AZ-500$^{\text{Q\&As}}$

Microsoft Azure Security Technologies

Pass Microsoft AZ-500 Exam with 100% Guarantee

QUESTION 1

References: https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

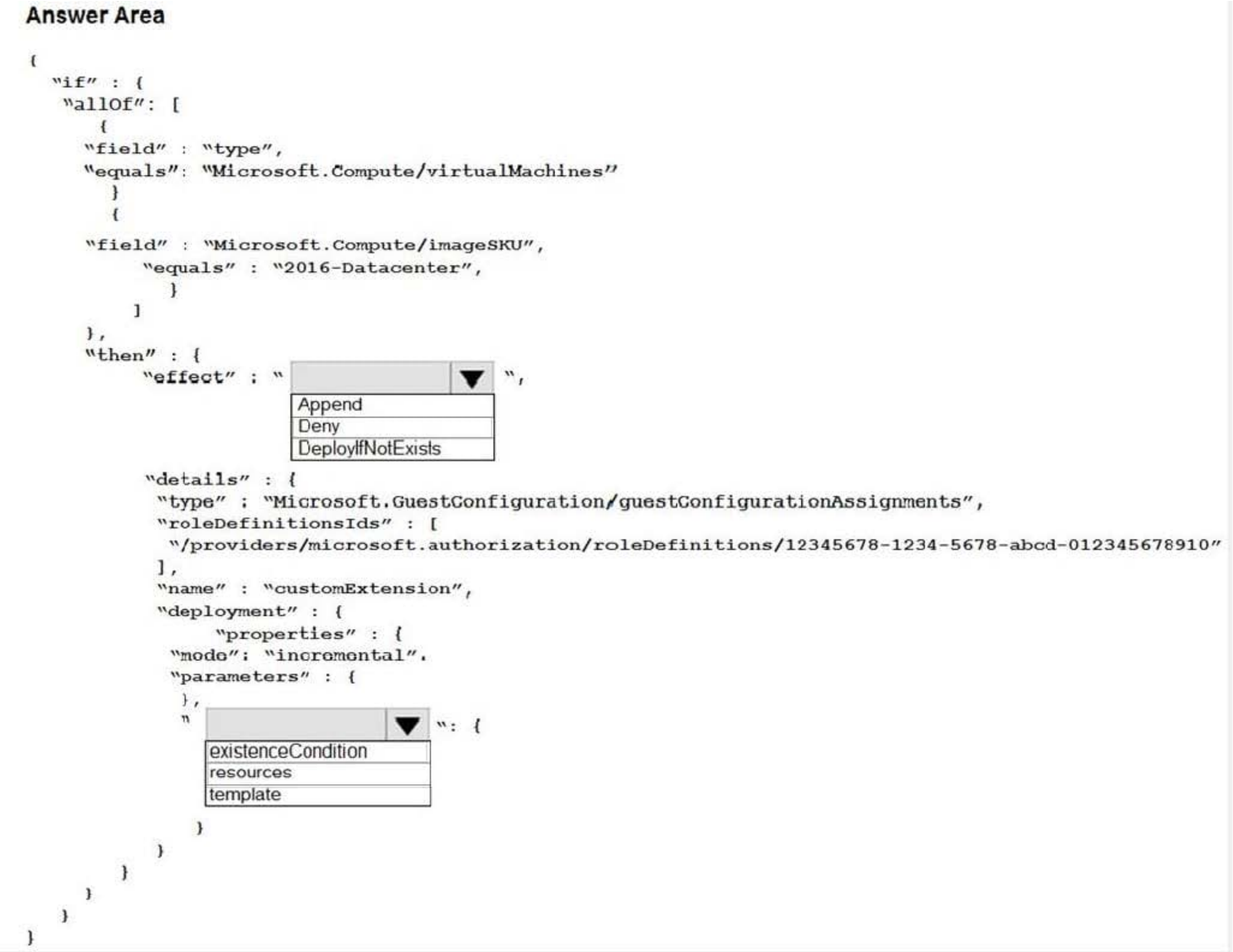
You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

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

NOTE: Each correct selection is worth one point.

