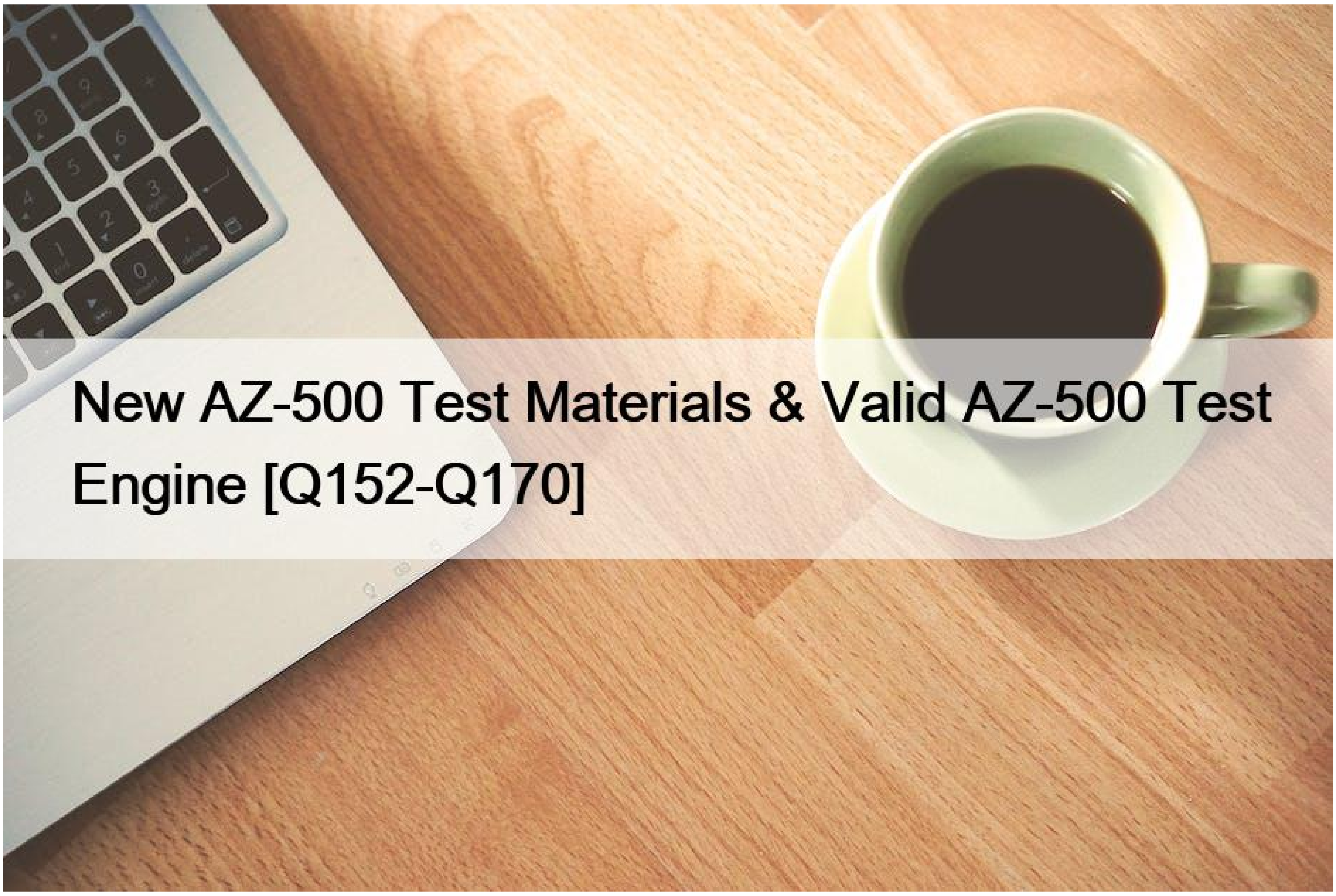
New AZ-500 Test Materials & Valid AZ-500 Test Engine [Q152-Q170


New AZ-500 Test Materials & Valid AZ-500 Test Engine [Q152-Q170]

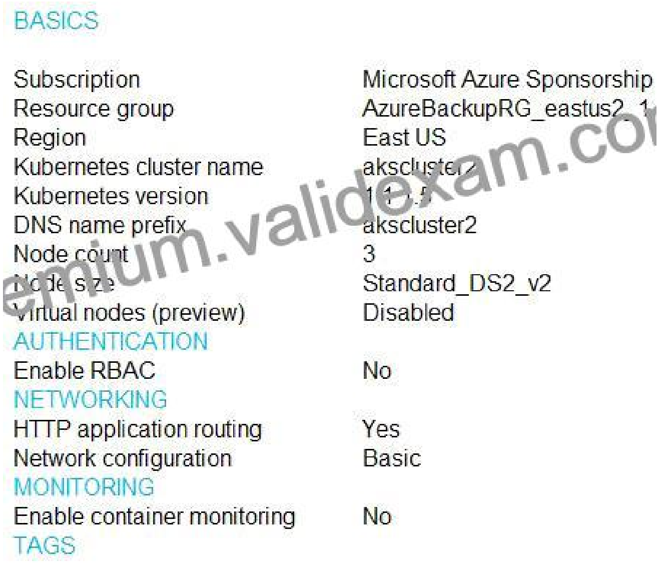
New AZ-500 Test Materials & Valid AZ-500 Test Engine
AZ-500 Updated Exam Dumps [2024] Practice Valid Exam Dumps Question

Microsoft AZ-500 certification exam is designed for professionals who want to demonstrate their skills in implementing security controls, maintaining security posture, and identifying and remediating vulnerabilities in the Microsoft Azure cloud platform. AZ-500 exam measures the candidate's ability to secure applications, data, and identities in the cloud environment using various security tools and services provided by Microsoft.

How to Start Reviewing the Microsoft AZ-500 Exam **Get the exam guide for Alibaba Cloud Certification Alibaba Cloud Certification: Tips to survive if you don't have time to read all the pages**
The Microsoft AZ-500 certification exam is the standard qualification required by many employers. The exam tests your skills in Microsoft Word, Excel, PowerPoint, Outlook, and more. It also covers an introduction to Microsoft Azure. This article gives you all the details on what this exam is about so that you can prepare for it with confidence. **Microsoft AZ-500 exam dumps** are also available to help you develop your skills further.

NO.152 You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit.

(Click the Exhibit tab.)



BASICS	
Subscription	Microsoft Azure Sponsorship
Resource group	AzureBackupRG_eastus2_1
Region	East US
Kubernetes cluster name	akscluster2
Kubernetes version	1.11.5
DNS name prefix	akscluster2
Node count	3
Node size	Standard_DS2_v2
Virtual nodes (preview)	Disabled
AUTHENTICATION	
Enable RBAC	No
NETWORKING	
HTTP application routing	Yes
Network configuration	Basic
MONITORING	
Enable container monitoring	No
TAGS	

You plan to deploy the cluster to production. You disable HTTP application routing.

You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.

