QUESTION 368
You have an Azure subscription that contains the resources shown in the following table.

Name	Type
storage1	Storage account
Vault1	Azure Key vault
Vault2	Azure Key vault

You plan to deploy the virtual machines shown in the following table.

Name	Role
VM1	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1
VM2	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1
VM3	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2
VM4	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2

You need to assign managed identities to the virtual machines. The solution must meet the following requirements:
- Assign each virtual machine the required roles.
- Use the principle of least privilege.
What is the minimum number of managed identities required?

A. 1

B. 2
C. 3
D. 4

Answer: B
Explanation:
We have two different sets of required permissions. VM1 and VM2 have the same permission requirements. VM3 and VM4 have the same permission requirements.
A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

QUESTION 369
You have an Azure subscription that uses Microsoft Sentinel. You need to create a Microsoft Sentinel notebook that will use the Guided Investigation - Anomaly Lookup template.
What should you create first?

A. an analytics rule
B. a Log Analytics workspace
C. an Azure Machine Learning workspace
D. a hunting query

Answer: A

QUESTION 370
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
You need to ensure that User1 can create and manage administrative units. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. Privileged role administrator
B. Helpdesk administrator
C. Global administrator
D. Security administrator

Answer: A

QUESTION 371
You have an Azure subscription that contains the resources shown in the following Table.

Name	Type
VM1	Virtual machine
VNET1	Virtual network
storage1	Storage account
Vault1	Key vault

You plan to enable Microsoft Defender for Cloud for the subscription.
Which resources can be protected by using Microsoft Defender for Cloud?

A. VM1, VNET1, and storage1 only
B. VM1, storage1, and Vault1 only
C. VM1.VNET1, storage1, and Vault1
D. VM1 and storage1 only
E. VM1 and VNET only

Answer: C

QUESTION 372
You have the Azure resource shown in the following table.

Name	Type	Parent
Management1	Management group	Tenant Root Group
Subscription1	Subscription	Management1
RG1	Resource group	Subscription1
RG2	Resource group	Subscription1
VM1	Virtual machine	RG1
VM2	Virtual machine	RG2

You need to meet the following requirements:
- Internet-facing virtual machines must be protected by using network security groups (NSGs).
- All the virtual machines must have disk encryption enabled.
What is the minimum number of security that you should create in Azure Security Center?

A. 1
B. 2
C. 3
D. 4

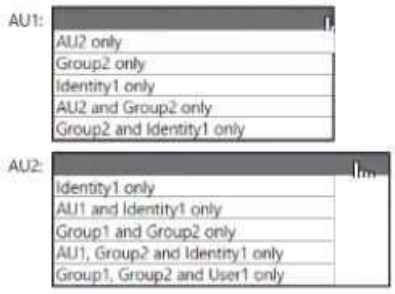
Answer: D

QUESTION 373
Hotspot Question
You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the resources shown in the following table.
Which resources can be added to AUI and AU2? To answer, select the appropriate options in the answer area.

Name	Type	Assigned object
AU1	Administrative unit	User1, Group1
AU2	Administrative unit	**None**
User1	User	**Not applicable**
Group1	Security group	**Not applicable**
Group2	Microsoft 365 group	**Not applicable**

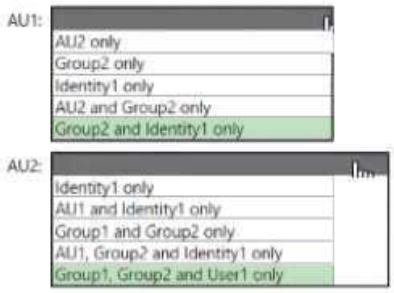
Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