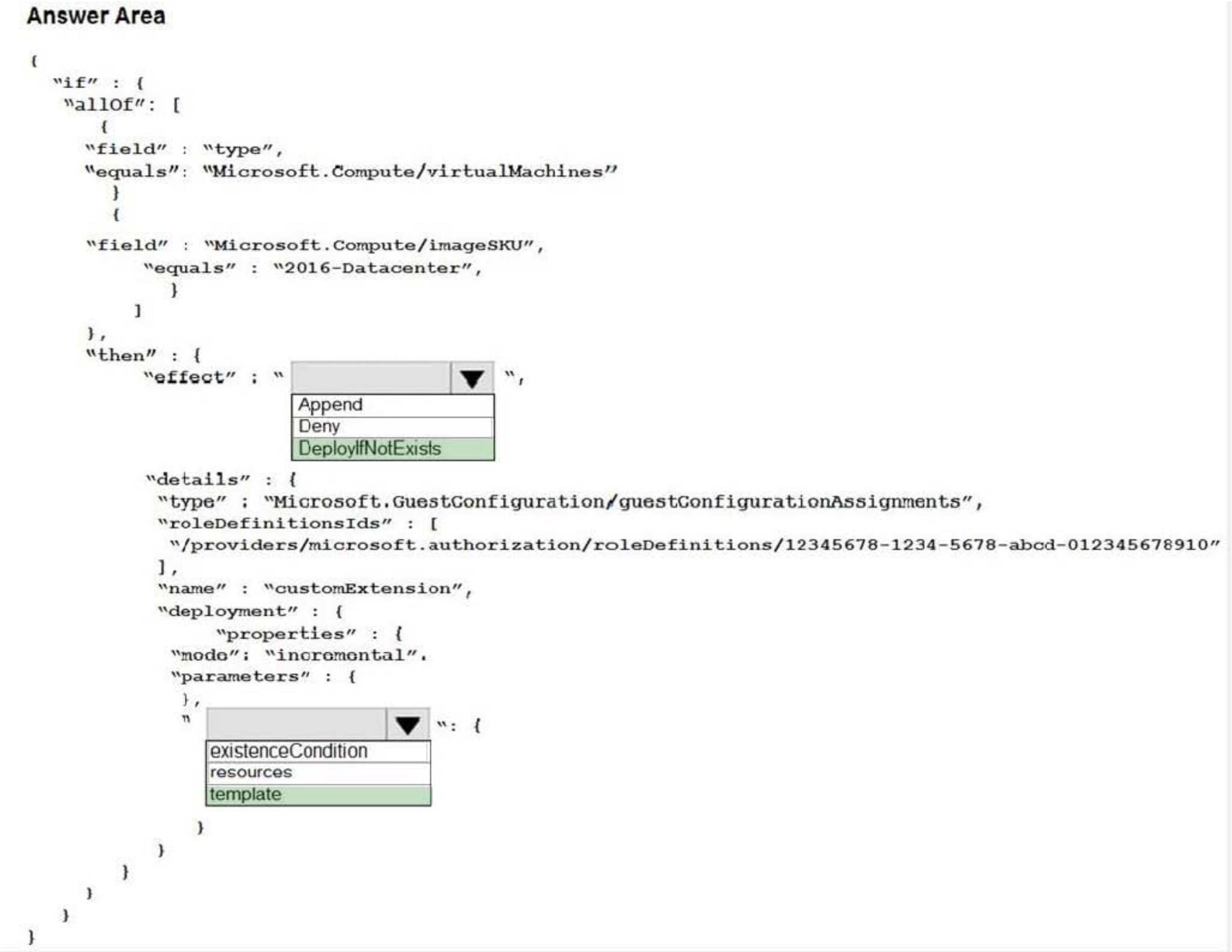
Hot Area:



Answer Area

```
{
  "if" : {
   "allOf": [
      {
     "field" : "type",
     "equals": "Microsoft.Compute/virtualMachines"
       }
       {
     "field" : "Microsoft.Compute/imageSKU",
          "equals" : "2016-Datacenter",
            }
         ]
     },
     "then" : {
          "effect" : "  [          ▼]  ",
                       Append
                       Deny
                       DeployIfNotExists
          "details" : {
           "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
           "roleDefinitionsIds" : [
            "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
           ],
           "name" : "customExtension",
           "deployment" : {
                "properties" : {
            "mode": "incremental",
            "parameters" : {
             },
             "  [          ▼]  ": {
                 existenceCondition
                 resources
                 template
                }
            }
         }
      }
    }
}
```

Correct Answer:



Answer Area

```
{
  "if" : {
   "allOf": [
      {
    "field" : "type",
    "equals": "Microsoft.Compute/virtualMachines"
       }
       {
    "field" : "Microsoft.Compute/imageSKU",
         "equals" : "2016-Datacenter",
           }
        ]
    },
    "then" : {
         "effect" : "                ",
         "details" : {
          "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
          "roleDefinitionsIds" : [
           "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
          ],
          "name" : "customExtension",
          "deployment" : {
               "properties" : {
           "mode": "incremental".
           "parameters" : {
            },
            "               ": {

             }
           }
         }
       }
    }
}
```

Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template

The details property of the DeployIfNotExists effects has all the subproperties that define the related resources to match and the template deployment to execute.

Deployment [required]

This property should include the full template deployment as it would be passed to the Microsoft.Resources/deployment

References:

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

QUESTION 2

HOTSPOT

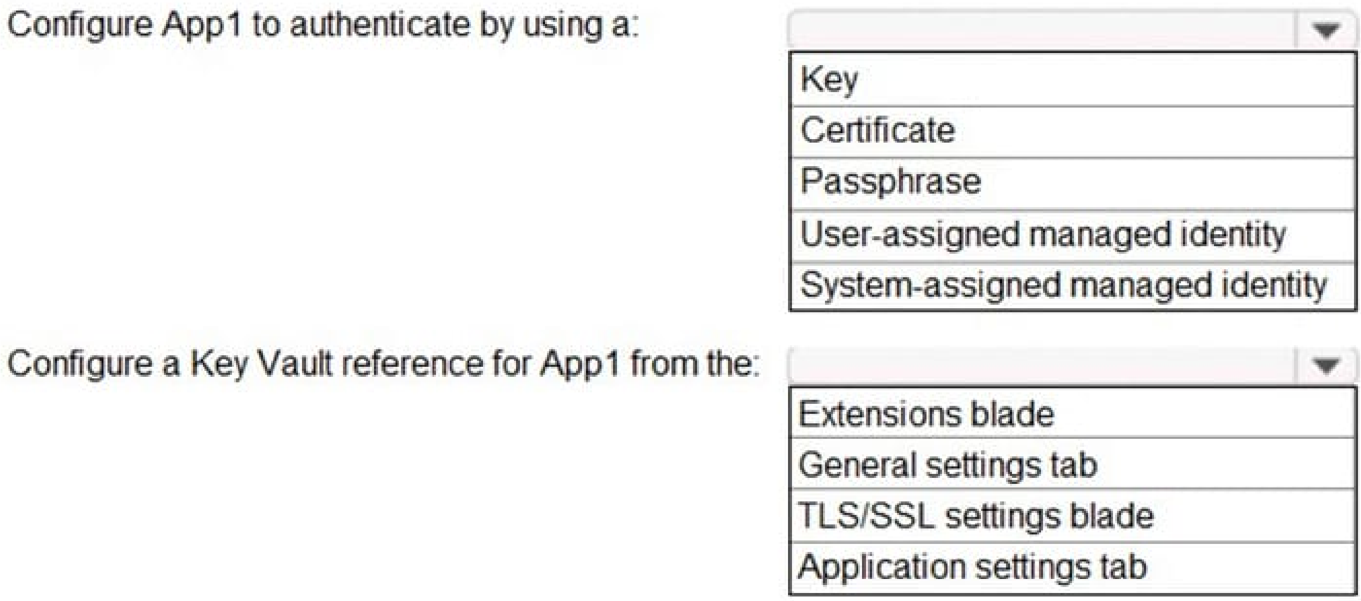
You have an Azure subscription that contains a web app named App1 and an Azure key vault named Vault1.

You need to configure App1 to store and access the secrets in Vault1.

How should you configure App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



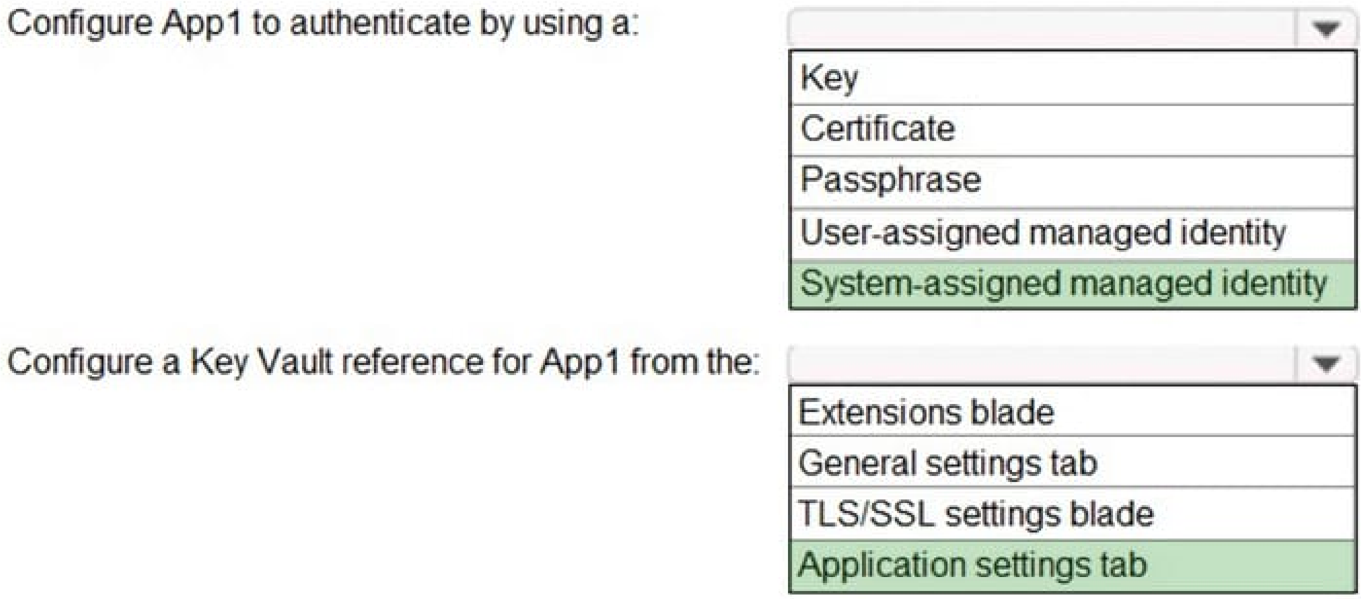
Configure App1 to authenticate by using a:

- Key
- Certificate
- Passphrase
- User-assigned managed identity
- System-assigned managed identity

Configure a Key Vault reference for App1 from the:

- Extensions blade
- General settings tab
- TLS/SSL settings blade
- Application settings tab

Correct Answer:



Configure App1 to authenticate by using a:

- Key
- Certificate
- Passphrase
- User-assigned managed identity
- [✓ System-assigned managed identity]

Configure a Key Vault reference for App1 from the:

- Extensions blade
- General settings tab
- TLS/SSL settings blade
- [✓ Application settings tab]

Reference: https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

QUESTION 3

You have been tasked with delegate administrative access to your company\\'s Azure key vault.

You have to make sure that a specific user is able to add and delete certificates in the key vault. You also have to make sure that access is assigned based on the principle of least privilege.

Which of the following options should you use to achieve your goal?

A. A key vault access policy

B. Azure policy

C. Azure AD Privileged Identity Management (PIM)

D. Azure DevOps

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

QUESTION 4

SIMULATION

You need to ensure that the AzureBackupReport log for the Vault1 Recovery Services vault is stored in the WS11641655 Azure Log Analytics workspace.

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

A. See the explanation below.

Correct Answer: A

1.

In the Azure portal, type Recovery Services Vaults in the search box, select Recovery Services Vaults from the search results then select Vault1. Alternatively, browse to Recovery Services Vaults in the left navigation pane.

2.

In the properties of Vault1, scroll down to the Monitoring section and select Diagnostic Settings.

3.

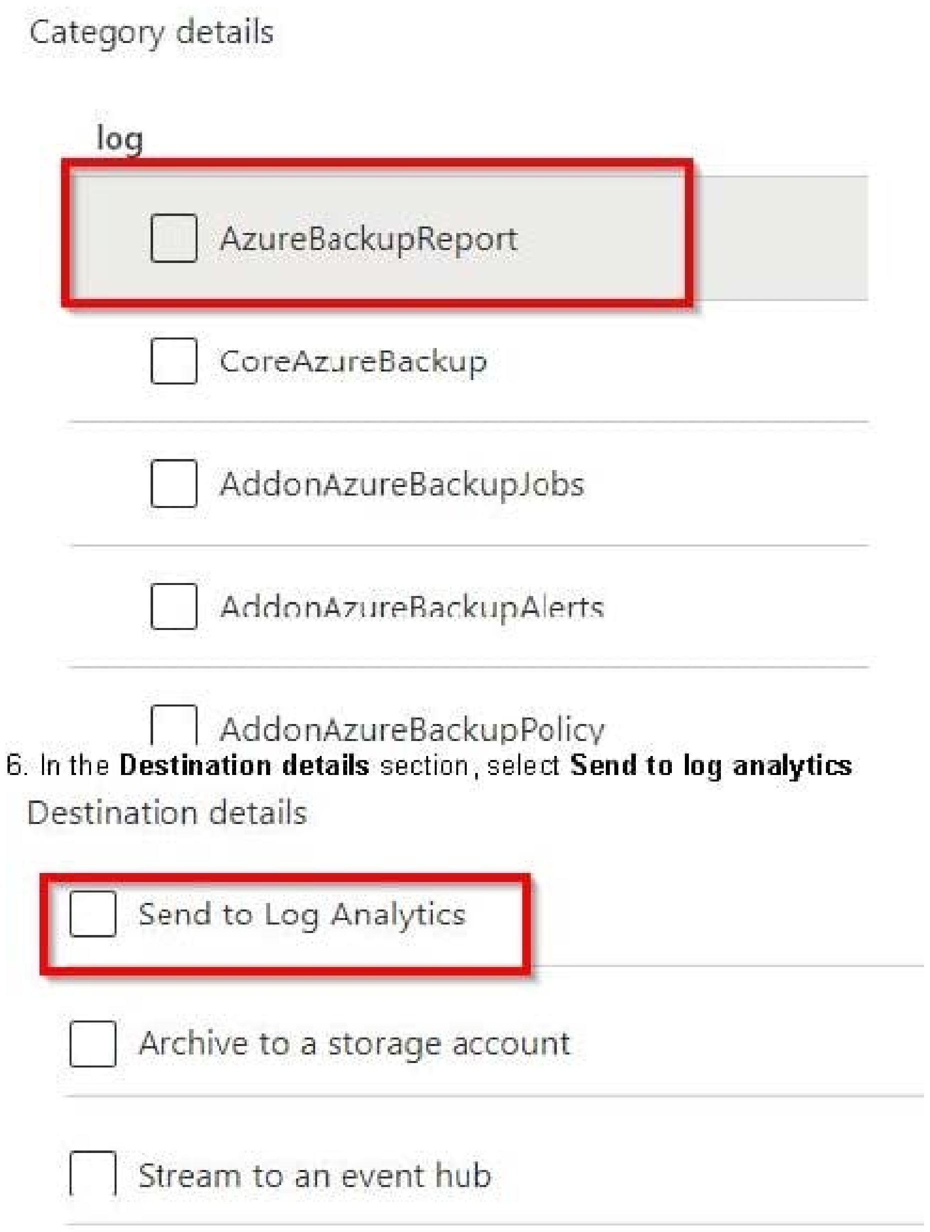
Click the Add a diagnostic setting link.

4.

Enter a name in the Diagnostic settings name box.

5.

In the Log section, select AzureBackupReport.



Category details

log

□ AzureBackupReport

□ CoreAzureBackup

□ AddonAzureBackupJobs

□ AddonAzureBackupAlerts

□ AddonAzureBackupPolicy

6. In the **Destination details** section, select **Send to log analytics**

Destination details

□ Send to Log Analytics

□ Archive to a storage account

□ Stream to an event hub

6. In the Destination details section, select Send to log analytics

7.

Select the WS11641655 Azure Log Analytics workspace.

8.

Click the Save button to save the changes.

Reference: https://docs.microsoft.com/en-us/azure/backup/backup-azure-diagnostic-events

QUESTION 5

HOTSPOT

You have an Azure subscription that contains the following resources:

1.

An Azure key vault

2.

An Azure SQL database named Database1

3.

Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1

You need to implement an encryption solution for Database1 that meets the following requirements:

1.

The data in a column named Discount in Database1 must be encrypted so that only AppSrv1 can decrypt the data.

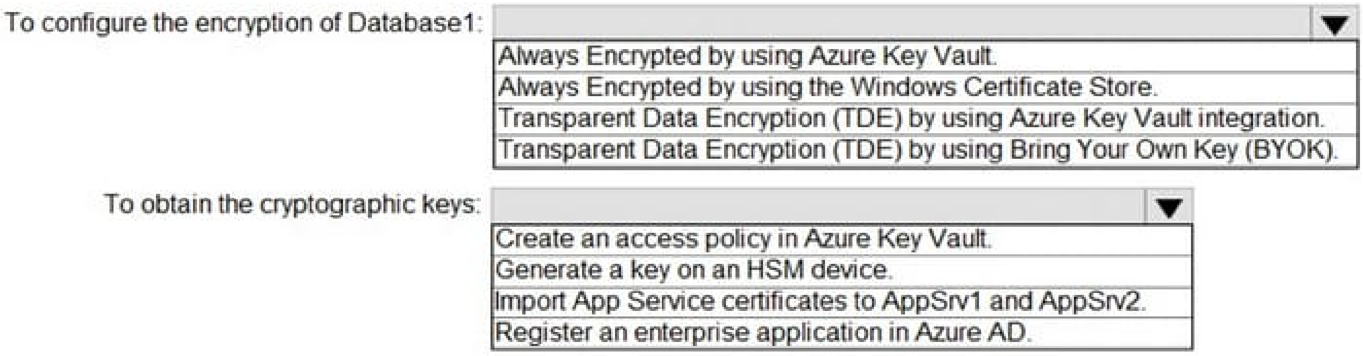
2.

AppSrv1 and AppSrv2 must be authorized by using managed identities to obtain cryptographic keys.

How should you configure the encryption settings for Database1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



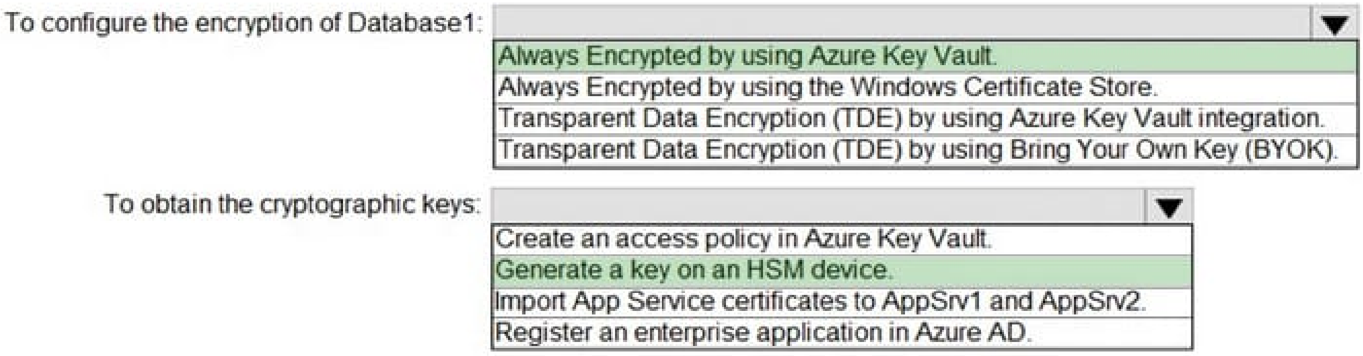
To configure the encryption of Database1:

- Always Encrypted by using Azure Key Vault.
- Always Encrypted by using the Windows Certificate Store.
- Transparent Data Encryption (TDE) by using Azure Key Vault integration.
- Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK).

To obtain the cryptographic keys:

- Create an access policy in Azure Key Vault.
- Generate a key on an HSM device.
- Import App Service certificates to AppSrv1 and AppSrv2.
- Register an enterprise application in Azure AD.

Correct Answer:



To configure the encryption of Database1:

- Always Encrypted by using Azure Key Vault.
- Always Encrypted by using the Windows Certificate Store.
- Transparent Data Encryption (TDE) by using Azure Key Vault integration.
- Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK).

To obtain the cryptographic keys:

- Create an access policy in Azure Key Vault.
- Generate a key on an HSM device.
- Import App Service certificates to AppSrv1 and AppSrv2.
- Register an enterprise application in Azure AD.

Reference: https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=azure-powershell

QUESTION 6

You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure SQL Database instance that is configured to support Azure AD authentication.

Database developers must connect to the database instance and authenticate by using their on-premises Active Directory account.

You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.

Which authentication method should you recommend?

A. Active Directory - Password

B. Active Directory - Universal with MFA support

C. SQL Server Authentication

D. Active Directory - Integrated

Correct Answer: D

Use Active Directory password authentication when connecting with an Azure AD principal name using the Azure AD managed domain.

Use this method to authenticate to SQL DB/DW with Azure AD for native or federated Azure AD users. A native user is one explicitly created in Azure AD and being authenticated using user name and password, while a federated user is a Windows user whose domain is federated with Azure AD. The latter method (using user and password) can be used when a user wants to use their windows credential, but their local machine is not joined with the domain (for example, using a remote access). In this case, a Windows user can indicate their domain account and password and can authenticate to SQL DB/DW using federated credentials.

Incorrect Answers:

D: Use Active Directory integrated authentication if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

References: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

QUESTION 7

You have an Azure subscription that uses Microsoft Defender for Cloud. You have an Amazon Web Services (AWS) account. You need to ensure that when you deploy a new AWS Elastic Compute Cloud (EC2) instance, the Microsoft Defender for Servers agent installs automatically. What should you configure first?

A. the classic cloud connector

B. the Azure Monitor agent

C. the Log Analytics agent

D. the native cloud connector

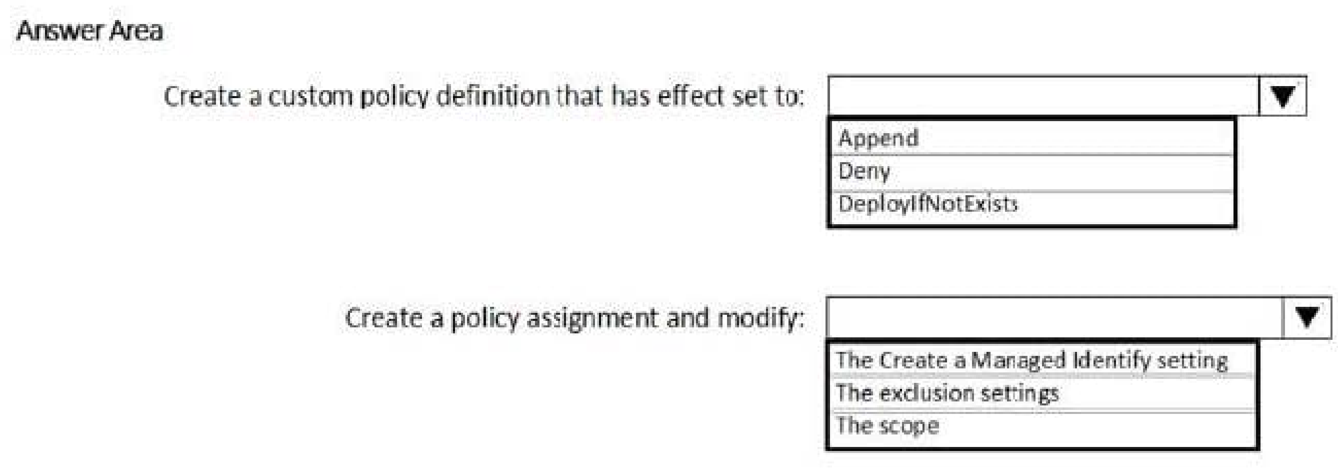
Correct Answer: D

Native cloud connector is the recommended way and provides an agentless connection to your AWS account that can extend with Defender for Cloud\\'s Defender plans to secure the AWS resources. https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings

QUESTION 8

You need to deploy Microsoft Antimalware to meet the platform protection requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

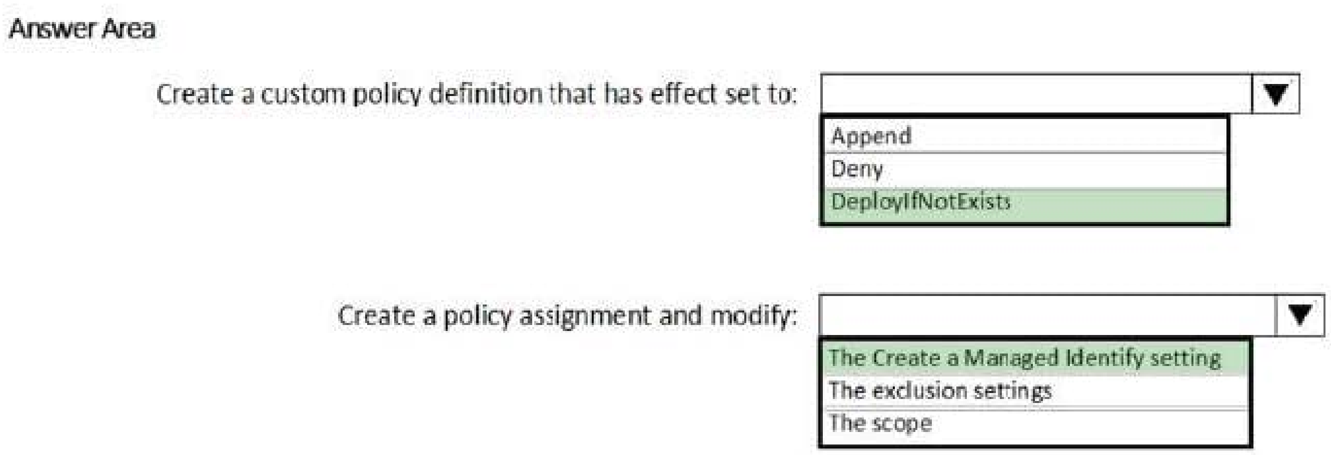
Create a custom policy definition that has effect set to:

- Append
- Deny
- DeployIfNotExists

Create a policy assignment and modify:

- The Create a Managed Identify setting
- The exclusion settings
- The scope

Correct Answer:



Answer Area

Create a custom policy definition that has effect set to: ▼

- Append
- Deny
- DeployIfNotExists

Create a policy assignment and modify: ▼

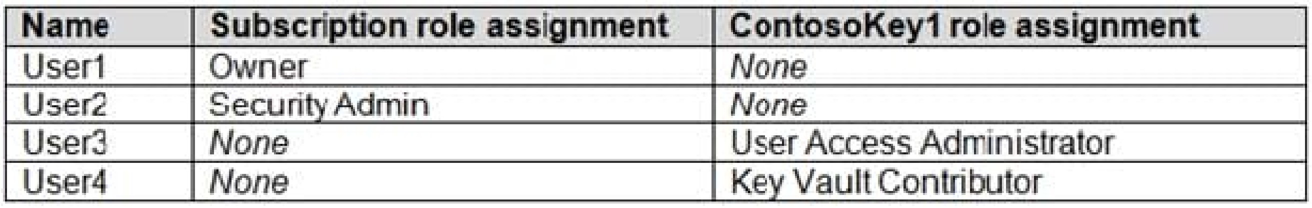
- The Create a Managed Identify setting
- The exclusion settings
- The scope

QUESTION 9

HOTSPOT

You have an Azure subscription that contains an Azure key vault named ContosoKey1.

You create users and assign them roles as shown in the following table.



Name	Subscription role assignment	ContosoKey1 role assignment
User1	Owner	*None*
User2	Security Admin	*None*
User3	*None*	User Access Administrator
User4	*None*	Key Vault Contributor

You need to identify which users can perform the following actions:

1.

Delegate permissions for ContsosKey1.

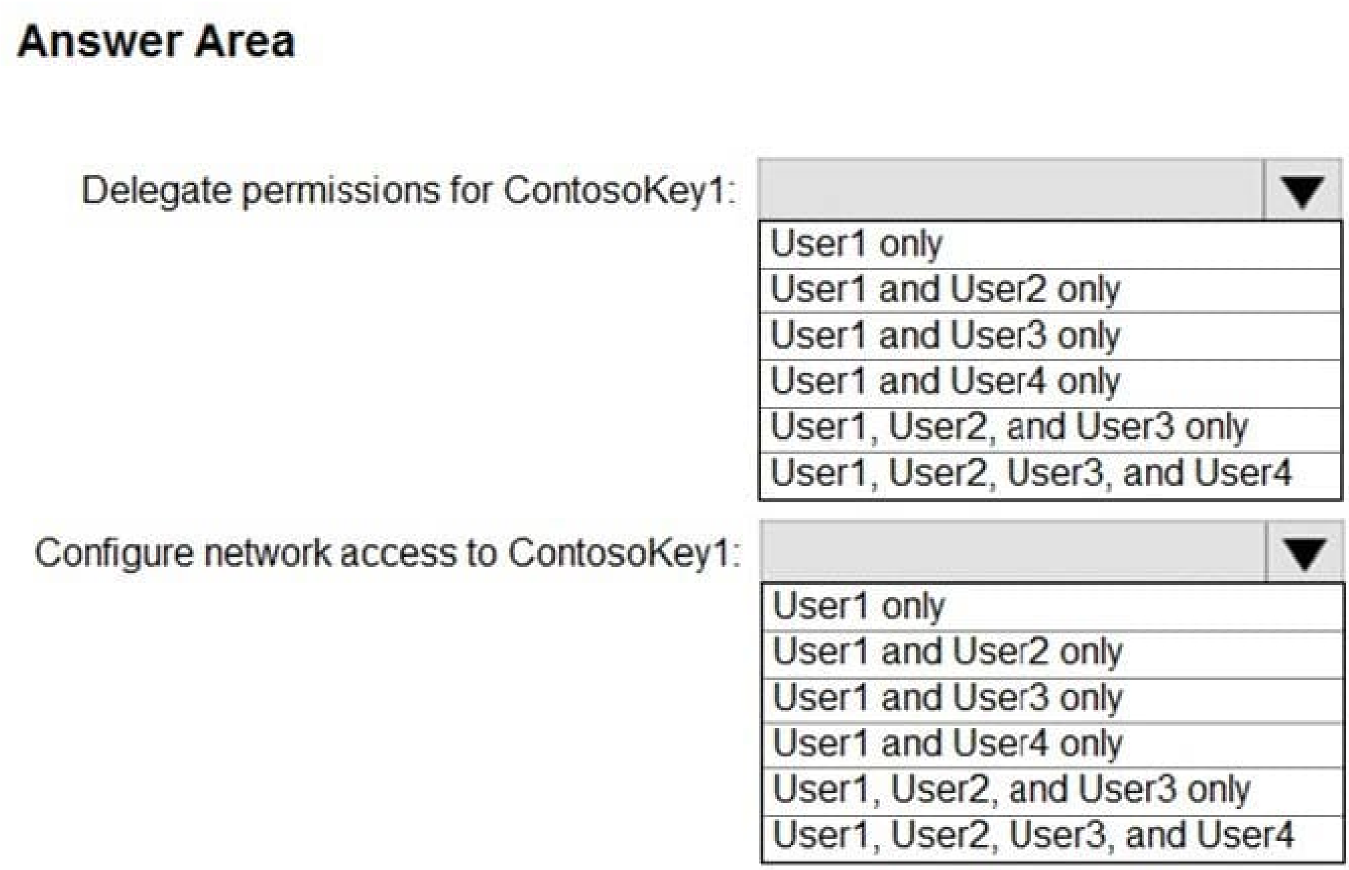
2.

Configure network access to ContosoKey1.

Which users should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

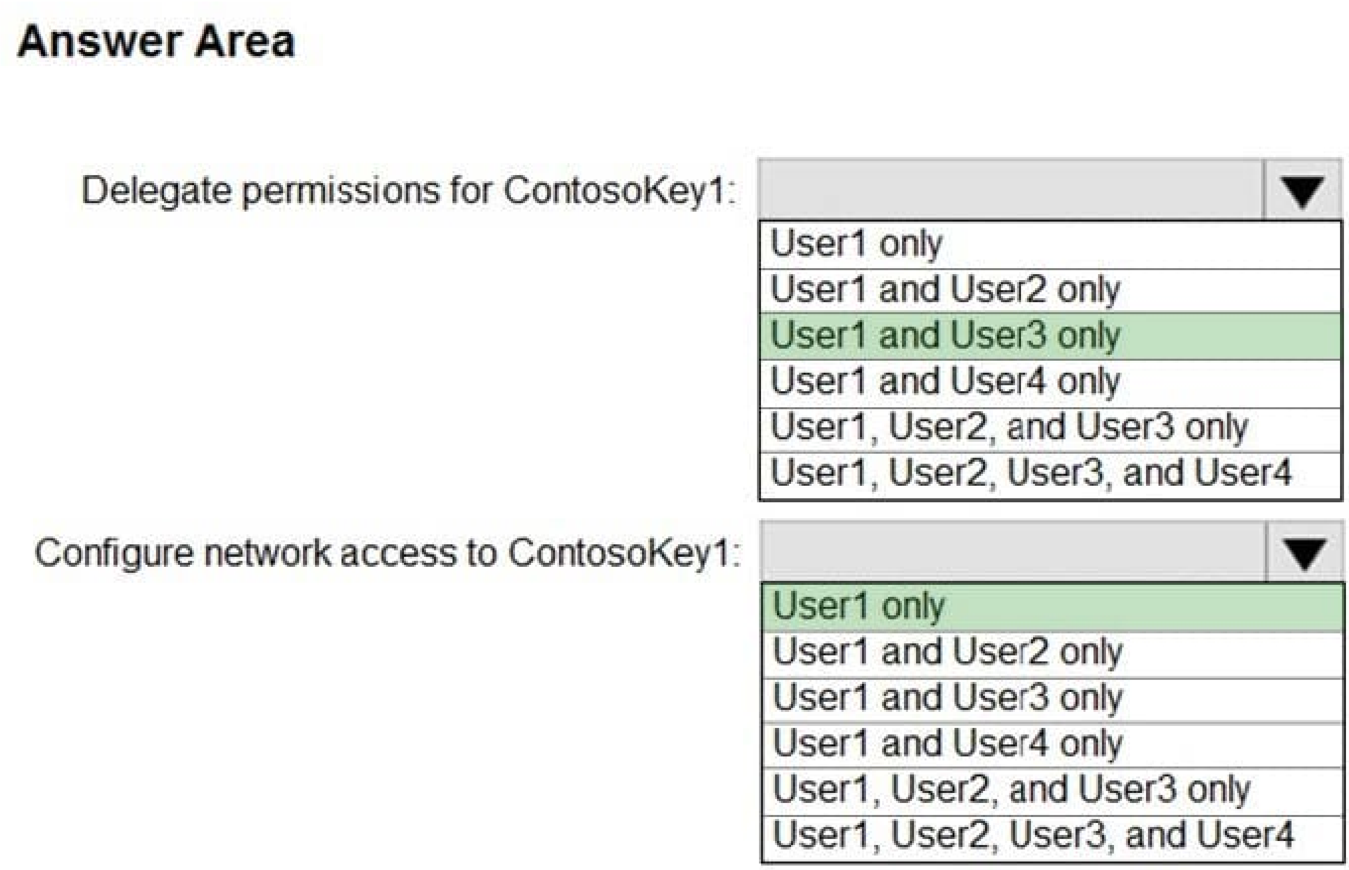
Delegate permissions for ContosoKey1: ▼

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1 and User4 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Configure network access to ContosoKey1: ▼

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1 and User4 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Correct Answer:



Answer Area

Delegate permissions for ContosoKey1:

- User1 only
- User1 and User2 only
- [✓ User1 and User3 only]
- User1 and User4 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Configure network access to ContosoKey1:

- [✓ User1 only]
- User1 and User2 only
- User1 and User3 only
- User1 and User4 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Reference: https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide

QUESTION 10

Your company recently created an Azure subscription. You have, subsequently, been tasked with making sure that you are able to secure Azure AD roles by making use of Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

Which of the following actions should you take FIRST?

A. You should sign up Azure Active Directory (Azure AD) Privileged Identity Management (PIM) for Azure AD roles.

B. You should consent to Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

C. You should discover privileged roles.

D. You should discover resources.

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

QUESTION 11

You have an Azure subscription.

You create an Azure web app named Contoso1812 that uses an S1 App service plan.

You create a DNS record for www.contoso.com that points to the IP address of Contoso1812.

You need to ensure that users can access Contoso1812 by using the https://www.contoso.com URL.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Turn on the system-assigned managed identity for Contoso1812.

B. Add a hostname to Contoso1812.

C. Scale out the App Service plan of Contoso1812.

D. Add a deployment slot to Contoso1812.

E. Scale up the App Service plan of Contoso1812.

F. Upload a PFX file to Contoso1812.

Correct Answer: BF

B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either www.contoso.com or contoso.com as a fully qualified domain name

(FQDN).

To do this, you have to create three records:

A root "A" record pointing to contoso.com

A root "TXT" record for verification

A "CNAME" record for the www name that points to the A record

E: To map a custom DNS name to a web app, the web app\\'s App Service plan must be a paid tier (Shared, Basic, Standard, Premium or Consumption for Azure Functions). I

Scale up the App Service plan: Select any of the non-free tiers (D1, B1, B2, B3, or any tier in the Production category).

References:

https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain

QUESTION 12

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Azure subscription that includes an Azure key vault. You have previously created a secret in the key vault.

After an application developer registers an application in Azure Active Directory (Azure AD), you are instructed to make sure that the application is able to use the secret you created.

Solution: You should create a key in Azure Key Vault.

Does the solution meet the goal?

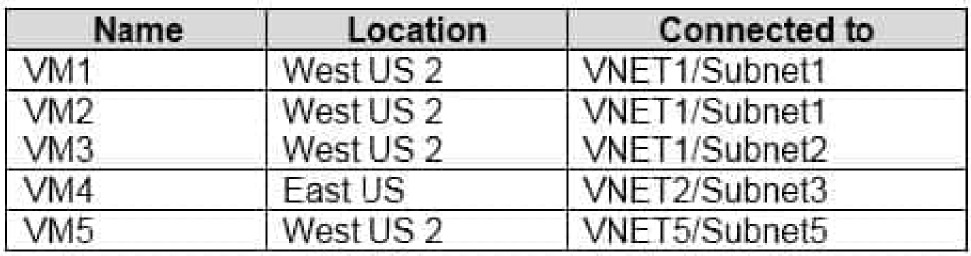
A. Yes

B. No

Correct Answer: B

QUESTION 13

You have the Azure virtual machines shown in the following table.



Name	Location	Connected to
VM1	West US 2	VNET1/Subnet1
VM2	West US 2	VNET1/Subnet1
VM3	West US 2	VNET1/Subnet2
VM4	East US	VNET2/Subnet3
VM5	West US 2	VNET5/Subnet5

Each virtual machine has a single network interface.

You add the network interface of VM1 to an application security group named ASG1.

You need to identify the network interfaces of which virtual machines you can add to ASG1.

What should you identify?

A. VM2 only

B. VM2, VM3, VM4, and VM5

C. VM2, VM3, and VM5 only

D. VM2 and VM3 only

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups

QUESTION 14

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You create a new stored access policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Shared access signatures provides access to a particular resource such as blog. Stored access policies are a group of Shared Access Signatures (SAS). In order to revoke access to a SAS you can either:

1.

Rotate the Key1 or Key 2, that is the access keys used to sign the SAS. Rotating the access keys used to sign the SAS, invalidates any previously signed SAS hence revoking the SAS issused before

2.

Remove the stored access policy which an SAS is linked to. If a Stored Access Policy is removed, it also invalidates the SASs liked to the Stored Access Policy.

QUESTION 15

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create an initiative and an assignment that is scoped to a management group.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/azure/governance/policy/overview