DUMPSARENA

Microsoft Azure Security Technologies

Microsoft AZ-500

Version Demo

Total Demo Questions: 20

Total Premium Questions: 623

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, New Update	287
Topic 2, Case Study 1	2
Topic 3, Case Study 2	3
Topic 4, Case Study 3	4
Topic 5, Case Study 4	3
Topic 6, Case Study 5	5
Topic 7, Case Study 6	2
Topic 8, Case Study 7	2
Topic 9, Case Study 8	3
Topic 10, Mixed Questions	312
Total	623

QUESTION NO: 1

You are responsible for gathering logs from a substantial number of Windows Server 2016 computers using Azure Log Analytics.

Currently, you are configuring an Azure Resource Manager template to deploy the Microsoft Monitoring Agent across all servers automatically.

Which of the following elements should be incorporated into the template for successful deployment? (Choose all that apply.)

A. WorkspaceID

B. AzureADApplicationID

C. WorkspaceKey

D. StorageAccountKey

ANSWER: A C

Explanation:

Reference:

https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/

QUESTION NO: 2 - (DRAG DROP)

DRAG DROP

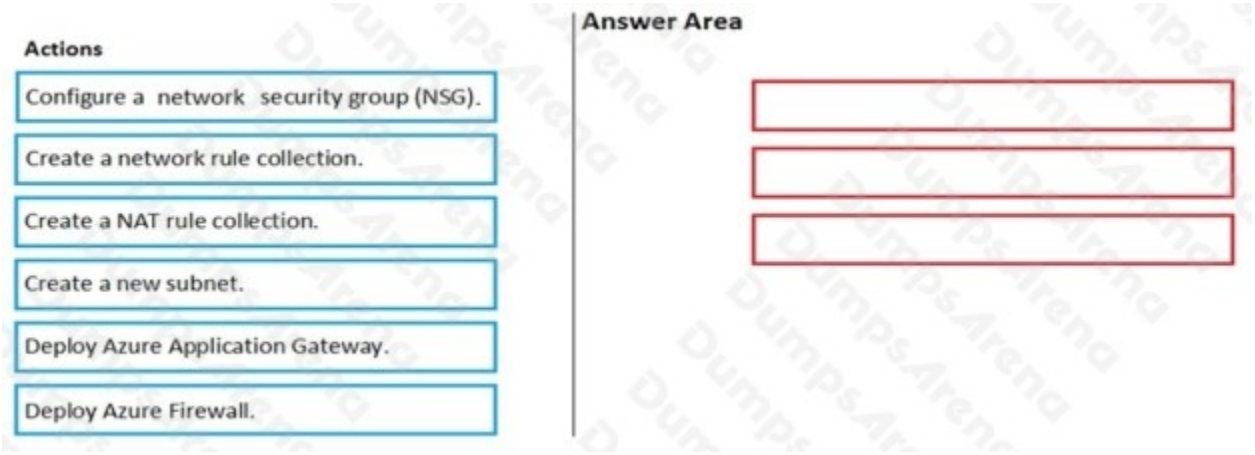
You have an Azure subscription that contains the following resources:

- A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.
- A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

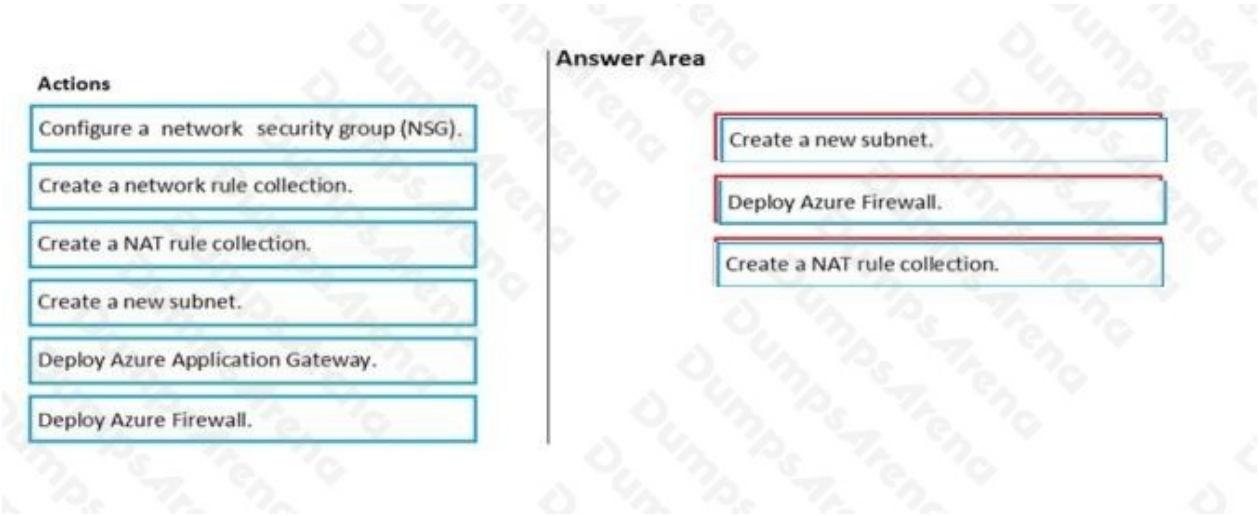
You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange then in the correct order.

Select and Place:



ANSWER:



Explanation:

QUESTION NO: 3

You have an Azure subscription that includes a web application named App1. Users must have the option to choose either a Google identity or a Microsoft identity for authentication to App1. Which two pieces of information must you configure to add Google as an identity provider in Azure Active Directory? Select two options, each correct choice is worth one point.

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:

https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-google

QUESTION NO: 4

You have an Azure Active Directory (Azure AD) tenant named contoso.com that includes a user called User1. You are planning to publish several applications in the tenant. You need to ensure that User1 can grant admin consent for these published applications. Which two user roles can you assign to User1 to achieve this goal? Each correct answer provides a complete solution.

NOTE: Each correct selection is worth one point.

A. Application developer

B. Security administrator

C. Application administrator

D. User administrator

E. Cloud application administrator

ANSWER: C E

Explanation:

In Azure Active Directory, certain roles have the ability to grant admin consent for applications. The roles "Application Administrator" and "Cloud Application Administrator" have the permissions required to grant admin consent to applications. For more information, you can visit the official Microsoft documentation on granting admin consent in Azure AD.

QUESTION NO: 5 - (SIMULATION)

SIMULATION

You need to create a new Azure Active Directory (Azure AD) directory named 12345678.onmicrosoft.com. The new directory must contain a user named user12345678 who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

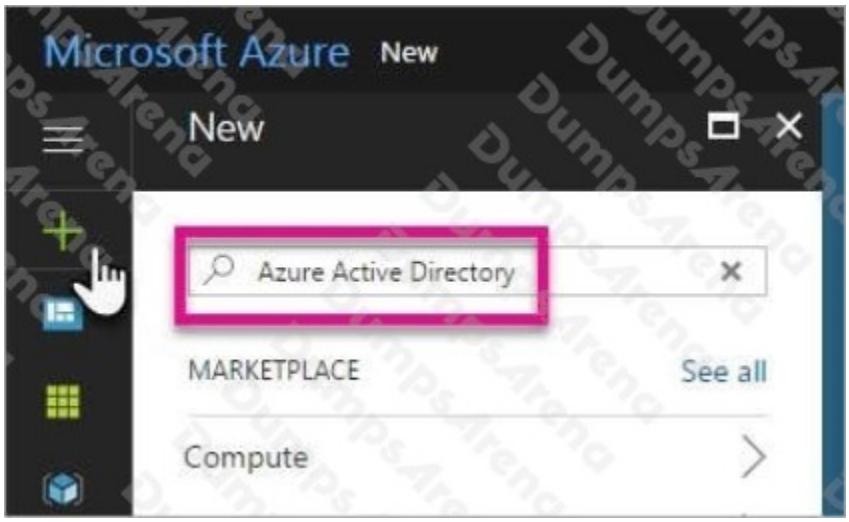
ANSWER: See the explanation below.

Explanation:

To create a new Azure AD tenant:

1. Browse to the Azure portal and sign in with an account that has an Azure subscription.

2. Select the plus icon (+) and search for Azure Active Directory.



3. Select Azure Active Directory in the search results.

4. Select Create.

5. Provide an Organization name (12345678) and an Initial domain name (12345678). Then select Create. This will create the directory named 12345678.onmicrosoft.com.

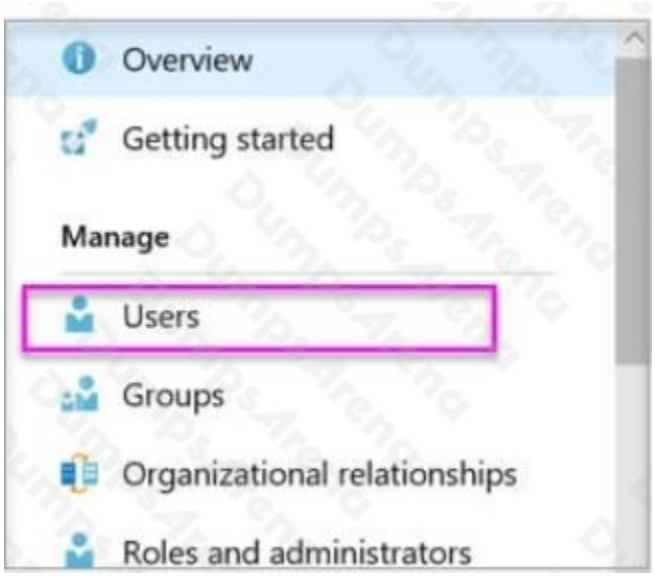
6. After directory creation is complete, select the information box to manage your new directory.

To create the user:

1. In the Azure portal, make sure you are on the Azure Active Directory fly out.

If not, select the Azure Active Directory icon from the left services navigation.

2. Under Manage, select Users.



3. Select All users and then select + New user.

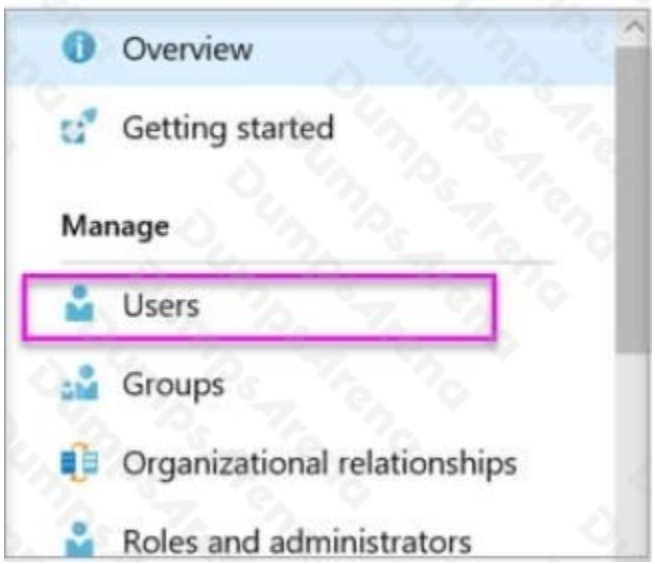
4. Provide a Name and User name (user12345678) for the user. When you're done, select Create.

To enable MFA:

1. In the Azure portal, make sure you are on the Azure Active Directory fly out.

If not, select the Azure Active Directory icon from the left services navigation.

2. Under Manage, select Users.



3. Click on the Multi-Factor Authentication link.

4. Tick the checkbox next to the user's name and click the Enable link.

Reference:

https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

QUESTION NO: 6

You have an Azure Active Directory (Azure AD) tenant that includes users with Azure AD Premium Plan 2 licenses. A partner company has a domain named fabrikam.com, which includes a user referred to as User1 with the email address user1@fabrikam.com. You need to provide User1 access to resources within your tenant while ensuring the implementation meets specific requirements. What action should you take?

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:

To provide a user from an external domain access to your Azure AD resources, you should use Azure AD B2B collaboration by creating an invitation link for the user. This approach allows the external user to access your resources securely without the need to establish a separate user account in your domain. More details can be found in the official Microsoft documentation: Microsoft B2B documentation.

QUESTION NO: 7

You have an Azure subscription that includes an Azure SQL database named SQL1 and an Azure Key Vault named KeyVault1. The Key Vault contains the following keys as shown in the table:

Your task is to configure Transparent Data Encryption (TDE) for SQL1 using a customer-managed key. Which of the keys listed in KeyVault1 can be used for this purpose?

A. Key2 only

B. Key1 only

C. Key2 and Key3 only

D. Key1, Key2, Key3, and Key4

E. Key1 and Key2 only

ANSWER: E

Explanation:

The key must be an asymmetric, RSA or RSA HSM key. The supported key lengths are 2048-bit and 3072-bit.

Reference: https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview

QUESTION NO: 8

You have configured your Azure subscription to use an alternative Azure Active Directory (Azure AD) tenant. What are two possible impacts of this change? Each correct answer presents a complete solution.

Note: Each correct selection is worth one point.

A. Role assignments at the subscription level are lost.

B. Virtual machine managed identities are lost.

C. Virtual machine disk snapshots are lost.

D. Existing Azure resources are deleted.

ANSWER: A B

Explanation:

Changing the Azure Active Directory associated with an Azure subscription can have several effects. When you change the directory:
Role assignments at the subscription level might be lost because role assignments depend on users, groups, and service principals which belong to the Azure AD directory associated with the subscription.
Managed identities for Azure resources are tied to the Azure AD tenant that the subscription is associated with. If the directory changes, these identities may no longer be valid.

For more details, you can refer to the official documentation on Azure AD and subscription association.

QUESTION NO: 9 - (HOTSPOT)

HOTSPOT

You plan to use Azure Monitor Logs to collect logs from 200 servers that run Windows Server 2016.

You need to automate the deployment of the Log Analytics Agent to all the servers by using an Azure Resource Manager template.

How should you complete the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

ANSWER:

Explanation:

References: https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/

QUESTION NO: 10 - (DRAG DROP)

You have an Azure subscription.

You plan to create two custom roles named Role1 and Role2.

The custom roles will be used to perform the following tasks:

• Members of Role1 will manage application security groups.

• Members of Role2 will manage Azure Bastion.

You need to add permissions to the custom roles.

Which resource provider should you use for each role? To answer, drag the appropriate resource providers to the correct roles. Each resource provider 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:

Explanation:

QUESTION NO: 11

You are addressing a security concern related to an Azure Storage account. Diagnostic logs have been enabled for this storage account. Which tool would you utilize to access and retrieve these diagnostic logs?

A. Azure Storage Explorer

B. SQL query editor in Azure

C. File Explorer in Windows

D. Azure Security Center

ANSWER: A

Explanation:

To download metrics for long-term storage or local analysis, a tool or custom code is necessary to read the diagnostics tables directly by their names, as they aren't listed among all tables in your storage account. Many storage-browsing tools facilitate direct viewing of these tables. Available graphical user interface (GUI) tools provided by Microsoft for interacting with your Azure Storage account data include Azure Storage Explorer and AzCopy. These tools are free and recommended for retrieving diagnostic logs. For more details, you can visit the following resources: Azure Storage Analytics Metrics and Azure Storage Explorers.

QUESTION NO: 12

Note: This question is part of a series concerning the same scenario. Each question in this series includes a distinct solution which may or may not fulfill the specified goals. Some sets of questions may contain more than one correct solution, whereas others might not have any correct solution.

Once you answer a question in this section, you cannot revisit it later. These questions therefore will not appear in the review screen.

Scenario: You have an Azure subscription containing 50 virtual machines running either Windows Server 2012 R2 or Windows Server 2016.

Objective: Deploy Microsoft Antimalware to these virtual machines.

Solution: You connect to each virtual machine individually and install it as a Windows feature.

Does this solution achieve the objective?

A. Yes

B. No

ANSWER: B

Explanation:

Microsoft Antimalware is deployed as an extension and not a feature.

Reference:

https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

QUESTION NO: 13

Upon onboarding Microsoft Azure Sentinel and establishing a connection to Azure Security Center, you aim to automate the resolution of incidents within Azure Sentinel. Your chosen solution should ensure administrative efforts are kept to a minimum. What should you create to achieve this goal?

A. an alert rule

B. a playbook

C. a function app

D. a runbook

ANSWER: B

Explanation:

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION NO: 14

You have an Azure subscription that contains 100 virtual machines with the Azure Security Center's Standard tier enabled.

To assess the security posture of these virtual machines, you plan to execute a vulnerability scan on each of them.

In order to automate the deployment of the vulnerability scanner extension across all virtual machines, you intend to utilize an Azure Resource Manager template.

Which two parameters must you specify in the template to ensure successful deployment of the extension to the virtual machines? Each correct answer constitutes part of the total solution.

Note: Each correct selection is worth one point.

A. the user assigned managed identity

B. the Key Vault managed storage account Key

C. the Azure Active Directory (Azure AD) ID

D. the system-assigned managed identity

E. the primary shared key

F. the workspace ID

ANSWER: A C

Explanation:

To deploy the vulnerability scanner extension to virtual machines using an Azure Resource Manager template, you typically need to use values like user assigned managed identity and the Azure Active Directory (Azure AD) ID. Managed identities allow Azure resources to authenticate to cloud services securely without the need to store credentials in the code. For more information, you can visit the official documentation at Azure Resource Manager Templates.

QUESTION NO: 15

You have been tasked with configuring an access review, which you intend to assign to a new collection of reviews. Additionally, you must ensure that the reviews can be assessed by resource owners.

You begin by creating an access review program and an access review control.

Your next step is to configure the Reviewers.

Which of the following should you designate as Reviewers?

A. Selected users.

B. Members (Self).

C. Group Owners.

D. Anyone.

ANSWER: C

Explanation:

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review
https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

QUESTION NO: 16

Consider the following scenario: Your organization utilizes an Active Directory forest with a single domain, currently identified as weylandindustries.com, and an Azure Active Directory (Azure AD) tenant that is similarly named. You are responsible for integrating the on-premises Active Directory with the Azure AD tenant by deploying Azure AD Connect. The integration strategy must ensure that password policies and user logon restrictions are consistently applied to user accounts synchronized to the Azure AD tenant, while minimizing the number of servers required. Proposed Solution: You suggest implementing federation using Active Directory Federation Services (AD FS). Does this recommendation fulfill the integration requirements?

A. Yes

B. No

ANSWER: B

Explanation:

A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

QUESTION NO: 17

You have an Azure Active Directory (Azure AD) tenant with several deleted objects, as shown in the table below:

On May 4, 2020, you attempt to restore the deleted objects using the Azure Active Directory admin center.

Which two objects can you restore? Each correct answer represents a complete solution.

Note: Each correct selection is worth one point.

A. Group1

B. Group2

C. User2

D. User1

ANSWER: B C

Explanation:

Deleted users and deleted Office 365 groups can be restored within 30 days of their deletion. However, deleted security groups cannot be restored. For more information, refer to the official documentation: https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted.

QUESTION NO: 18

You have an Azure subscription that includes the resources listed in the following table.

Name	Type	Description
RG1	Resource Group	Used to store virtual machines
RG2	Resource Group	Used to store virtual networks
ServerAdmins	Security Group	Used to manage virtual machines

You need to allow ServerAdmins to perform the following task: Create a virtual machine in the existing virtual network located in RG2 only. The solution must adhere to the principle of least privilege.
Which two role-based access control (RBAC) roles should you assign to the ServerAdmins group? Each correct answer is part of the needed solution.
NOTE: Each correct selection is worth one point.

A. the Contributor role for the subscription

B. the Network Contributor role for RG2

C. A custom RBAC role for the subscription

D. a custom RBAC role for RG2

E. the Network Contributor role for RG1.

F. the Virtual Machine Contributor role for RG1.

ANSWER: B F

Explanation:

To allow ServerAdmins to create virtual machines in RG2's virtual network while adhering to the principle of least privilege, two specific roles should be assigned:
The **Network Contributor** role for RG2 allows network modifications needed for the virtual machines.
The **Virtual Machine Contributor** role for RG1 allows creation and management of virtual machines. However, given this requires access to RG2, it's clarified by specifying access to VM needs in its network, not storage.
For more information on role assignments, you can refer to Microsoft's official documentation on Role Assignments.

QUESTION NO: 19 - (HOTSPOT)

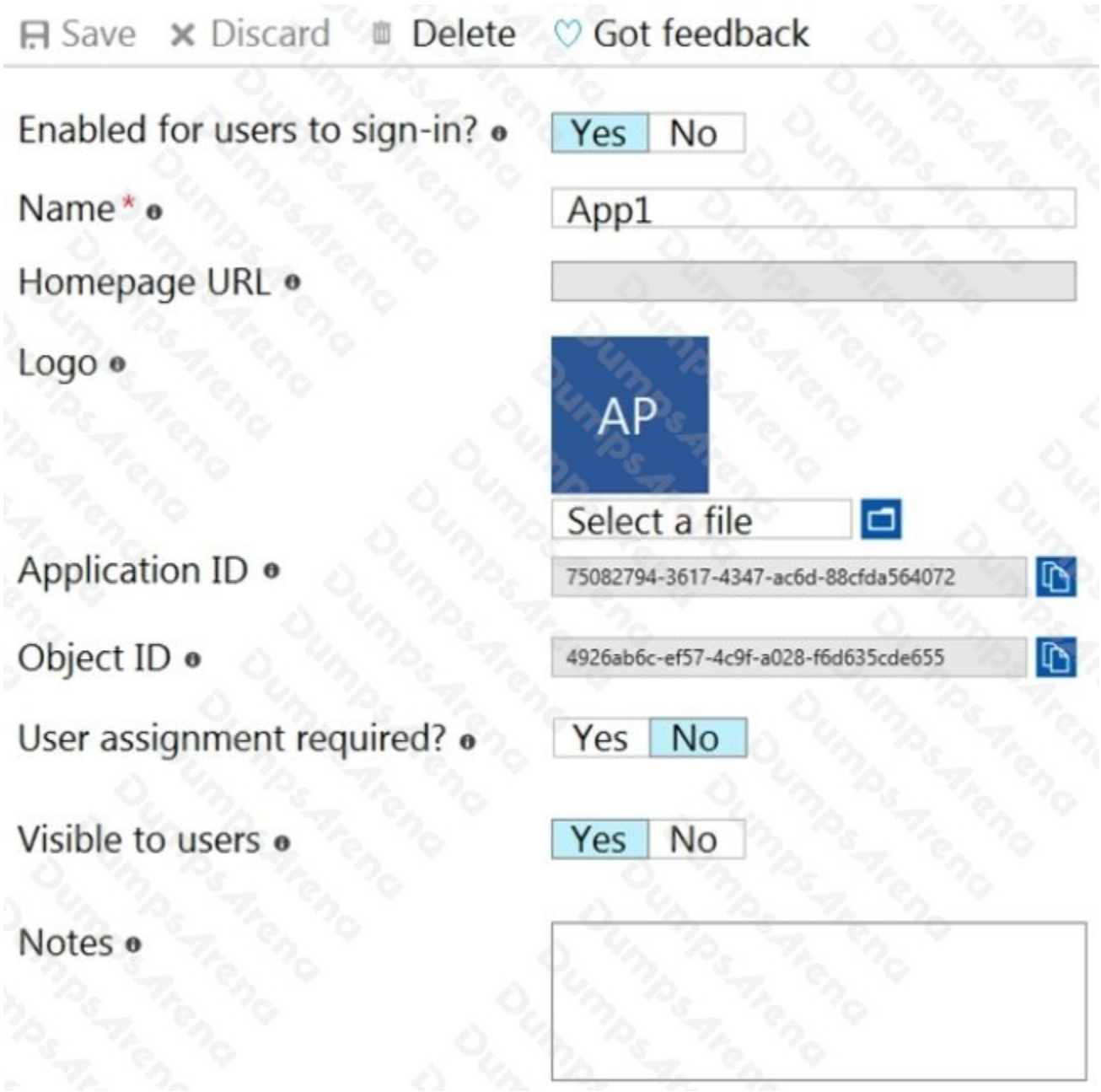
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.

Name	Role	Member of
User1	Application administrator	Group1
User2	Application developer	Group2
User3	Cloud application administrator	Group3

Group3 is a member of Group2.

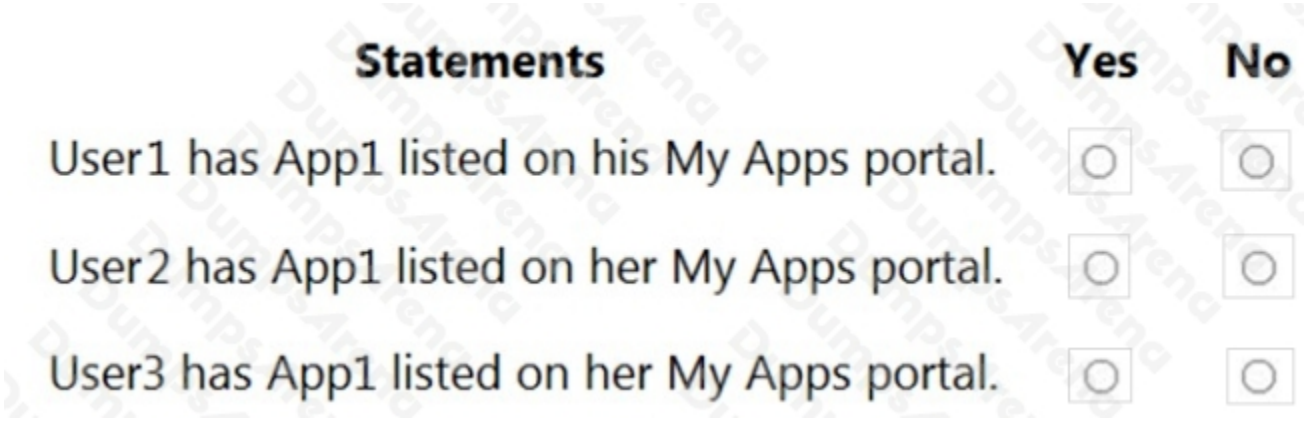
In contoso.com, you register an enterprise application named App1 that has the following settings:

You configure the properties of App1 as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.



ANSWER:

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal

QUESTION NO: 20 - (SIMULATION)

SIMULATION

You need to configure network connectivity between a virtual network named VNET1 and a virtual network named VNET2. The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2.

To complete this task, sign in to the Azure portal and modify the Azure resources.

ANSWER: See the explanation below.

Explanation:

You need to configure VNet Peering between the two networks. The questions states, “The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2”. It doesn’t say the VMs on VNET2 should be able to communicate with VMs on VNET1. Therefore, we need to configure the peering to allow just the one-way communication.

1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.

2. In the properties of VNET1, click on Peerings.

3. In the Peerings blade, click Add to add a new peering.

4. In the Name of the peering from VNET1 to remote virtual network box, enter a name such as VNET1-VNET2 (this is the name that the peering will be displayed as in VNET1)

5. In the Virtual Network box, select VNET2.

6. In the Name of the peering from remote virtual network to VNET1 box, enter a name such as VNET2-VNET1 (this is the name that the peering will be displayed as in VNET2).

There is an option Allow virtual network access from VNET to remote virtual network. This should be left as Enabled.

7. For the option Allow virtual network access from remote network to VNET1, click the slider button to Disabled.

8. Click the OK button to save the changes.

Reference:

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