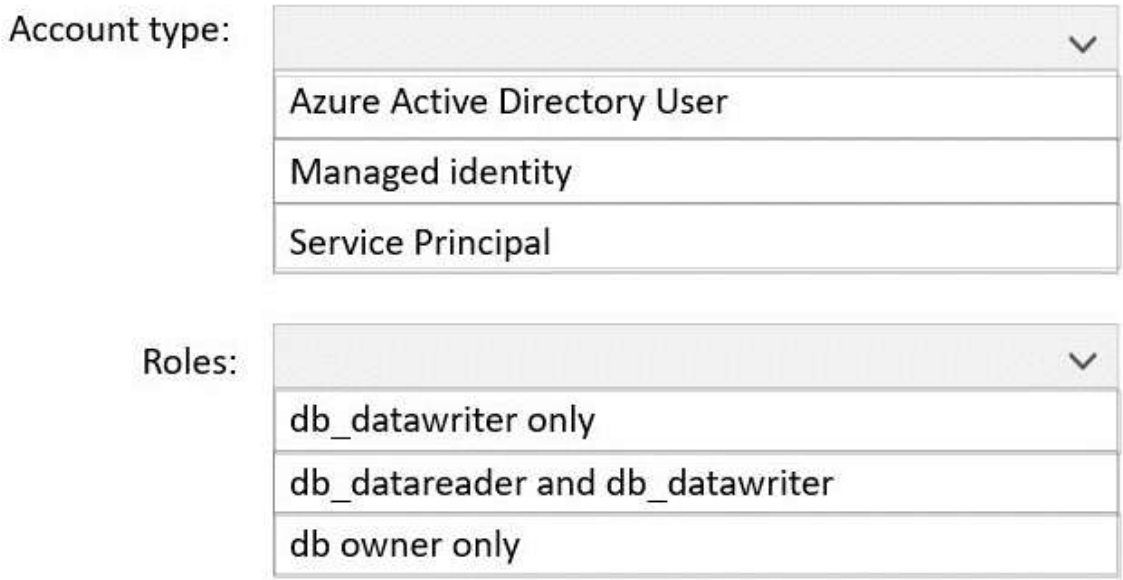


Answer:

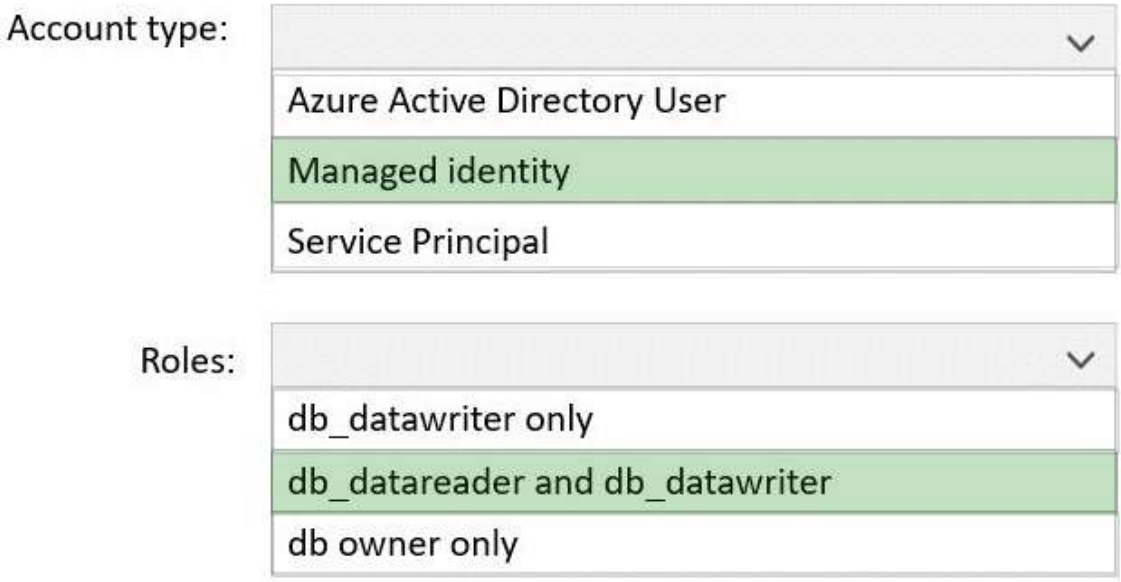
Answer Area



QUESTION 374
Hotspot Question
You have an Azure subscription that contains an Azure SQL database named SQL1.
You plan to deploy a web app named App1.
You need to provide App1 with read and write access to SQL1. The solution must meet the following requirements:
- Provide App1 with access to SQL1 without storing a password.
- Use the principle of least privilege.
- Minimize administrative effort.
Which type of account should App1 use to access SQL1, and which database roles should you assign to App1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cdotnet

QUESTION 375
SIMULATION
You need to ensure that a user named user2-12345678 can manage the properties of the virtual machines in the RG1lod12345678 resource group. The solution must use the principle of least privilege.
To complete this task, sign in to the Azure portal.
Answer:
Sign in to the Azure portal.
Browse to Resource Groups.
Select the RG1lod12345678 resource group.
Select Access control (IAM).
Select Add > role assignment.
Select Virtual Machine Contributor (you can filter the list of available roles by typing `virtual' in the search box) then click Next.
Select the +Select members option and select user2-12345678 then click the Select button.
Click the Review + assign button twice.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=current

QUESTION 376
SIMULATION
You need to create a new Azure Active Directory (Azure AD) directory named 12345678.onmicrosoft.com. The new directory must contain a new user named user1@12345678.onmicrosoft.com.
To complete this task, sign in to the Azure portal.
Answer:
The first step is to create the Azure Active Directory tenant.
Sign in to the Azure portal.
From the Azure portal menu, select Azure Active Directory.
On the overview page, select Manage tenants.
Select +Create.
On the Basics tab, select Azure Active Directory.
Select Next: Configuration to move on to the Configuration tab.
For Organization name, enter 12345678.
For the Initial domain name, enter 12345678.
Leave the Country/Region as the default.
The next step is to create the user.

From the Azure portal menu, select Azure Active Directory.
Select Users then select New user.
Enter User1 in the User name and Name fields.
Leave the default option of Auto-generate password.
Click the Create button.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory