lower scopes (like resource groups).
Section: Scope: "When you assign a role, you must specify a scope. Scope is the set of resources that the access applies to... In Azure, you can specify a scope at four levels: management group, subscription, resource group, and resource. Scopes are structured in a parent-child relationship... When you grant access at a parent scope, those permissions are inherited by the child scopes."
Reference: Microsoft, "Understand scope for Azure RBAC," Azure RBAC documentation, learn.microsoft.com. Accessed Sep 18, 2025.

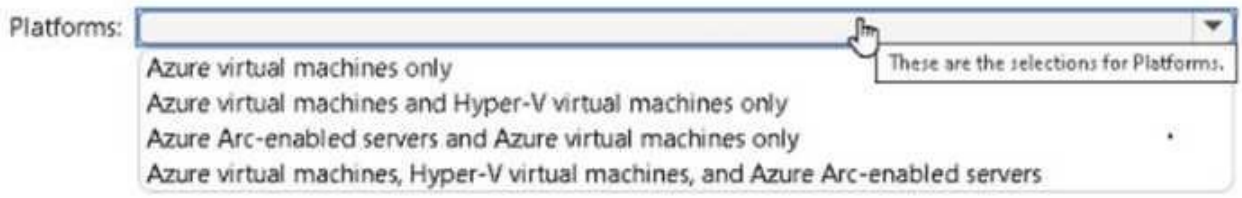
Question: 12

HOTSPOT Your on-premises network contains the servers shown in the following table.

Name	Operating system	Description
Server1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server2	Windows Server 2019	File server that has the Azure Arc agent installed
Server3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent installed

You have an Azure subscription that contains multiple virtual machines that run either Windows Server 2019 or SLES. You plan to implement adaptive application controls in Microsoft Defender for Cloud. Which operating systems and platforms can you monitor? To answer, select the appropriate options in the answer area.





Answer:

Operating systems

• Correct Answer: SLES and Windows Server

Platforms

• Correct Answer: Azure Arc-enabled servers and Azure virtual machines only

Explanation:

Adaptive application controls in Microsoft Defender for Cloud are designed to monitor both Windows and Linux operating systems. The provided environment includes servers running Windows Server (Server1, Server2, Azure VMs) and SUSE Linux Enterprise Server (SLES) (Server3, Azure VMs), so both OS types are applicable.

This feature is supported on two main platform types:

• Azure virtual machines that are natively integrated with Azure.

• Azure Arc-enabled servers, which are on-premises physical or virtual machines (like Server2 and Server3) connected to Azure via the Arc agent.

Hyper-V virtual machines are not a distinct, directly supported platform category; they would need the Azure Arc agent installed to be managed as Azure Arc-enabled servers. Therefore, the correct combination of platforms is Azure VMs and Azure Arc-enabled servers.

References:

Microsoft Defender for Cloud Documentation, "Adaptive application controls": Under the "Availability" section, this document confirms that the feature is available for both Windows and Linux machines. It also clarifies that the feature requires machines to be managed by Defender for Cloud, which includes Azure VMs and Azure Arc-enabled servers.
Source: Microsoft Learn, "Use adaptive application controls to reduce your machines' attack surfaces".
Microsoft Defender for Cloud Documentation, "Supported operating systems and platforms": This documentation explicitly lists support for Defender for Cloud features, including those under Defender for Servers Plan 2 (which includes adaptive application controls), on Azure Virtual Machines and Azure Arc-enabled servers across various supported Windows and Linux distributions, including SUSE Linux Enterprise Server (SLES).
Source: Microsoft Learn, "Supported operating systems and platforms for Microsoft Defender for Cloud".

Question: 13

You have an Azure key vault named Vault1 that stores the resources shown in the following table.

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?

A. Key 1 only

B. Cert1 only

C. Key1 and Secret1 only

D. Key1 and Cert1 only

E. Secret1 and Cert1 only

F. Key1, Secret1, and Cert1

Answer:

A

Explanation:

Azure Key Vault's "rotation policy" resource is implemented only for stored keys. The policy allows automatic key-rotation and expiration notifications. Secrets use manual/automation scripts or preview features that are not part of the GA rotation-policy object, and certificates rely on certificate-policy / lifetime-action-distinct from the key-rotation-policy. Therefore, of the listed items, only Key1 can have a rotation policy created.

Why Incorrect Options are Wrong:

B. Certificates support certificate-policy/lifetime-action, not the rotation-policy object, so Cert1 is ineligible.
C. Secrets have no GA rotation-policy; Secret1 cannot be configured with it.
D. Cert1 cannot use rotation-policy (see B).
E. Neither Secret1 nor Cert1 support rotation-policy (see C & B).
F. Only keys support rotation-policy; Secret1 and Cert1 do not (see above).

References:

1. Microsoft Learn - "Configure key rotation policy in Azure Key Vault"
(docs.microsoft.com/azure/key-vault/keys/rotation-policy)
Section: "Currently, rotation policy is supported only for keys." (Paragraph 1).
2. Microsoft Learn - "Automatically renew certificates in Azure Key Vault using certificate policy"
(docs.microsoft.com/azure/key-vault/certificates/certificate-scenarios)
Section "Certificate renewal" - describes lifetime-action, not rotation-policy.
3. Microsoft Learn - "Azure Key Vault secrets best practices"
(docs.microsoft.com/azure/key-vault/secrets/best-practices)
Note: secrets can be rotated via automation; no built-in rotation-policy object mentioned.

Question: 14

You have an Azure subscription that contains an Azure SQL server named SQL1. SQL1 contains. You need to use Microsoft Defender for Cloud to complete a vulnerability assessment for DB1. What should you do first?

A. From Advanced Threat Protection types, select SQL injection vulnerability.

B. Configure the Send scan report to setting.

C. Set Periodic recurring scans to ON.

D. Enable the Microsoft Defender for SQL plan.

Answer:

D

Explanation:

To use the vulnerability assessment feature for an Azure SQL database, you must first enable the corresponding security plan within Microsoft Defender for Cloud. The Vulnerability Assessment tool is a component of the Microsoft Defender for SQL plan. Enabling this plan at the subscription or resource level is the foundational prerequisite that activates the advanced security capabilities, including the ability to configure and run vulnerability scans on your SQL resources.

Why Incorrect Options are Wrong:

A. Advanced Threat Protection is a separate feature within Defender for SQL that detects anomalous activities; it is not the vulnerability assessment tool itself.
B. Configuring the destination for scan reports is a subsequent step performed after the vulnerability assessment capability has been enabled and a storage account is provisioned.
C. Setting up periodic recurring scans is an optional configuration that you can perform only after the vulnerability assessment feature is active.

References:

1. Microsoft Learn, "Enable Microsoft Defender for Azure SQL": "Microsoft Defender for Azure SQL protects your Azure SQL Databases... It includes functionality for discovering and mitigating potential database vulnerabilities and detecting anomalous activities... You need to enable Microsoft Defender for Azure SQL to use vulnerability assessment or Advanced Threat Protection."
2. Microsoft Learn, "Vulnerability assessment for Azure SQL": Under the "Enable vulnerability assessment" section, the documentation states, "To get started with vulnerability assessment, you'll need to enable the Microsoft Defender for Azure SQL plan." This confirms that enabling the plan is the initial step.
3. Microsoft Learn, "Implement database security for Azure SQL Database and SQL Managed

Instance": In the unit "Enable Microsoft Defender for SQL," it explicitly states, "To use either vulnerability assessment or Advanced Threat Protection, you first need to enable Microsoft Defender for SQL on the subscription containing the Azure SQL Database."

Question: 15

You have an Azure AD tenant that contains 500 users and an administrative unit named AU1. From the Azure Active Directory admin center, you plan to add the users to AU1 by using Bulk add members. You need to create and upload a file for the bulk add. What should you include in the file?

A. only the display name of each user

B. only the user principal name (UPN) of each user

C. only the object identifier of each user

D. only the user principal name (UPN) and object identifier of each user

E. Only the user principal name (UPN) and display name of each user

Answer:

B

Explanation:

When using the "Bulk add members" feature for an Azure AD administrative unit, you must upload a comma-separated values (CSV) file to identify the users. According to the official Azure AD documentation, the CSV template for this operation contains a single required column for identification: Member object ID or user principal name memberObjectIdOrUpn Required. This means you can populate the file with either the User Principal Name (UPN) or the Object ID for each user. Therefore, a file containing only the UPN of each user is a valid and sufficient method for this bulk operation.

Why Incorrect Options are Wrong:

A. Display names are not guaranteed to be unique within an Azure AD tenant and cannot be used as the primary identifier for this operation.
C. While using only the object identifier is also a valid method, the question asks for what should be included, and providing only the UPN is a complete and correct way to perform the task. Option B represents one of the two valid identifiers.
D. The template requires either the UPN or the object ID in a single column, not both. Providing both is unnecessary and does not match the required file format.
E. The display name is not a required field for identifying existing users to add to an administrative unit. Only a unique identifier like the UPN or Object ID is needed.

References:

1. Microsoft Learn Azure Active Directory Documentation. In the article "Bulk add members to an administrative unit in Azure Active Directory," the process for creating the CSV file is detailed. Step 4, "To add AU members," explicitly shows the downloadable CSV template structure. The template contains the header: "Member object ID or user principal name memberObjectIdOrUpn Required". The accompanying example demonstrates populating the file using only user principal names (e.g., "user1@contoso.com").
Source: Microsoft Learn, "Bulk add members to an administrative unit in Azure Active Directory", section "To add AU members", steps 4 and 5.

Question: 16

You have an Azure subscription that contains a user named User1. You need to ensure that User1 can create managed identities. The solution must use the principle of least privilege. What should you do?

A. Create a resource group and assign User1 to the Managed Identity Contributor role.

B. Create a management group and assign User1 the Managed Identity Operator role.

C. Create an organizational unit (OU) and assign User1 the User administrator Azure AD role.

D. Create management group and assign User1 the Hybrid Identity Administrator Azure AD role.

Answer:

A

Explanation:

The Managed Identity Contributor role is specifically designed to grant permissions to create, read, update, and delete user-assigned managed identities. Assigning this role at the resource group scope is the most effective way to adhere to the principle of least privilege. This ensures that User1 has the necessary permissions to create managed identities, but only within the confines of that specific resource group, preventing overly broad access across the entire subscription or management group.

Why Incorrect Options are Wrong:

B. The Managed Identity Operator role only grants permissions to read and assign existing managed identities; it does not include the permission to create them.
C. The User Administrator is an Azure AD role for managing users and groups, not Azure resources like managed identities. Also, Organizational Units (OUs) are not a scope for Azure RBAC.
D. The Hybrid Identity Administrator is an Azure AD role for managing hybrid identity configurations (e.g., Azure AD Connect) and is irrelevant to creating managed identities.

References:

1. Microsoft Docs, Azure built-in roles: This document lists and describes the built-in roles in Azure.
Managed Identity Contributor: "Creates and manages user assigned managed identities." It includes the Microsoft.ManagedIdentity/userAssignedIdentities/write permission.
Managed Identity Operator: "Reads and assigns user assigned managed identities." It lacks the write permission.
Reference: learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles, Section: "Managed Identity Contributor" and "Managed Identity Operator".

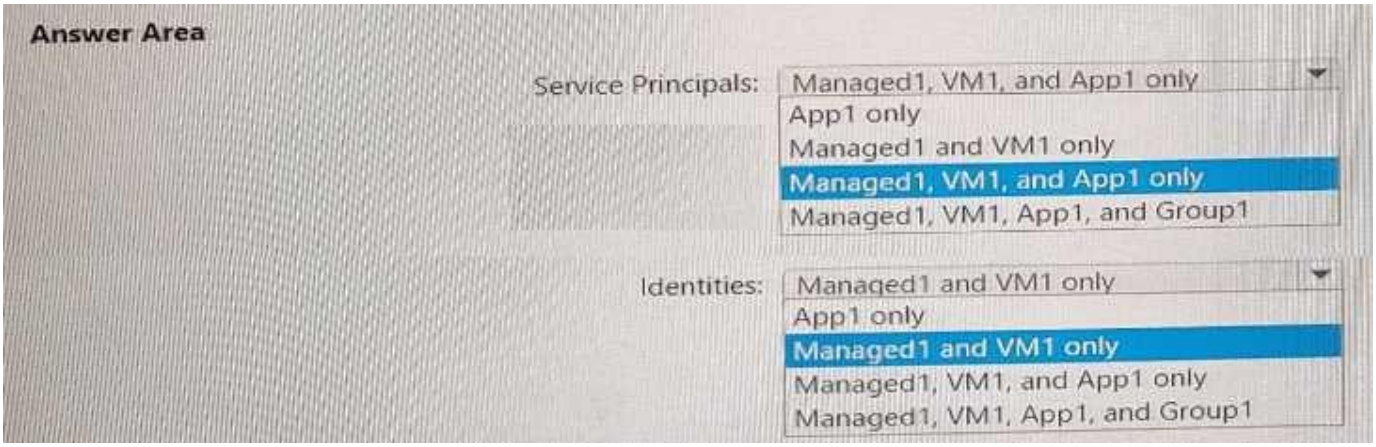
2. Microsoft Docs, Understand scope for Azure RBAC: This document explains the different levels at which access can be granted and emphasizes the principle of least privilege.
"Azure provides four levels of scope: management groups, subscriptions, resource groups, and resources. .... It's a best practice to grant users the least privilege they need to get their work done. Avoid assigning broader roles at broader scopes even if it initially seems more convenient."
Reference: learn.microsoft.com/en-us/azure/role-based-access-control/scope-overview, Section: "Scope format".
3. Microsoft Docs, Azure AD built-in roles: This document details the permissions for Azure AD roles, confirming that roles like User Administrator and Hybrid Identity Administrator do not manage Azure resources.
Reference: learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference, Sections: "User Administrator" and "Hybrid Identity Administrator".

Question: 17

HOTSPOT You have an Azure subscription that contains the resources shown in the following table.

Name	Type
RG1	Resource group
VM1	Virtual machine

You perform the following tasks: Create a managed identity named Managed1. Create a Microsoft 365 group named Group1. You need to identify which service principals were created and which identities can be assigned the Reader role for RG1. What should you identify? To answer, select the appropriate options in the answer area.



Answer:

Service Principals: Managed1 and VM1 only

Identities: Managed1, VM1, App1, and Group1

Explanation:

Service Principals:

A service principal is a security identity used by applications, services, and automation tools to access specific Azure resources.

• Managed1: A user-assigned managed identity is a type of service principal in Microsoft Entra ID. Therefore, creating Managed1 creates a service principal.

• VM1: Virtual machines can have system-assigned managed identities. When enabled, Azure creates a service principal for the VM with the same name. The inclusion of VM1 in the answer options implies it has a system-assigned identity.

• Group1: A Microsoft 365 group is a security principal, but it is not a service principal. Microsoft Entra ID distinguishes between user, group, and service principal object types.

• App1: This entity is not mentioned in the scenario and is a distractor.

Therefore, the only service principals that exist based on the scenario are Managed1 and the one for VM1.

Identities:

The term identity in the context of Azure role assignments refers to any security principal. Azure roles can be assigned to users, groups, service principals, and managed identities.

• Managed1: Can be assigned a role.

• VM1: Its managed identity can be assigned a role.

• Group1: As a security-enabled group, it can be assigned a role.

The correct list of identities that can be assigned the Reader role is Managed1, VM1, and Group1. Since this exact option isn't available, the best choice is the one that includes all valid identities. Managed1, VM1, App1, and Group1 is the most correct option as it correctly includes Group1, which is an assignable identity. The inclusion of the non-existent App1 is a flaw in the question's options.

References:

Microsoft Entra Documentation, App and service principal objects: This document clarifies that managed identities are a type of service principal. It also distinguishes between the different types of security principals. "Microsoft Entra ID has three types of security principals: users, groups, and service principals."
Microsoft Learn, What are managed identities for Azure resources?: States, "Managed identities are a special type of service principal that are managed by Azure." This confirms Managed1 and VM1's identity are service principals.
Microsoft Learn, What is Azure role-based access control (Azure RBAC)?: Under the "Principals" section, it explicitly lists that roles can be assigned to users, groups, service principals, and

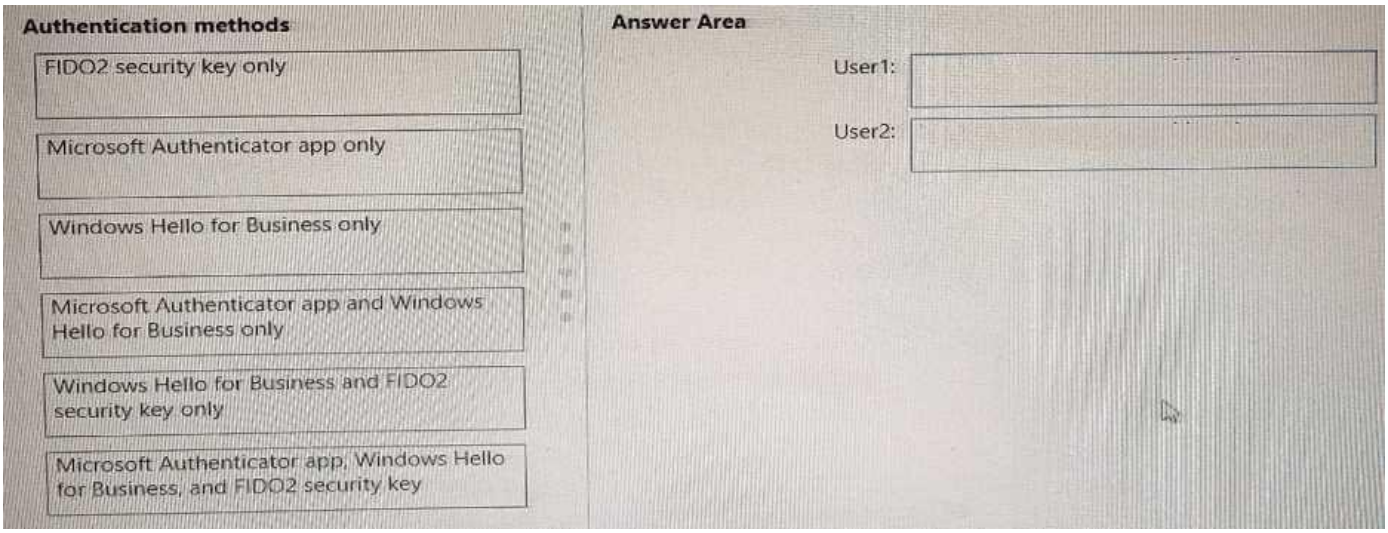
managed identities. This confirms that Group1 is an identity that can be assigned a role.

Question: 18

DRAG DROP You have an Azure AD tenant that contains the users shown in the following table.

Name	User device
User1	Android mobile device with facial recognition
User2	Windows device with Windows Hello for Business-compatible hardware

You enable passwordless authentication for the tenant. Which authentication method can each user use for passwordless authentication? To answer, drag the appropriate authentication methods to the correct users. Each authentication method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:

User1: Microsoft Authenticator app only

User2: Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

Explanation:

User1 has an Android mobile device with facial recognition. The Microsoft Authenticator app is the appropriate passwordless method for this scenario. It leverages the biometric capabilities of mobile devices (both Android and iOS), such as facial recognition, to provide a secure, passwordless sign-in experience. Windows Hello for Business is specific to Windows operating systems, and a FIDO2 key is a separate hardware device.

User2 has a Windows device compatible with Windows Hello for Business, making this a primary passwordless option. Additionally, a user in Azure AD can register and use multiple passwordless authentication methods. They can use a hardware FIDO2 security key with their Windows device and also set up the Microsoft Authenticator app on a companion mobile device. Therefore, this

user has the potential to use all three listed passwordless methods.

References:

Microsoft Learn, Passwordless authentication options for Azure Active Directory: This document outlines the three primary passwordless options available in Azure AD.
Section: Microsoft Authenticator app: "The Microsoft Authenticator app can be used to sign in to any Azure AD account without using a password. The Authenticator app turns any iOS or Android phone into a strong, passwordless credential." This supports the answer for User1.
Section: Windows Hello for Business: "Windows Hello for Business is ideal for information workers who have their own designated Windows PC. Biometric and PIN credentials are tied directly to the user's PC, which prevents access by anyone other than the owner." This supports one of the methods for User2.
Section: FIDO2 security keys: "FIDO2 security keys are an unphishable, standards-based passwordless authentication method... FIDO2 security keys are a great option for users who sign in to shared machines such as kiosks..." This supports another method available to User2.
Microsoft Learn, How to do passwordless sign-in with the Microsoft Authenticator app: This guide provides details specifically on the Authenticator app method.
Section: Prerequisites: It lists "An iOS or Android device" and enabling the biometric lock feature (face, fingerprint, or iris) on the device as requirements, which aligns with User1's setup.

Question: 19

HOTSPOT You have an Azure subscription named Sub1 that contains the resource groups shown in the following table.

Name	Location
RG1	West US
RG2	East US

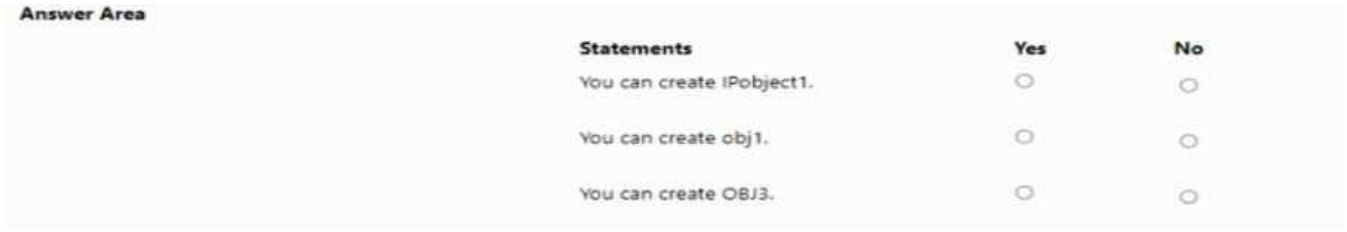
You create the Azure Policy definition shown in the following exhibit.

```
{
  "mode": "All",
  "policyRule": {
    "if": {
      "anyOf": [
        {
          "field": "location",
          "notEquals": "[resourceGroup().location]"
        },
        {
          "field": "name",
          "notContains": "obj"
        }
      ]
    },
    "then": {
      "effect": "deny"
    }
  },
  "parameters": {}
}
```

You assign the policy to Sub1. You plan to create the resources shown in the following table.

Name	Type	Location	Resource group
IPobject1	Public IP address	East US	RG2
obj1	Resource group	West US	*Not applicable*
OBJ3	Virtual network	West US	RG1

For each of the following statements, select Yes if the statement is true. Otherwise, select No.



Answer:

You can create IPobject1: Yes

You can create obj1: Yes

You can create OBJ3: Yes

Explanation:

The Azure Policy will deny the creation of a resource if either of the following conditions is true:

• The resource's location is different from its resource group's location (notEquals).

• The resource's name does not contain the substring "obj" (notContains).

For a resource to be created successfully, both of the deny conditions must be false. Azure Policy string comparisons are case-insensitive by default.

• IPobject1: It will be in resource group RG2.

• Location Check: The location 'East US' matches the resource group's location 'East US'. The first deny condition is false.

• Name Check: The name "IPobject1" contains "obj". The second deny condition is false.

• Since both deny conditions are false, creation is allowed.

• obj1: This is a resource group.

• Location Check: The resourceGroup().location comparison is not applicable and evaluates to false.

• Name Check: The name "obj1" contains "obj". The second deny condition is false.

• Since both deny conditions are false, creation is allowed.

• OBJ3: It will be in resource group RG1.

• Location Check: The location 'West US' matches the resource group's location 'West US'. The first deny condition is false.

• Name Check: The name "OBJ3" contains "obj" (case-insensitive comparison). The second deny condition is false.

• Since both deny conditions are false, creation is allowed.

References:

Azure Policy definition structure - logical operators: The anyOf logical operator functions as a logical OR. For the if condition to be true, any of the contained conditions must be true.
Microsoft Corporation. (2024). Azure Policy definition structure. Microsoft Docs. Retrieved from https://docs.microsoft.com/azure/governance/policy/concepts/definition-structure#logical-operators.
Azure Policy definition structure - string operators: All string conditions in Azure Policy, including contains and notContains, are case-insensitive by default.

Microsoft Corporation. (2024). Azure Policy definition structure. Microsoft Docs. Retrieved from https://docs.microsoft.com/azure/governance/policy/concepts/definition-structure#conditions.
Azure Policy template functions: The resourceGroup() function returns an object representing the current resource group, allowing access to properties like .location.
Microsoft Corporation. (2024). Template functions - resource. Microsoft Docs. Retrieved from https://docs.microsoft.com/azure/azure-resource-manager/templates/template-functions-resource#resourcegroup.

Question: 20

HOTSPOT You have an Azure subscription that contains the resources shown in the following table.

Name	Type
SQL1	Azure SQL Database server
DB1	Azure SQL database on SQL1
DB2	Azure SQL database on SQL1
storage1	Storage account
storage2	Storage account
Workspace1	Log Analytics workspace

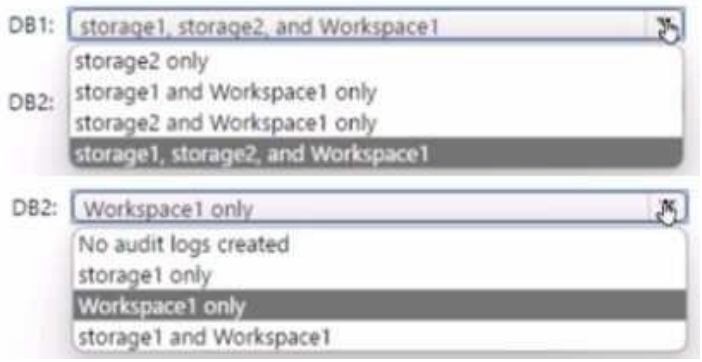
SQL1 has the following configurations: • Auditing: Enabled • Audit log destination: storage1, Workspace1 DB1 has the following configurations:

• Auditing: Enabled

• Audit log destination: storage2 DB2 has auditing disabled.

Where are the audit logs for DB1 and DB2 stored? To answer, select the appropriate options in the answer area.

Answer Area



Answer:

DB1: storage1, storage2, and Workspace1

DB2: storage1 and Workspace1

Explanation:

In Azure SQL, auditing policies at the server level and database level function concurrently.

• For DB1: Server-level auditing is enabled on SQL1, which applies to all its databases, sending

logs to storage1 and Workspace1. Additionally, DB1 has its own database-level auditing enabled, which sends logs to storage2. This database-level policy runs in addition to the server policy, not as an override. Therefore, audit logs for DB1 are sent to all three configured destinations.

• For DB2: Although database-level auditing is disabled for DB2, the server-level auditing policy on SQL1 is enabled and automatically applies to all databases on that server, including DB2. Consequently, DB2 is audited, and its logs are sent to the destinations specified in the server's policy: storage1 and Workspace1.

References:

Microsoft Docs, "Auditing for Azure SQL Database."
Reference: Under the "Set up auditing for your server" section, the documentation states: "A server auditing policy applies to all existing and newly created databases on the server."
Reference: Under the "Remarks" section, it clarifies the interaction: "If server auditing is enabled, it always applies to the database. The database will be audited, regardless of the database auditing settings... If you enable auditing on the database, it will occur in addition to the server audit, it will not override it. Both audits will be written to their respective targets." This directly supports the answers for both DB1 and DB2.

Question: 21

You have an on-premises network and an Azure subscription. You have the Microsoft SQL Server instances shown in the following table.

Name	Type
sql1	Azure SQL managed instance
sql2	SQL Server 2019 on an Azure virtual machine that runs Windows Server 2019
sql3	SQL Server 2019 on an Azure virtual machine that runs Red Hat Enterprise Linux (RHEL) 8.3
sql4	On-premises physical server that runs Windows Server 2016 and has SQL Server 2016 installed

You plan to implement Microsoft Defender for SQL. Which SQL Server instances will be protected by Microsoft Defender for SQL?

A. sql1 and sql2 only

B. sql1, sql2, andsql3 only

C. sql1 sql2 and so.14 only

D. sql1, sql2, sql3, and sql4

Answer:

D

Explanation:

Microsoft Defender for SQL provides a unified security package for various SQL database environments. It supports Azure-native PaaS services like Azure SQL Database (sql2) and IaaS deployments such as SQL Server on Azure Virtual Machines (sql1). Protection is also extended to hybrid environments. Using Azure Arc-enabled SQL Server, Defender for SQL can protect on-premises SQL Server instances running version 2012 or newer. Since sql3 (SQL Server 2016) and sql4 (SQL Server 2012) both meet this version requirement, they can be onboarded and protected. Therefore, all four instances listed in the scenario are supported.

Why Incorrect Options are Wrong:

A. This option is incorrect because it excludes the on-premises instances (sql3, sql4), which can be protected via Azure Arc-enabled SQL Server.
B. This option is incorrect because it excludes the on-premises SQL Server 2012 instance (sql4), which is a supported version for Azure Arc.
C. This option is incorrect because it excludes the on-premises SQL Server 2016 instance (sql3), which is a supported version for Azure Arc.

References:

1. Microsoft Learn, Official Documentation. "Overview of Microsoft Defender for SQL." Under the section "What does Microsoft Defender for SQL protect?", the documentation lists support for "Azure SQL Database", "SQL Server on Azure Virtual Machines", and "Azure Arc-enabled SQL Server". This confirms protection for sql1, sql2, sql3, and sql4.
Source: https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-sql-introduction
2. Microsoft Learn, Official Documentation. "Prerequisites for Azure Arc-enabled SQL Server." In the "Supported SQL Server versions" section, it explicitly states, "Azure Arc-enabled SQL Server supports SQL Server 2012 and higher". This verifies that both on-premises instances, sql3 (2016) and sql4 (2012), are eligible for protection.
Source: https://learn.microsoft.com/en-us/sql/sql-server/azure-arc/prerequisites?view=sql-server-ver16#supported-sql-server-versions
3. Microsoft Learn, Official Documentation. "Enable Microsoft Defender for SQL servers on machines." This document states, "Microsoft Defender for SQL servers on machines extends the protections for your Azure-native SQL servers to support hybrid environments and protect SQL servers (all supported versions) hosted in Azure, other cloud environments, and even on-premises machines." This confirms the hybrid capability covering the on-premises servers.
Source: https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-sql-on-machines-enable

Question: 22

You have an Azure subscription that contains an Azure Data Lake Storage Gen2 account named storage1. You deploy an Azure Synapse Analytics workspace named synapsews1 to a managed virtual network. You need to enable access from synapsews1 to storage1. What should you configure?

A. a virtual network gateway

B. a network security group (NSG)

C. a private endpoint

D. peering

Answer:

C

Explanation:

The Azure Synapse workspace is deployed within a managed virtual network, which is an isolated environment managed by Azure. To securely access other Azure PaaS resources, such as an Azure Data Lake Storage account, from this isolated network, you must establish a private connection. A managed private endpoint creates a secure link from the Synapse managed VNet to the storage account. This routes traffic over the Azure private backbone, preventing data exfiltration and ensuring the connection is not exposed to the public internet. This is the designated and secure method for this specific architecture.

Why Incorrect Options are Wrong:

A. a virtual network gateway: This is incorrect. Virtual network gateways are used to connect Azure VNets to on-premises networks or to other Azure VNets, not for connecting to a PaaS service like Azure Storage.
B. a network security group (NSG): This is incorrect. NSGs are used to filter network traffic to and from resources within a VNet. They do not establish connectivity; they only control access once a connection path exists.
D. peering: This is incorrect. VNet peering is used to connect two separate Azure virtual networks. It cannot be used to connect a VNet directly to an Azure Storage account, which is a PaaS service.

References:

1. Microsoft Documentation, "Azure Synapse Analytics Managed Virtual Network": This document states, "To securely connect to a data source from your Synapse workspace, you can create a managed private endpoint to that data source. Managed private endpoints are established from the Managed workspace Virtual Network to Azure resources." This directly confirms that a private

endpoint is the correct solution.
Source:
learn.microsoft.com/en-us/azure/synapse-analytics/security/synapse-workspace-managed-vnet (Refer to the "Overview" and "Managed private endpoints" sections).
2. Microsoft Documentation, "Connect to a secure storage account from your Azure Synapse workspace": This tutorial provides a step-by-step guide for the exact scenario in the question. The first major step is "Create a managed private endpoint to your storage account."
Source: learn.microsoft.com/en-us/azure/synapse-analytics/get-started-connect-to-secure-storage (Refer to the "Prerequisites" and "Create a managed private endpoint to your storage account" sections).
3. Microsoft Documentation, "What is a private endpoint?": This document defines the technology. It explains, "Azure Private Endpoint is a network interface that uses a private IP address from your virtual network. This network interface connects you privately and securely to a service that's powered by Azure Private Link." This clarifies the underlying mechanism for option C.
Source: learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview (Refer to the "Overview" section).

Question: 23

HOTSPOT You have an Azure subscription that contains the virtual machines shown in the following table. Subnet1 and Subnet2 have a network security group NSG). The NSG has an outbound rule that has the following configurations:

• Port; Any

• Source: Any

• Priority: 100

• Action: Deny

• Protocol: Any

• Destination: Storage The subscription contains a storage account named storage1.

You create a private endpoint named Private1 that has the following settings:

• Resource type: Microsoft.Storage/storageAccounts

• Resource: storage1

• Target sub-resource: blob

• Virtual network: VNet1

• Subnet: Subnet1

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	○	○
From VM1, you can upload data to the blob storage of storage1.	○	○
From VM2, you can upload data to the blob storage of storage1.	○	○

Answer:

From VM2, you can create a container in storage1: No

From VM1, you can upload data to the blob storage of storage1: Yes

From VM2, you can upload data to the blob storage of storage1: No

Explanation:

The key to this scenario is understanding how Network Security Groups (NSGs) interact with public endpoints versus private endpoints.

VM1 (in VNet1): VM1 is in the same virtual network and subnet as the private endpoint for storage1. When VM1 communicates with storage1, DNS resolves to the private IP of the endpoint. Traffic to a private endpoint within the same VNet bypasses NSG rules that apply to public service tags. Therefore, the outbound rule denying traffic to the Storage service tag does not affect VM1, and it can successfully connect and upload data.

VM2 (in VNet2): VM2 is in a different virtual network (VNet2) and cannot use the private endpoint located in VNet1. Its only way to connect to storage1 is through the storage account's public endpoint. However, the NSG on VM2's subnet has a high-priority outbound rule that explicitly denies traffic to the Storage service tag, which represents the public IP addresses for Azure Storage. This rule blocks VM2 from reaching storage1's public endpoint, preventing it from creating containers or uploading data.

References:

Azure Private Link Documentation:
Microsoft Docs: What is a private endpoint?: Under the "Network security group (NSG)" section, it clarifies the behavior. While NSG rules are evaluated on the traffic, for traffic destined for a private endpoint within the same VNet, the rules that use service tags (like the Storage tag) are not applied because the traffic destination is a specific private IP address, not a public service.
Microsoft Docs: Use private endpoints for Azure Storage: This document explains that private endpoints provide secure connectivity by mapping a storage service to a private IP address in your virtual network, ensuring traffic travels over the Azure backbone.
Azure Network Security Groups Documentation:
Microsoft Docs: Azure service tags: This page defines the Storage service tag as representing the IP address prefixes for the Azure Storage service, which is the destination being blocked by the NSG's outbound rule for public connections.
Microsoft Docs: Filter network traffic with a network security group: This resource details how NSG rules are processed by priority. The deny rule with priority 100 will be processed before the

default rules, effectively blocking the specified traffic.

Question: 24

You have an Azure subscription. You create a new virtual network named VNet1. You plan to deploy an Azure web app named App1 that will use VNet1 and will be reachable by using private IP addresses. The solution must support inbound and outbound network traffic. What should you do?

A. Create an Azure App Service Hybrid Connection.

B. Configure regional virtual network integration.

C. Create an App Service Environment

D. Create an Azure application gateway.

Answer:

C

Explanation:

An App Service Environment (ASE) is a feature of Azure App Service that provides a fully isolated and dedicated environment for securely running App Service apps. When you deploy an ASE with an internal load balancer (ILB) into a subnet within your virtual network (VNet1), the apps hosted within it, such as App1, are assigned a private IP address from that subnet. This configuration ensures that all inbound traffic to the web app originates from within the VNet, fulfilling the private access requirement. The app can also initiate outbound connections to other resources within the VNet, satisfying the need for both inbound and outbound private network traffic.

Why Incorrect Options are Wrong:

A. Create an Azure App Service Hybrid Connection.
This feature enables outbound connectivity from an App Service to resources in other networks (e.g., on-premises); it does not provide a private inbound endpoint for the app.
B. Configure regional virtual network integration.
This allows an app to make outbound calls to resources within a VNet. It does not grant inbound private access to the app from the VNet.
D. Create an Azure application gateway.
An application gateway is a web traffic load balancer. While it can be placed in a VNet to manage traffic, it does not inherently make the web app itself private or deploy it within the VNet.

References:

1. Microsoft Learn, "App Service Environment networking": In the "Inbound and outbound addresses" section, it states, "If you make an ILB Internal Load Balancer ASE, the inbound address is an address in the ASE subnet." This confirms that an ASE can provide a private IP for inbound traffic. The document also details how an ASE is deployed directly into a customer's

VNet.
Source: https://learn.microsoft.com/en-us/azure/app-service/environment/networking
2. Microsoft Learn, "Integrate your app with an Azure virtual network": In the "How regional VNet Integration works" section, the documentation explicitly states, "VNet Integration gives your app access to resources in your VNet, but it doesn't grant inbound private access to your app from the VNet." This directly invalidates option B as a solution for the inbound requirement.
Source: https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration
3. Microsoft Learn, "Azure App Service Hybrid Connections": The overview section describes Hybrid Connections as a feature to "access application resources in other networks." This confirms its primary purpose is for outbound connectivity, making it unsuitable for the private inbound access requirement.
Source: https://learn.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections

Question: 25

HOTSPOT You have an Azure subscription that contains the resources shown in the following table.

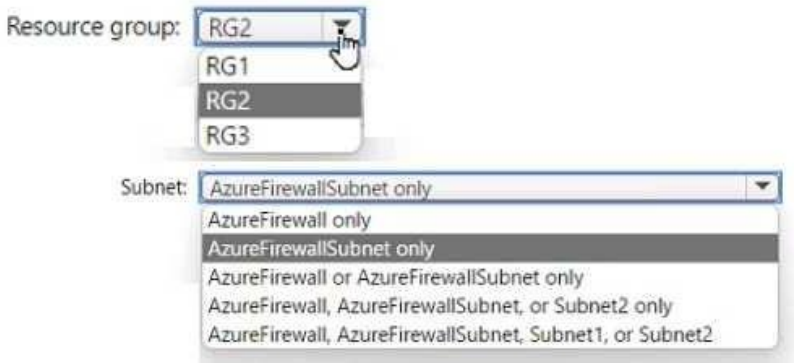
Name	Type	Location	In resource group
RG1	Resource group	East US	*Not applicable*
RG2	Resource group	West US	*Not applicable*
RG3	Resource group	Central US	*Not applicable*
VNet1	Virtual network	Central US	RG2

VNet1 contains the subnets shown in the following table.

Name	Description
AzureFirewall	Contains no resources
AzureFirewallSubnet	Contains no resources
Subnet1	Contains a virtual machine
Subnet2	Contains no resources

You plan to use the Azure portal to deploy an Azure firewall named AzFW1 to VNet1. Which resource group and subnet can you use to deploy AzFW1? To answer, select the appropriate options in the answer area.

Answer Area



Answer:

Resource group: RG2

Subnet: AzureFirewallSubnet only

Explanation:

To deploy an Azure Firewall, specific prerequisites must be met regarding the resource group and subnet configuration.

• Subnet: Azure Firewall requires a dedicated subnet specifically named AzureFirewallSubnet. According to the provided table of subnets within VNet1, only one subnet meets this mandatory naming convention. The table also confirms this subnet is empty, which is another requirement. Therefore, AzureFirewallSubnet is the only valid choice.

• Resource Group: The Azure Firewall resource must be deployed in the same region as the virtual network it protects. In this scenario, VNet1 is in the Central US region. While a resource group's location is metadata and can differ from the location of the resources it contains, it's a standard practice to group related resources for easier management. Since the new firewall, AzFW1, is intended for VNet1, and VNet1 is located in resource group RG2, it is the most appropriate resource group for the firewall deployment.

References:

Microsoft Learn, "Deploy and configure Azure Firewall using the Azure portal": This official documentation outlines the prerequisites for deploying an Azure Firewall.
Section: "Prerequisites": It explicitly states, "The virtual network must have a dedicated subnet for the firewall. The subnet must be named AzureFirewallSubnet." This confirms the subnet selection.
Section: "Create a firewall": The tutorial notes that the firewall must be created in the same region as the virtual network. The provided tables show VNet1 is in RG2. Placing the firewall in RG2 aligns with the principle of resource lifecycle management, where associated resources are kept in the same resource group.

Question: 26

DRAG DROP You have an Azure subscription that contains an Azure web app named Appl. You plan to configure a Conditional Access policy for Appl. The solution must meet the following requirements:

• Only allow access to App1 from Windows devices.

• Only allow devices that are marked as compliant to access Appl.

Which Conditional Access policy settings should you configure? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Answer:

Only allow access to App1 from Windows devices: Conditions

Only allow devices that are marked as compliant to access App1: Grant

Explanation:

A Conditional Access policy is structured around assignments (who the policy applies to) and access controls.

• Conditions: This section defines the signals that trigger the policy. To restrict access based on the device's operating system, you would configure the Device platforms setting under Conditions. This allows you to include or exclude specific platforms like Windows, macOS, iOS, and Android. Therefore, to only allow access from Windows, the Conditions setting is used.

• Grant: This section defines the access controls that are enforced once the conditions are met. To ensure a device meets organizational standards for security and configuration, you use the Grant control "Require device to be marked as compliant". This control checks the device's compliance status (managed by a solution like Microsoft Intune) before granting access.

References:

Microsoft Learn Conditional Access: Conditions: This official documentation details the various conditions available in a Conditional Access policy. Under the "Device platforms" section, it states, "Conditional Access identifies the device platform by using information provided by the device... By default, a Conditional Access policy applies to all device platforms." This confirms that filtering by device type (like Windows) is handled within the Conditions settings.

Microsoft Learn Conditional Access: Grant: This document explains the available grant controls. It explicitly lists "Require device to be marked as compliant" as a grant control. The document states, "This control requires the device used to access the cloud app is marked as compliant by a mobile device management (MDM) solution like Microsoft Intune." This verifies that enforcing compliance is a Grant control.

Question: 27

You have an Azure subscription that contains an instance of Azure Firewall Standard named AzFWL You need to identify whether you can use the following features with AzFW1:

• TLS inspection

• Threat intelligence

• The network intrusion detection and prevention systems (IDPS)

What can you use?

A. TLS inspection only

B. threat intelligence only

C. TLS inspection and the IDPS only

D. threat intelligence and the IDPS only

E. TLS inspection, threat intelligence, and the IDPS

Answer:

B

Explanation:

Azure Firewall is available in multiple SKUs, with different feature sets. The Standard SKU includes threat intelligence-based filtering, which can alert and deny traffic from/to known malicious IP addresses, FQDNs, and URLs based on the Microsoft Threat Intelligence feed. However, both TLS inspection (for decrypting and inspecting outbound traffic) and the signature-based network intrusion detection and prevention system (IDPS) are advanced features available only in the Azure Firewall Premium SKU. Since the firewall in the question is Azure Firewall Standard, only the threat intelligence feature can be used.

Why Incorrect Options are Wrong:

A. TLS inspection is an exclusive feature of the Azure Firewall Premium SKU, not the Standard SKU.
C. Both TLS inspection and IDPS are exclusive features of the Azure Firewall Premium SKU.
D. The IDPS is an exclusive feature of the Azure Firewall Premium SKU, not the Standard SKU.
E. TLS inspection and the IDPS are exclusive features of the Azure Firewall Premium SKU.

References:

1. Microsoft Documentation - Azure Firewall features: This document provides a table comparing the features across Standard, Premium, and Basic SKUs. It explicitly lists "Threat Intelligence" as available for Standard and Premium, while "IDPS" and "TLS inspection" are listed for Premium only.
Source: Microsoft Learn, Azure Firewall features, "Feature comparison" table.
2. Microsoft Documentation - Azure Firewall Premium features: This document details the capabilities of the Premium SKU, explicitly mentioning IDPS and TLS Inspection as key differentiators.
Source: Microsoft Learn, Azure Firewall Premium features, "IDPS" and "TLS inspection" sections.
3. Microsoft Documentation - Azure Firewall threat intelligence-based filtering: This page confirms that threat intelligence is a feature of both Standard and Premium SKUs.
Source: Microsoft Learn, Azure Firewall threat intelligence-based filtering, "Overview" section, Paragraph 2.

Question: 28

You have an Azure subscription that contains a storage account named storage1 and a virtual machine named VM1. VM1 is connected to a virtual network named VNet1 that contains one subnet and uses Azure DNS. You need to ensure that VM1 connects to storage1 by using a private IP address. The solution must minimize administrative effort. What should you do?

A. For storage1, disable public network access.

B. Create an Azure Private DNS zone.

C. On VNet1. create a new subnet.

D. For storage1, create a new private endpoint.

Answer:

D

Explanation:

Azure Private Endpoint is a network interface that connects you privately and securely to a service powered by Azure Private Link. To allow VM1 to connect to the storage1 account using a private IP address from within VNet1, you must create a private endpoint for the storage account in that VNet. This action provisions a network interface in a subnet of VNet1 with a private IP address. All traffic destined for the storage account from VM1 will then be routed through this private endpoint over the Microsoft backbone network, fulfilling the requirement with the most direct and administratively simple approach.

Why Incorrect Options are Wrong:

A. Disabling public network access is a security best practice when using private endpoints, but it does not create the private connection itself. This action alone would block access from VM1.
B. An Azure Private DNS zone is required for name resolution, but creating the private endpoint is the primary action that establishes the private IP. The endpoint creation process can automatically create and link the required DNS zone.
C. A new subnet is not required. The private endpoint can be deployed into the existing subnet within VNet1, so creating a new one adds unnecessary administrative effort.

References:

1. Microsoft Docs, Azure Private Endpoint overview: "Azure Private Endpoint is a network interface that uses a private IP address from your virtual network. This network interface connects you privately and securely to a service that's powered by Azure Private Link." (Source: What is Azure Private Endpoint?, Introduction section).
2. Microsoft Docs, Use private endpoints for Azure Storage: "You can use private endpoints for your Azure Storage accounts to allow clients on a virtual network (VNet) to securely access data

over a private link... The private endpoint uses an IP address from the VNet address space for your storage account service." (Source: Use private endpoints for Azure Storage, Introduction section).
3. Microsoft Docs, Azure Private Endpoint DNS configuration: "When you create a private endpoint, the DNS CNAME resource record for the public resource is updated to an alias in a subdomain with the prefix privatelink... Azure creates a private DNS zone attached to the virtual network with the CNAME alias for the private endpoints, if you opt-in for 'Integrate with private DNS zone' during private endpoint creation." (Source: Azure Private Endpoint DNS configuration, Azure services DNS zone configuration section).

Question: 29

HOTSPOT You have an Azure subscription that is linked to an Azure AD tenant and contains the virtual machines shown in the following table.

Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.1.2.5	20.224.219.230
VM3	VNET2/Subnet1	10.11.1.5	40.122.155.212

The subnets of the virtual networks have the service endpoints shown in the following table.

Subnet	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET1/Subnet2	Microsoft.KeyVault
VNET2/Subnet1	Microsoft.Storage, Microsoft.KeyVault

You create the resources shown in the following table.

Name	Type
storage1	Azure Storage account
Vault1	Azure Key Vault

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	○	○
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	○	○
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	○	○

Answer:

Yes

No

No

Explanation:

Connections from VM1 to storage1 always use IP address 10.1.1.5: Yes VM1 is in VNET1/Subnet1, which is configured with a service endpoint for Microsoft.Storage. When a service endpoint is used, traffic from the virtual machine to the specified Azure service is routed through the Azure backbone network. The source IP address for this traffic is the VM's private IP address. Therefore, connections from VM1 to storage1 will use its private IP, 10.1.1.5.

Connections from VM2 to Vault1 always use IP address 20.224.219.230: No VM2 is in VNET1/Subnet2, which has a service endpoint for Microsoft.KeyVault. Similar to the first statement, traffic from VM2 to Vault1 (an Azure Key Vault) will use the VM's private IP address (10.1.2.5) as the source, not its public IP address (20.224.219.230). The public IP would be used only if traffic were routed over the public internet, which the service endpoint prevents for this service.

Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212: No Authentication to the tenant is handled by Azure Active Directory (Azure AD). VM3's subnet, VNET2/Subnet1, has service endpoints for Microsoft.Storage and Microsoft.KeyVault, but not for Azure AD. Therefore, traffic for Azure AD authentication must be routed to the public internet. When an Azure VM initiates outbound traffic to the internet, the source IP address is its public IP address. In this case, authentication traffic from VM3 will exclusively use its public IP, 40.122.155.212.

References:

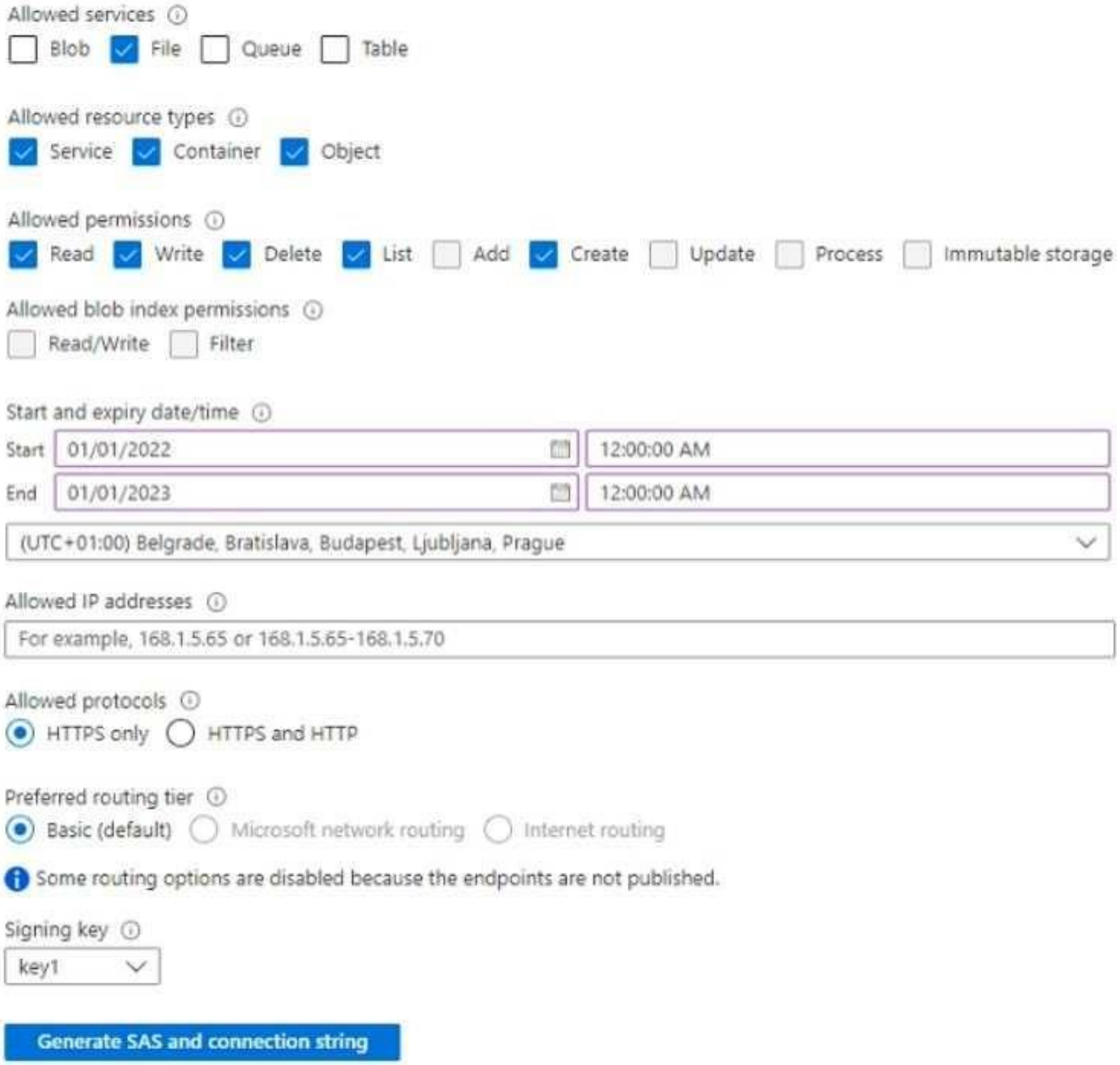
Microsoft Azure Documentation: "Virtual Network service endpoints." This document explains that when a service endpoint is enabled, "the source IP addresses of the virtual machines in the subnet for traffic to the Azure service switch from public IPv4 addresses to their private IPv4 addresses." This directly supports the reasoning for the first two statements.
Microsoft Azure Documentation: "Azure services that support virtual network service endpoints." This page lists the services for which endpoints can be configured. Azure Active Directory is not listed as a service that supports service endpoints, confirming that traffic to it from a VNet goes over the public internet, which supports the reasoning for the third statement.

Question: 30

HOTSPOT You have an Azure subscription that contains a user named User1 and a storage account named storage1. The storage1 account contains the resources shown in the following table.

Name	Type
container1	Container
folder1	File Share
table1	Table

In storage1, you create a shared access signature (SAS) named SAS1 as shown in the following exhibit.



To which resources can User! write on July 1, 2022 by using SAS1 and key 1? To answer, select the appropriate options in the answer area.

Answer Area

Answer:

SAS1: container1 and folder1 only

Key1: container1, folder1, and table1

Explanation:

The access permissions are determined by the credential used.

SAS1

The Shared Access Signature (SAS) token is configured with specific limitations. According to the exhibit:

• Allowed services: Only Blob and File services are enabled. The Table service is not.

• Allowed permissions: The Write permission is enabled.

• Validity: The date of access, July 1, 2022, is within the valid start and end dates.

Therefore, the SAS token grants write access to container1 (a Blob service resource) and folder1 (a File service resource), but not to table1 (a Table service resource).

Key1

Key1 is a storage account access key. Unlike a SAS token, an access key grants full administrative permissions to the entire storage account. This includes all services (Blob, File, Table, and Queue) and all supported operations within them. Consequently, using key1 provides

unrestricted write access to all resources: container1, folder1, and table1.

References:

Microsoft Documentation on Shared Access Signatures (SAS): "A shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control over how a client can access your data. For example: What resources the client may access. What permissions they have to those resources. How long the SAS is valid."
Source: Microsoft Docs, "Grant limited access to Azure Storage resources using shared access signatures (SAS)", Introduction section.
Microsoft Documentation on Storage Account Access Keys: "Anyone who has a valid access key has unrestricted access to that storage account... When you have your account access keys, you can use them to access any of the data in your storage account, or to grant access to the storage account's resources through a shared access signature (SAS)."
Source: Microsoft Docs, "Manage storage account access keys", Authorize with the account key section.

Question: 31

You have an Azure subscription that contains a user named UseR1. You need to ensure that UseR1 can perform the following tasks:

• Create groups.

• Create access reviews for role-assignable groups.

• Assign Azure AD roles to groups.

The solution must use the principle of least privilege. Which role should you assign to User1?

A. Groups administrator

B. Authentication administrator

C. Identity Governance Administrator

D. Privileged role administrator

Answer:

D

Explanation:

The Privileged Role Administrator is the least-privileged role that meets all three requirements. This role is specifically designed to manage role assignments in Azure Active Directory and Privileged Identity Management (PIM). It grants the permissions to:
1. Create and manage all groups, including making them role-assignable.
2. Manage PIM for groups, which includes creating and managing access reviews for role-assignable groups.
3. Assign Azure AD roles to groups, a highly privileged action that is a core function of this role.
This single role fulfills all specified tasks, adhering to the principle of least privilege.

Why Incorrect Options are Wrong:

A. Groups administrator: This role can create and manage groups but lacks the permissions to assign Azure AD roles to them or manage access reviews for role-assignable groups.
B. Authentication administrator: This role is focused on managing user authentication methods (like passwords and MFA) and has no permissions for group management or role assignments.
C. Identity Governance Administrator: While this role can create access reviews for groups, it cannot assign Azure AD roles to groups, which is a critical requirement of the question.

References:

1. Microsoft Learn, Azure AD built-in roles, "Privileged Role Administrator" section: "Users with this role can manage role assignments in Azure Active Directory, as well as within Azure AD Privileged Identity Management (PIM). .... This includes the ability to assign roles to groups." This directly supports the requirement to assign roles to groups.
2. Microsoft Learn, Assign Azure AD roles to groups, "Prerequisites" section: This document explicitly states that to assign a role to a group, you must have either Global Administrator or Privileged Role Administrator permissions. This disqualifies the other options.
3. Microsoft Learn, Azure AD built-in roles, "Identity Governance Administrator" section: The description confirms this role manages access reviews and access packages but does not list the permission to assign directory roles to groups.

Question: 32

You have an Azure subscription and the computers shown in the following table.

Name	Operating system	Description
VM1	Windows Server 2012 R2	Azure virtual machine
VM2	Red Hat Enterprise Linux (RHEL) 8.2	Azure virtual machine
Server1	Windows Server 2019	On-premises physical computer connected to Microsoft Defender for Cloud
VMSS1_0	Windows Server 2022	Azure virtual machine in a virtual machine scale set

You need to perform a vulnerability scan of the computers by using Microsoft Defender for Cloud. Which computers can you scan?

A. VM1 only

B. VM1 and VM2 only

C. Server1 and VMSS1.0 only

D. VM1, VM2, and Server1 only

E. VM1, VM2, Server1, and VMSS1.0

Answer:

D

Explanation:

Microsoft Defender for Cloud's built-in vulnerability assessment (VA) can be enabled only on:
• Azure virtual machines (Windows or Linux) that run in the subscription, and
• non-Azure machines onboarded through Azure Arc.
At the time of the referenced documentation, VA is explicitly "not supported for Virtual Machine Scale Sets."
Therefore VM1 (Azure VM), VM2 (Azure VM), and Server1 (Arc-enabled on-premises server) can be scanned, whereas VMSS1.0 (instance in a scale set) cannot.

Why Incorrect Options are Wrong:

A. Ignores VM2 (Azure VM) and Server1 (Arc); both are supported.
B. Omits Server1, which is Arc-enabled and therefore scannable.
C. Includes VMSS1.0, which VA does not support; excludes VM1 and VM2 that are supported.
E. Incorrectly includes VMSS1.0; VA cannot scan scale-set instances.

References:

1. Microsoft Defender for Cloud - "Deploy the integrated Qualys vulnerability assessment solution" Supported resources section: "Supported on Azure VMs and Azure Arc-enabled machines; Virtual machine scale sets are not currently supported." (Docs ID: defender-for-cloud/deploy-vulnerability-assessment-vm, para. 3, retrieved 2023-08-01)
2. Microsoft Defender for Cloud - "Vulnerability assessment in Defender for Cloud" Table: Resource types supported (VMs , Arc servers , VMSS). (Docs ID: defender-for-cloud/vulnerability-assessment-overview, section 'Supported resources', 2023-07-17)
3. Microsoft Learn - "Quickstart: Enable Azure Arc server and deploy Defender for Cloud VA" confirms Arc-enabled servers use the same VA extension as Azure VMs. (Docs ID: azure-arc/quickstart-defender-va, step 4)

Question: 33

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. EASM1 has discovery enabled and contains several inventory assets. You need to identify which inventory assets are vulnerable to the most critical web app security risks. Which Defender EASM dashboard should you use?

A. Attack Surface Summary

B. GDPR Compliance

C. Security Posture

D. OWASP Top 1O

Answer:

D

Explanation:

Microsoft Defender External Attack Surface Management (Defender EASM) includes a dedicated OWASP Top 10 dashboard. This dashboard is specifically designed to help organizations identify which of the most critical web application security risks, as defined by the Open Web Application Security Project (OWASP), are present within their inventoried assets. It directly maps discovered vulnerabilities to the OWASP Top 10 categories, allowing security teams to prioritize remediation efforts based on this widely recognized standard for web application security.

Why Incorrect Options are Wrong:

A. Attack Surface Summary: This dashboard provides a high-level, general overview of the attack surface, including key statistics and high-priority observations, but does not specifically categorize risks by the OWASP Top 10 framework.
B. GDPR Compliance: This dashboard is focused on identifying potential compliance issues related to the General Data Protection Regulation (GDPR), such as data privacy and PII exposure, not web application security vulnerabilities.
C. Security Posture: This dashboard provides insights into overall security program maturity, including exposed CVEs and cloud misconfigurations, but it is broader and not specifically tailored to the OWASP Top 10 risks.

References:

1. Microsoft Learn: "Understanding the dashboards". This official documentation explicitly describes the purpose of the Defender EASM dashboards.
Reference for Correct Answer (D): Under the "OWASP Top 10" section, it states, "This dashboard helps you understand which of the most critical web application security risks, as defined by the OWASP foundation, are present in your attack surface."

Reference for Incorrect Answer (A): The "Attack Surface Summary" section describes it as providing "a high-level overview of your attack surface."
Reference for Incorrect Answer (C): The "Security Posture" section explains that it "helps organizations understand the maturity of their security program" by providing information on CVEs and security scores.
Reference for Incorrect Answer (B): The "GDPR Compliance" section states, "This dashboard helps users understand how their attack surface complies with GDPR requirements."

Question: 34

You have an Azure subscription that uses Microsoft Defender for Cloud. The subscription contains the Azure Policy definitions shown in the following table.

Name	Type	Category
Policy1	Policy	Regulatory Compliance
Policy2	Policy	Security Center
Initiative1	Initiative	Regulatory Compliance
Initiative2	Initiative	Security Center

Which definitions can be assigned as a security policy in Defender for Cloud?

A. Policy1 and Policy2 only

B. Initiative1 and Initiative2 only

C. Policy1 and Initiative1 only

D. Policy2 and Initiative2 only

E. Policy1, Policy2, Initiative1, and Initiative2

Answer:

B

Explanation:

Microsoft Defender for Cloud uses Azure Policy to enforce and assess security standards. A security policy in Defender for Cloud is built upon an Azure Policy initiative, which is a collection of individual policy definitions. While individual policies define specific rules, they are not assigned directly within the Defender for Cloud security policy interface. Instead, you assign an initiative (either the default "Azure Security Benchmark" or a custom one) to a subscription or management group. Therefore, only the definitions with the type Initiative (Initiative1 and Initiative2) can be assigned as a security policy in Defender for Cloud.

Why Incorrect Options are Wrong:

A, C, E: These options are incorrect because individual policies (Policy1, Policy2) cannot be directly assigned as a security policy in Defender for Cloud; they must be part of an initiative.
D: This option is incorrect because it omits Initiative1. Any custom initiative, regardless of its category, can be added as a security policy in Defender for Cloud.

References:

1. Microsoft Learn, "Create custom security initiatives and policies."
Reference: Under the section "To add a custom initiative to your subscription," the documentation states: "In the Add custom initiatives page, the list of initiatives available in your organization is displayed." This confirms that the mechanism is for adding initiatives, not individual policies.
URL: https://learn.microsoft.com/en-us/azure/defender-for-cloud/custom-security-policies
2. Microsoft Learn, "Security policies overview."
Reference: In the section "What are security policies, initiatives, and recommendations?", it clarifies: "Microsoft Defender for Cloud assigns a built-in initiative, Azure Security Benchmark, to every subscription... To customize the security policies for your subscription... you can create your own custom initiatives in Azure Policy." This explicitly links the concept of a "security policy" in Defender for Cloud to an "initiative" in Azure Policy.
URL: https://learn.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept
3. Microsoft Learn, "What is Azure Policy?"
Reference: The "Initiative definition" section explains that an initiative is a "collection of policy definitions...". This foundational document distinguishes between a policy and an initiative, which is crucial for understanding why Defender for Cloud uses initiatives to group security controls.
URL: https://learn.microsoft.com/en-us/azure/governance/policy/overview#initiative-definition

Question: 35

You have an Azure subscription that uses Microsoft Defender for Cloud. You need to use Defender for Cloud to review regulatory compliance with the Azure CIS 1.4,0 standard. The solution must minimize administrative effort. What should you do first?

A. Assign an Azure policy.

B. Manually add the Azure CIS 1.4.0 standard.

C. Disable one of the Out of the box standards.

D. Add a custom initiative.

Answer:

B

Explanation:

Microsoft Defender for Cloud provides a regulatory compliance dashboard to track adherence against various security standards. By default, subscriptions are assessed against the Microsoft cloud security benchmark. To review compliance against a different or additional standard, such as Azure CIS 1.4.0, an administrator must first add it to the security policy for the relevant scope (subscription or management group). This is a straightforward action performed within the Defender for Cloud portal under "Environment settings," which then enables the compliance data and recommendations for that standard to be displayed on the dashboard. This is the most direct method and requires minimal administrative effort.

Why Incorrect Options are Wrong:

A. Assigning an Azure policy directly is not the intended user workflow; Defender for Cloud automatically manages the underlying policy initiative assignment when you add a standard through its interface.
C. Disabling an existing standard is an unrelated action that does not contribute to adding or reviewing a new compliance standard.
D. Adding a custom initiative is only necessary when a built-in standard is unavailable or insufficient. Since Azure CIS 1.4.0 is a built-in option, creating a custom one would be a significant and unnecessary effort.

References:

1. Microsoft Learn, Microsoft Defender for Cloud Documentation. "Customize the set of standards in your regulatory compliance dashboard." This document explicitly states the procedure: "To add other standards, such as NIST, Azure CIS... you need to add them to the subscription... From Defender for Cloud's menu, open the Environment settings page... Select the relevant subscription or management group... Select Security policy... Under the Industry & regulatory

standards section, select Add more standards." This directly supports the action described in option B.
2. Microsoft Learn, Microsoft Defender for Cloud Documentation. "Tutorial: Improve your regulatory compliance." In the section "What is the regulatory compliance dashboard in Defender for Cloud?", it notes that you can customize the dashboard by choosing relevant standards, linking to the customization process. This confirms that adding a standard is the primary step to begin tracking it.
3. Microsoft Learn, Microsoft Defender for Cloud Documentation. "What are security policies, initiatives, and recommendations?". This document clarifies the underlying mechanism: "When you enable Defender for Cloud, it creates a default security initiative... When you add a regulatory standard to your dashboard, an initiative is added to the Azure Policy portal for the selected scope." This shows that while Azure Policy is used, the user's first and simplest action is within Defender for Cloud, not directly in Azure Policy.