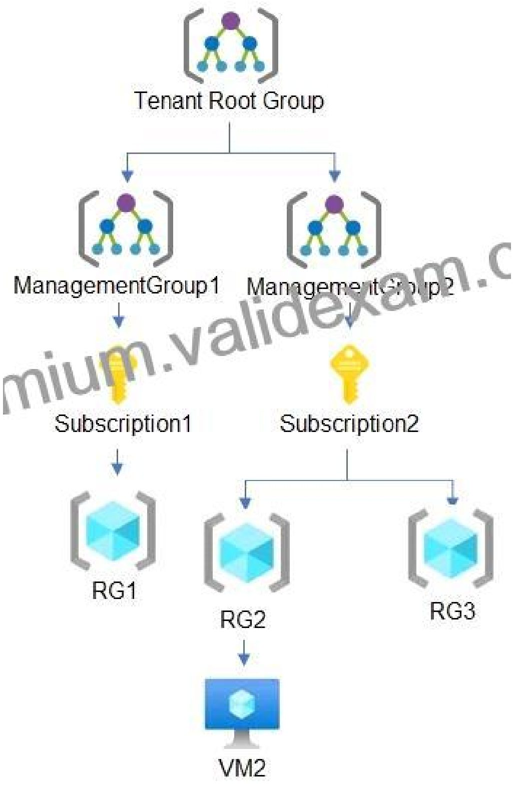
What should you do?
* Create an AKS Ingress controller.
* Install the container network interface (CNI) plug-in.
* Create an Azure Standard Load Balancer.
* Create an Azure Basic Load Balancer.
Explanation

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

References:

https://docs.microsoft.com/en-us/azure/aks/ingress-tls

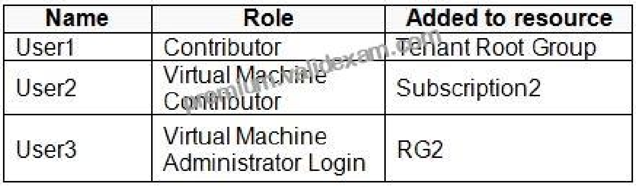
NO.153 You have the hierarchy of Azure resources shown in the following exhibit.



RG1, RG2, and RG3 are resource groups.

RG2 contains a virtual machine named VM1.

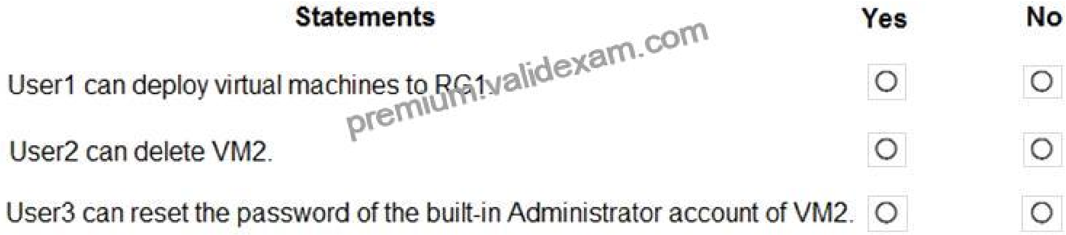
You assign role-based access control (RBAC) roles to the users shown in the following table.



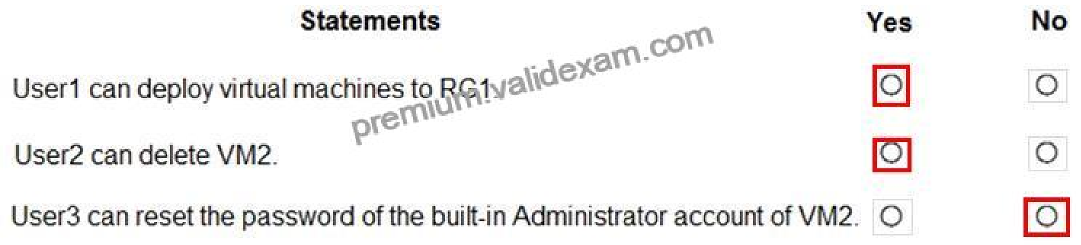
Name	Role	Added to resource
User1	Contributor	Tenant Root Group
User2	Virtual Machine Contributor	Subscription2
User3	Virtual Machine Administrator Login	RG2

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

NOTE: Each correct selection is worth one point.



Statements	Yes	No
User1 can deploy virtual machines to RG1.	○	○
User2 can delete VM2.	○	○
User3 can reset the password of the built-in Administrator account of VM2.	○	○



Statements	Yes	No
User1 can deploy virtual machines to RG1.	[✓ ○]	○
User2 can delete VM2.	[✓ ○]	○
User3 can reset the password of the built-in Administrator account of VM2.	○	[✓ ○]

NO.154 You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

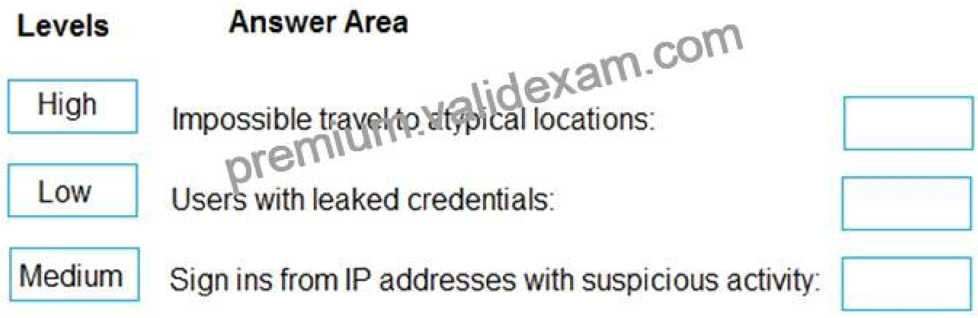
Users with leaked credentials

Impossible travel to atypical locations

Sign ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level 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.

NOTE: Each correct selection is worth one point.



Levels

High

Low

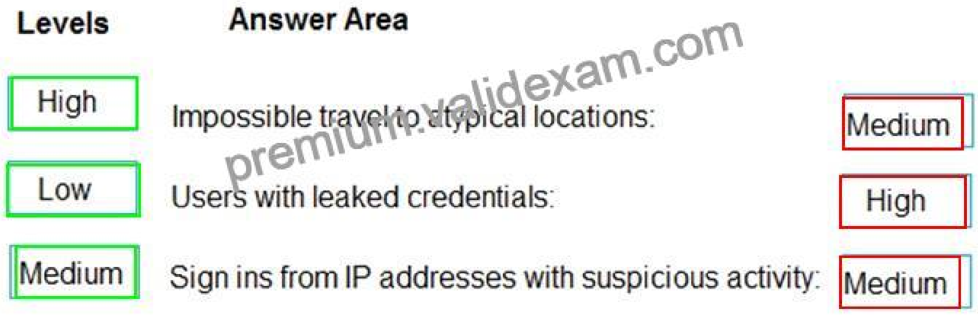
Medium

Answer Area

Impossible travel to atypical locations:

Users with leaked credentials:

Sign ins from IP addresses with suspicious activity:



Levels

High

Low

Medium

Answer Area

Impossible travel to atypical locations: Medium

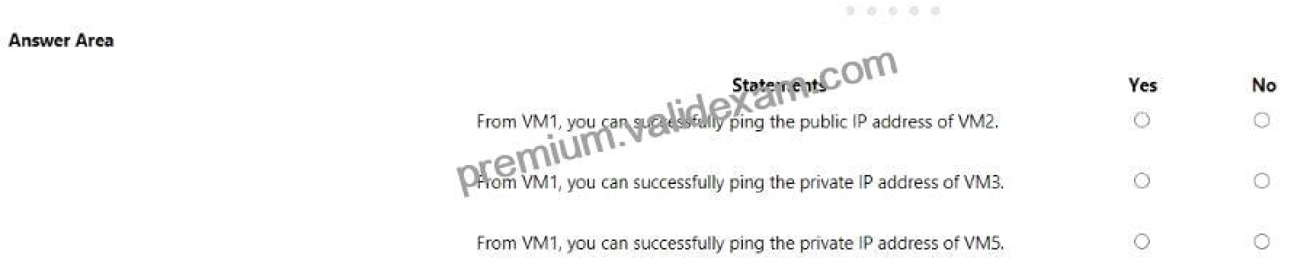
Users with leaked credentials: High

Sign ins from IP addresses with suspicious activity: Medium

NO.155 You ate evaluating the security of the network communication between the virtual machines in Sub2.

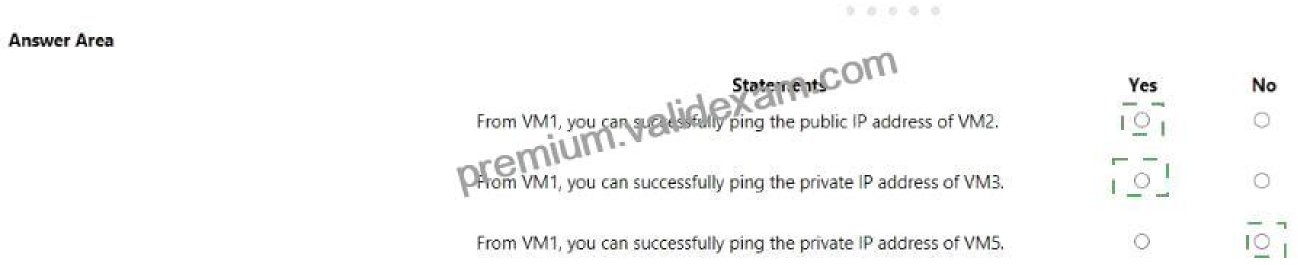
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Answer Area

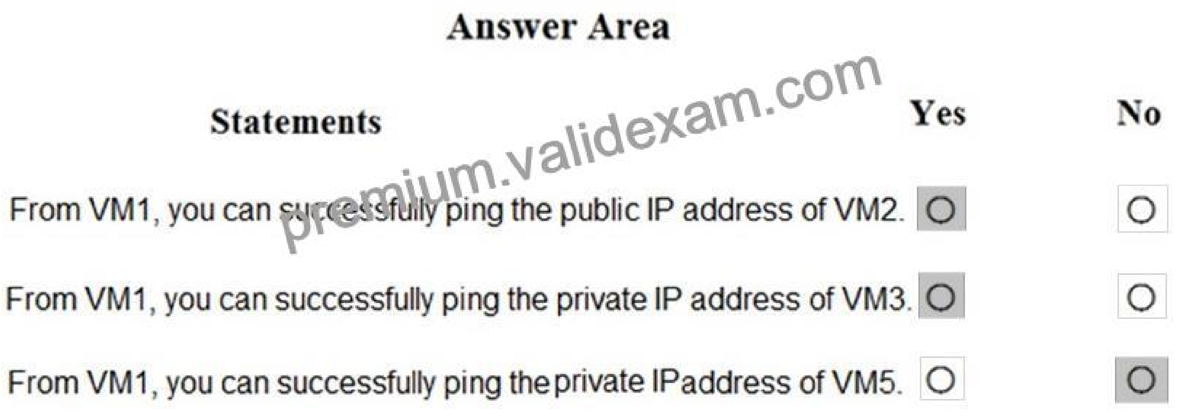
Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	○	○
From VM1, you can successfully ping the private IP address of VM3.	○	○
From VM1, you can successfully ping the private IP address of VM5.	○	○



Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	●	○
From VM1, you can successfully ping the private IP address of VM3.	●	○
From VM1, you can successfully ping the private IP address of VM5.	○	●

Explanation



Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	●	○
From VM1, you can successfully ping the private IP address of VM3.	●	○
From VM1, you can successfully ping theprivate IPaddress of VM5.	○	●

NO.156 From the Azure portal, you are configuring an Azure policy.

You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.

Which effect requires a managed identity for the assignment?

AuditIfNotExist
*
* Append

DeployIfNotExist
*
* Deny
Section: [none]

Explanation:

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.

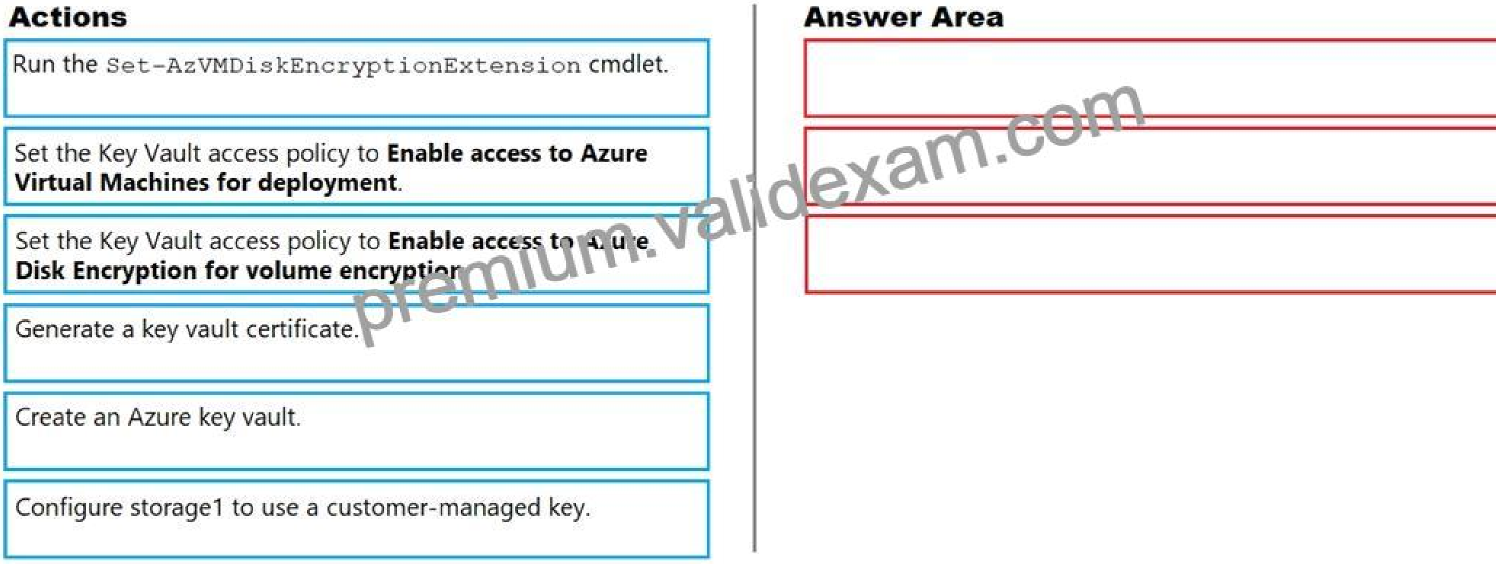
References:

https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

NO.157 You have an Azure Storage account named storage1 and an Azure virtual machine named VM1. VM1 has a premium SSD managed disk.

You need to enable Azure Disk Encryption for VM1.

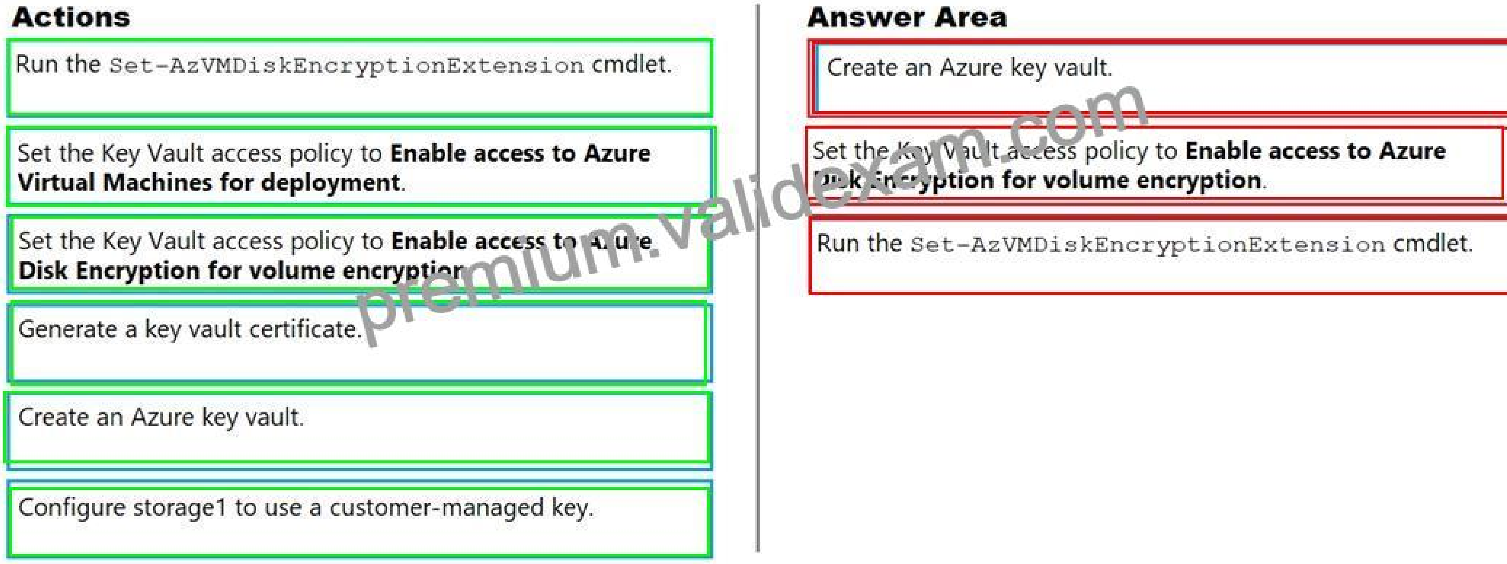
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange then in the correct order.



Actions

- Run the `Set-AzVMDiskEncryptionExtension` cmdlet.
- Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.
- Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.
- Generate a key vault certificate.
- Create an Azure key vault.
- Configure storage1 to use a customer-managed key.

Answer Area



Actions

- Run the `Set-AzVMDiskEncryptionExtension` cmdlet.
- Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.
- Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.
- Generate a key vault certificate.
- Create an Azure key vault.
- Configure storage1 to use a customer-managed key.

Answer Area

- Create an Azure key vault.
- Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.
- Run the `Set-AzVMDiskEncryptionExtension` cmdlet.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

NO.158 You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1 and a playbook named Playbook1.

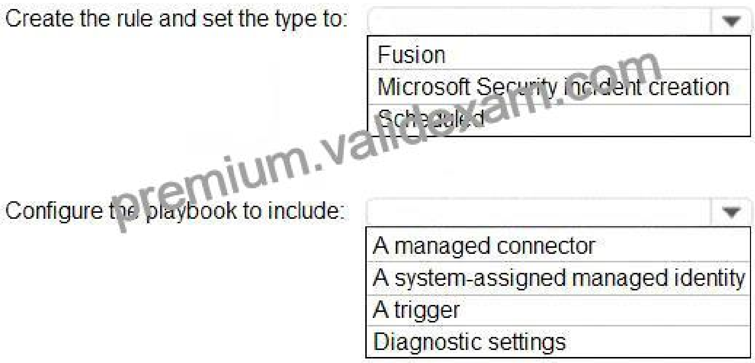
Query1 returns a subset of security events generated by Azure AD.

You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1.

You need to ensure that you can add Playbook1 to the new rule.

What should you do? To answer, select the appropriate options in the answer area.

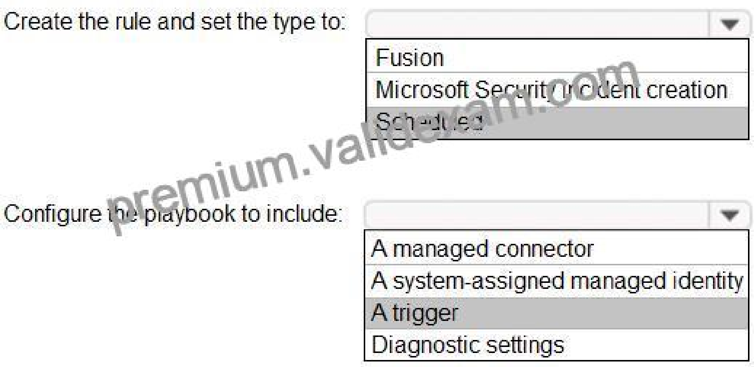
NOTE: Each correct selection is worth one point.



Create the rule and set the type to:
- Fusion
- Microsoft Security incident creation
- Scheduled

Configure the playbook to include:
- A managed connector
- A system-assigned managed identity
- A trigger
- Diagnostic settings

Explanation



Create the rule and set the type to:

- Fusion
- Microsoft Security incident creation
- [✓ Scheduled]

Configure the playbook to include:

- A managed connector
- A system-assigned managed identity
- [✓ A trigger]
- Diagnostic settings

Reference:

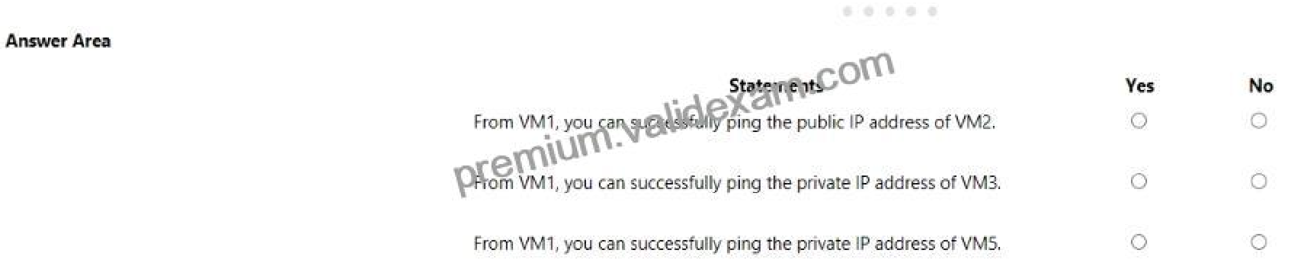
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

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

NO.159 You are evaluating the security of the network communication between the virtual machines in Sub2.

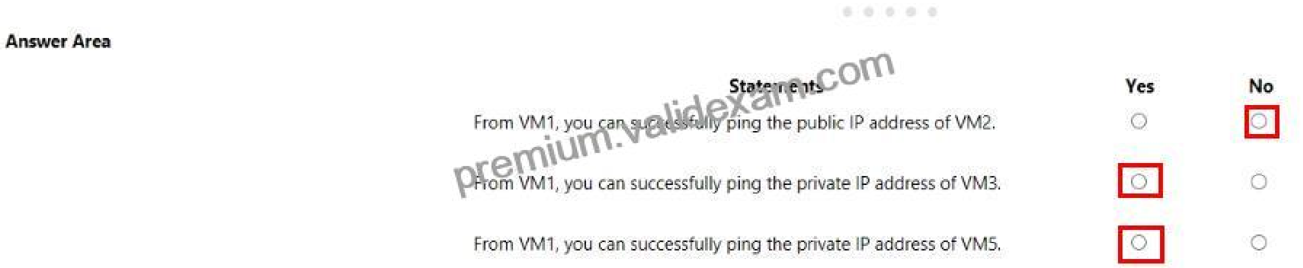
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	○	○
From VM1, you can successfully ping the private IP address of VM3.	○	○
From VM1, you can successfully ping the private IP address of VM5.	○	○



Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	○	[✓ ○]
From VM1, you can successfully ping the private IP address of VM3.	[✓ ○]	○
From VM1, you can successfully ping the private IP address of VM5.	[✓ ○]	○

NO.160 You have an Azure subscription that contains the following resources:

* An Azure key vault

* An Azure SQL database named Database1

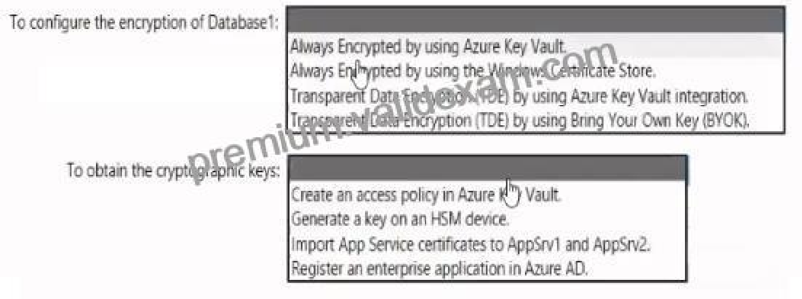
* Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1 You need to implement an encryption solution for Database1 that meets the following requirements:

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

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

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

NOTE: Each correct selection is worth one point

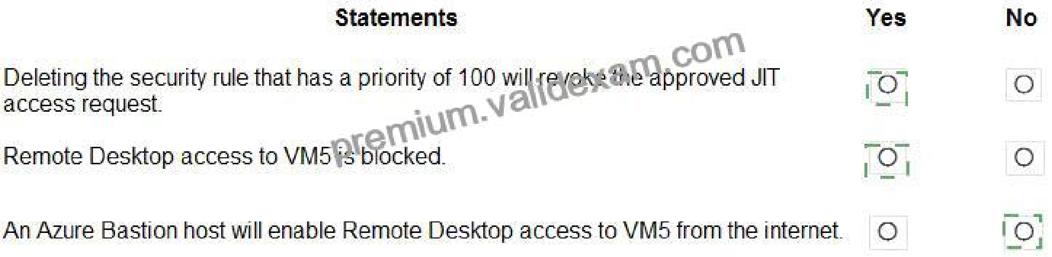


To configure the encryption of Database1:

- 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:

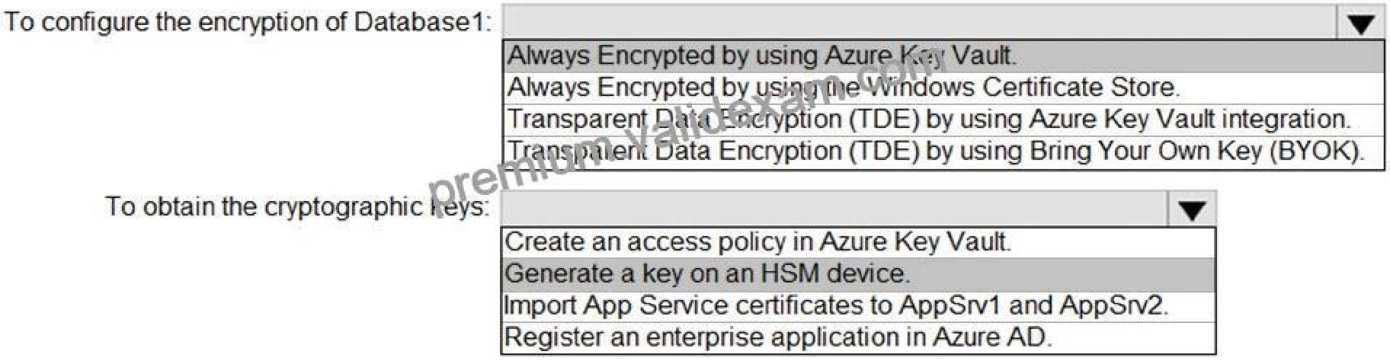
- Create an access policy in Azure Key Vault.
- Generate a key on an HSM device.
- Import App Service certificates to AppSrv1 and AppSrv2.
- Register an enterprise application in Azure AD.



Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	[✓ ○]	○
Remote Desktop access to VM5 is blocked.	[✓ ○]	○
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	○	[✓ ○]

Explanation

Text Description automatically generated with medium confidence



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).

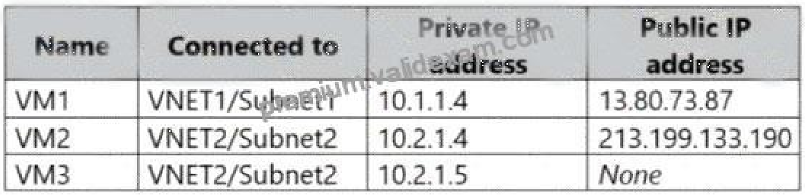
To obtain the cryptographic keys:

- 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=azu

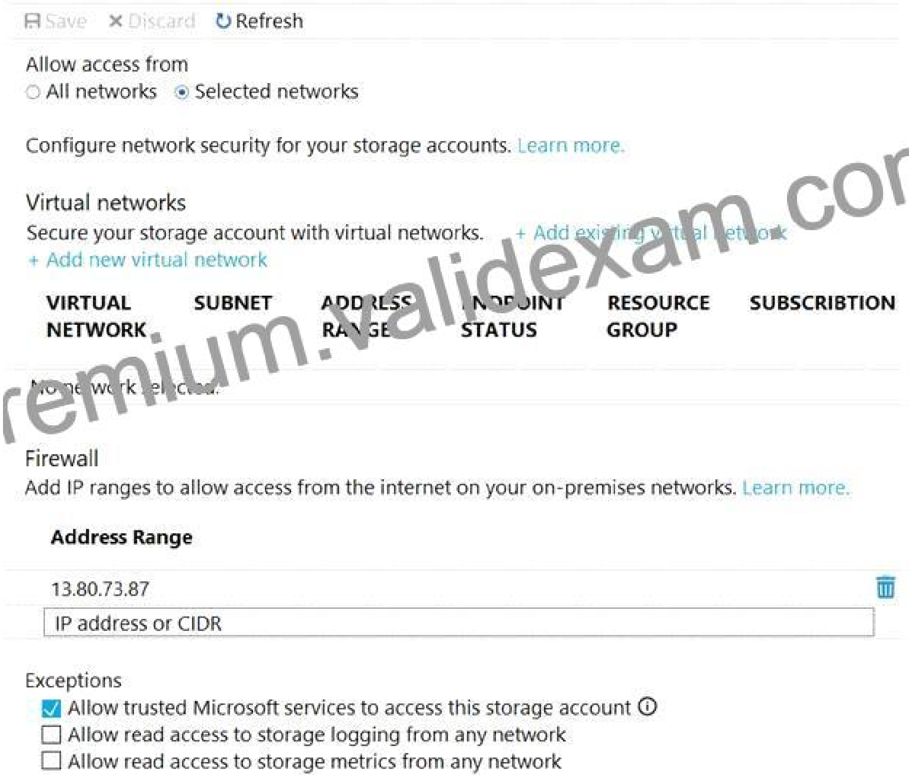
NO.161 You have an Azure subscription that contains the virtual machines shown in the following table.



Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.4	13.80.73.87
VM2	VNET2/Subnet2	10.2.1.4	213.199.133.190
VM3	VNET2/Subnet2	10.2.1.5	*None*

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.

You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.



Allow access from

○ All networks ● Selected networks

Configure network security for your storage accounts. Learn more.

Virtual networks

Secure your storage account with virtual networks. + Add existing virtual network
+ Add new virtual network

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIBTION
No network selected.					

Firewall

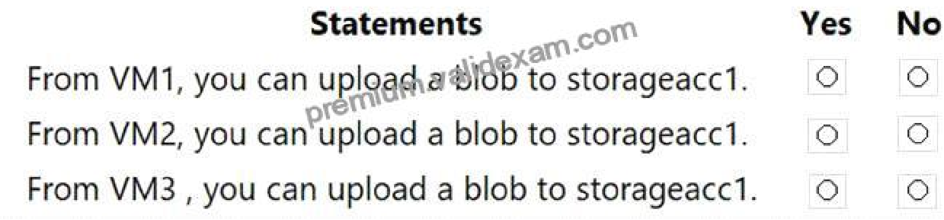
Add IP ranges to allow access from the internet on your on-premises networks. Learn more.

Address Range
13.80.73.87
IP address or CIDR

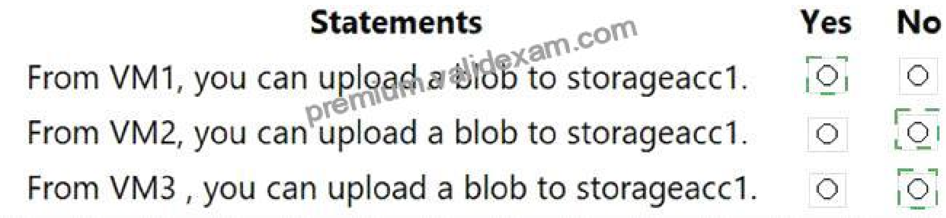
Exceptions

☑ Allow trusted Microsoft services to access this storage account ⓘ
☐ Allow read access to storage logging from any network
☐ Allow read access to storage metrics from any network

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

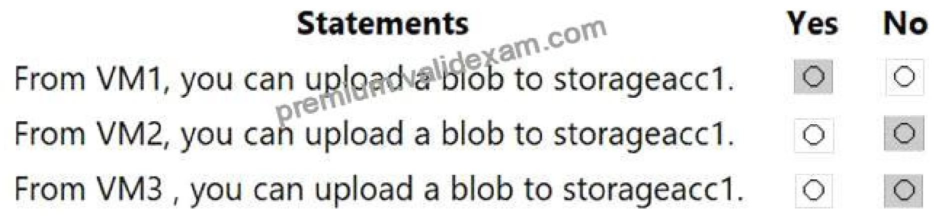


Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	○	○
From VM2, you can upload a blob to storageacc1.	○	○
From VM3 , you can upload a blob to storageacc1.	○	○



Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	○	○
From VM2, you can upload a blob to storageacc1.	○	○
From VM3 , you can upload a blob to storageacc1.	○	○

Explanation



Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	●	○
From VM2, you can upload a blob to storageacc1.	○	●
From VM3 , you can upload a blob to storageacc1.	○	●

Box 1: Yes

The public IP of VM1 is allowed through the firewall.

Box 2: No

The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.

Box 3: No

The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over the Internet.

Reference:

https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security

NO.162 You have an Azure subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

A PIM user that is assigned the User Access Administrator role reports receiving an authorization error when performing a role assignment or viewing the list of assignments.

You need to resolve the issue by ensuring that the PIM service principal has the correct permissions for the subscription. The solution must use the principle of least privilege.

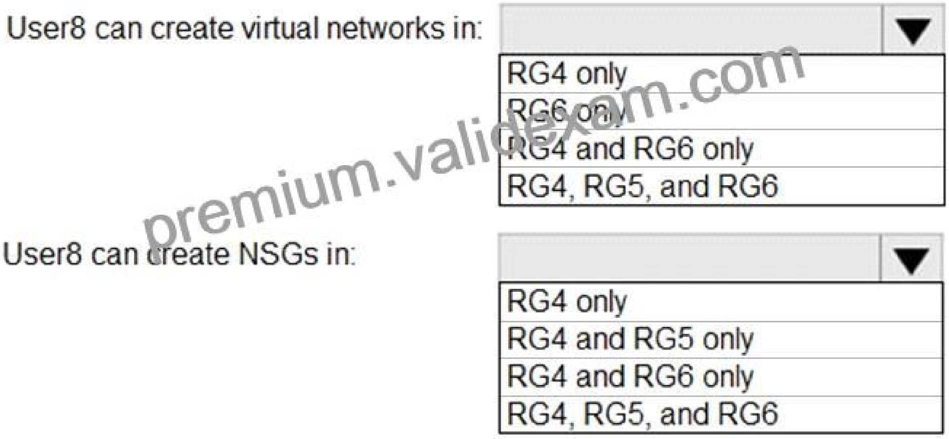
Which role should you assign to the PIM service principle?
* Contributor
* User Access Administrator

* Managed Application Operator
* Resource Policy Contributor

NO.163 You assign User8 the Owner role for RG4, RG5, and RG6.

In which resource groups can User8 create virtual networks and NSGs? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

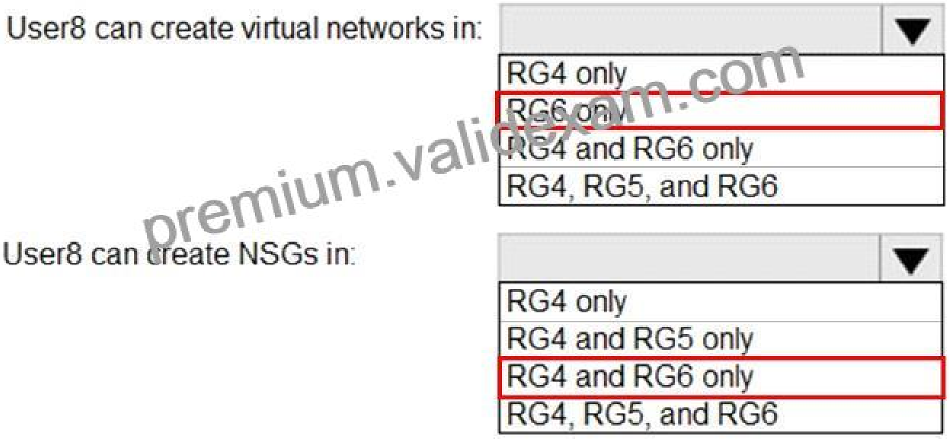


User8 can create virtual networks in:

- RG4 only
- RG6 only
- RG4 and RG6 only
- RG4, RG5, and RG6

User8 can create NSGs in:

- RG4 only
- RG4 and RG5 only
- RG4 and RG6 only
- RG4, RG5, and RG6



User8 can create virtual networks in:

- RG4 only
- [✓ RG6 only]
- RG4 and RG6 only
- RG4, RG5, and RG6

User8 can create NSGs in:

- RG4 only
- RG4 and RG5 only
- [✓ RG4 and RG6 only]
- RG4, RG5, and RG6

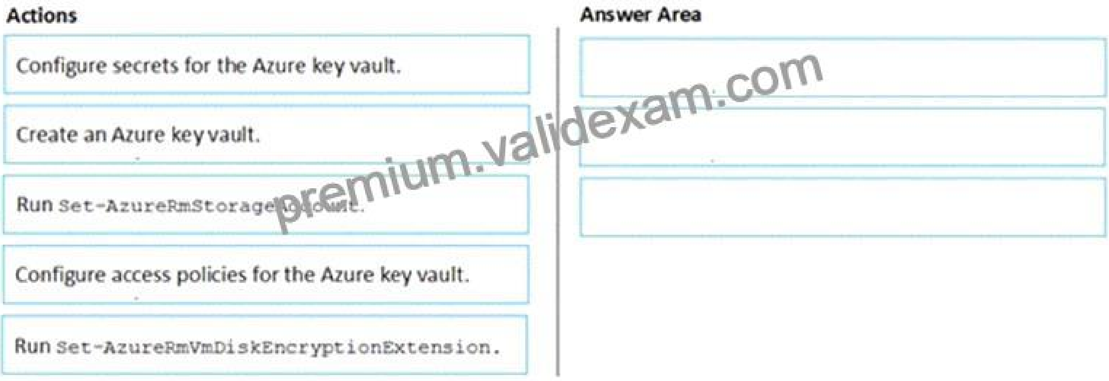
NO.164 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.

You need to encrypt VM1 disks by using Azure Disk Encryption.

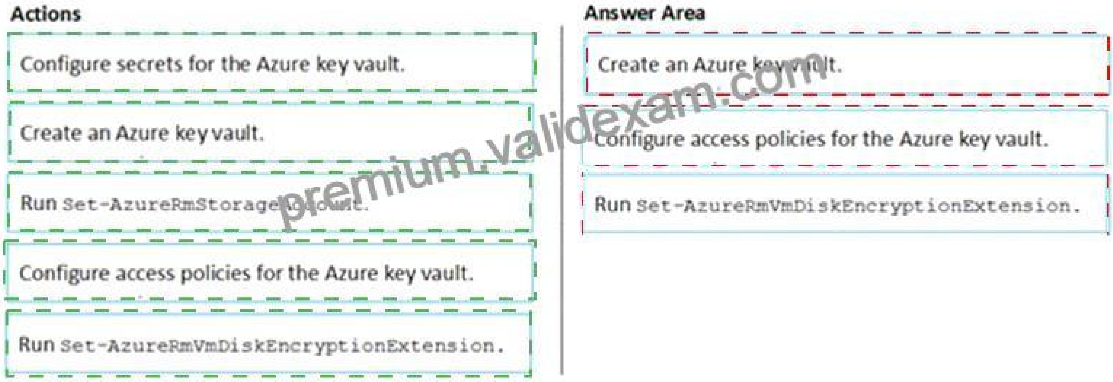
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

- Configure secrets for the Azure key vault.
- Create an Azure key vault.
- Run `Set-AzureRmStorageAccount.`
- Configure access policies for the Azure key vault.
- Run `Set-AzureRmVmDiskEncryptionExtension.`

Answer Area



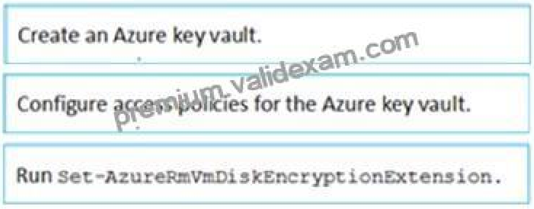
Actions

- Configure secrets for the Azure key vault.
- Create an Azure key vault.
- Run `Set-AzureRmStorageAccount.`
- Configure access policies for the Azure key vault.
- Run `Set-AzureRmVmDiskEncryptionExtension.`

Answer Area

- Create an Azure key vault.
- Configure access policies for the Azure key vault.
- Run `Set-AzureRmVmDiskEncryptionExtension.`

Explanation

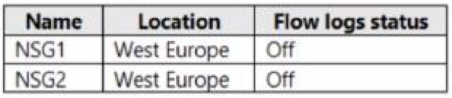


- Create an Azure key vault.
- Configure access policies for the Azure key vault.
- Run `Set-AzureRmVmDiskEncryptionExtension.`

References:

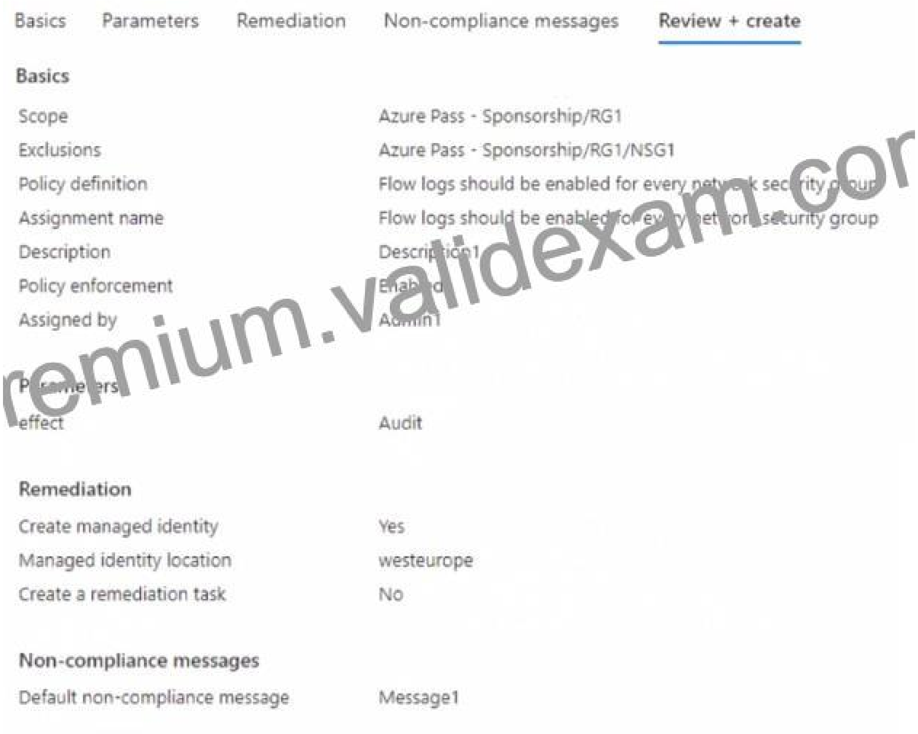
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/encrypt-disks

NO.165 You have an Azure subscription that contains a resource group named RG1 and the network security groups (NSGs) shown in the following table.



Name	Location	Flow logs status
NSG1	West Europe	Off
NSG2	West Europe	Off

You create the Azure policy shown in the following exhibit.



Basics

Scope	Azure Pass - Sponsorship/RG1
Exclusions	Azure Pass - Sponsorship/RG1/NSG1
Policy definition	Flow logs should be enabled for every network security group
Assignment name	Flow logs should be enabled for every network security group
Description	Description1
Policy enforcement	Enabled
Assigned by	Admin1

Parameters

effect	Audit

Remediation

Create managed identity	Yes
Managed identity location	westeurope
Create a remediation task	No

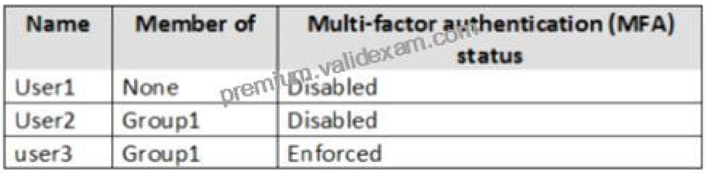
Non-compliance messages

Default non-compliance message	Message1

You assign the policy to RG1.

What will occur if you assign the policy to NSG1 and NSG2?
* Flow logs will be enabled for NSG1 and NSG2.
* Flow logs will be enabled for NSG2 only.
* Flow logs will be disabled for NSG1 and NSG2.
* Flow logs will be enabled for NSG1 only.

NO.166 You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.



Name	Member of	Multi-factor authentication (MFA) status
User1	None	Disabled
User2	Group1	Disabled
user3	Group1	Enforced

Azure AD Privileged Identity Management (PIM) is enabled for the tenant.

In PIM, the Password Administrator role has the following settings:

Maximum activation duration (hours): 2

Send email notifying admins of activation: Disable

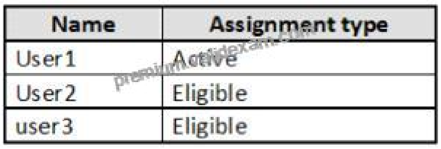
Require incident/request ticket number during activation: Disable

Require Azure Multi-Factor Authentication for activation: Enable

Require approval to activate this role: Enable

Selected approver: Group1

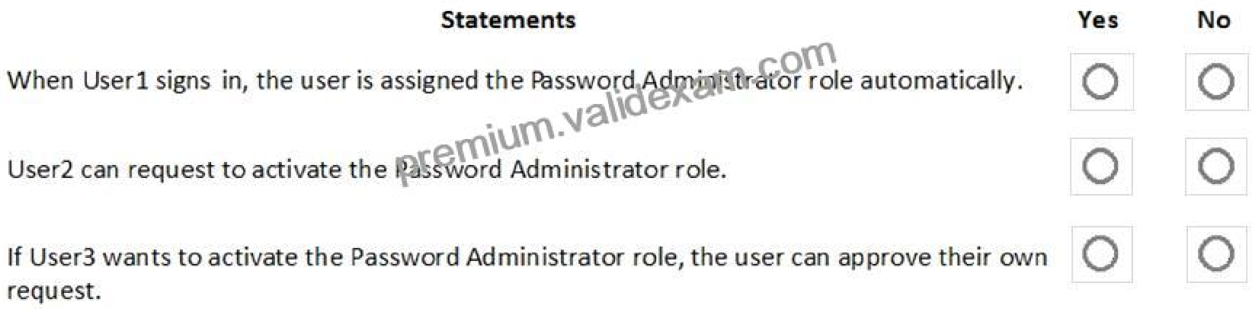
You assign users the Password Administrator role as shown in the following table.



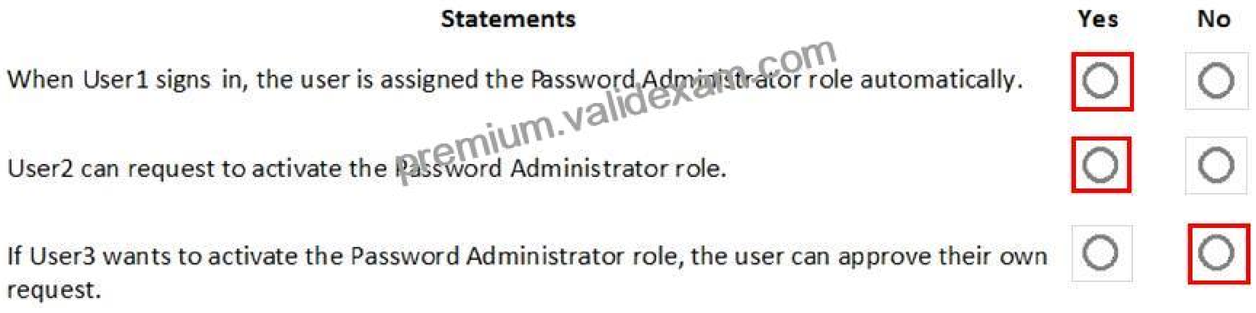
Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

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

NOTE: Each correct selection is worth one point.



Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	○	○
User2 can request to activate the Password Administrator role.	○	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	○



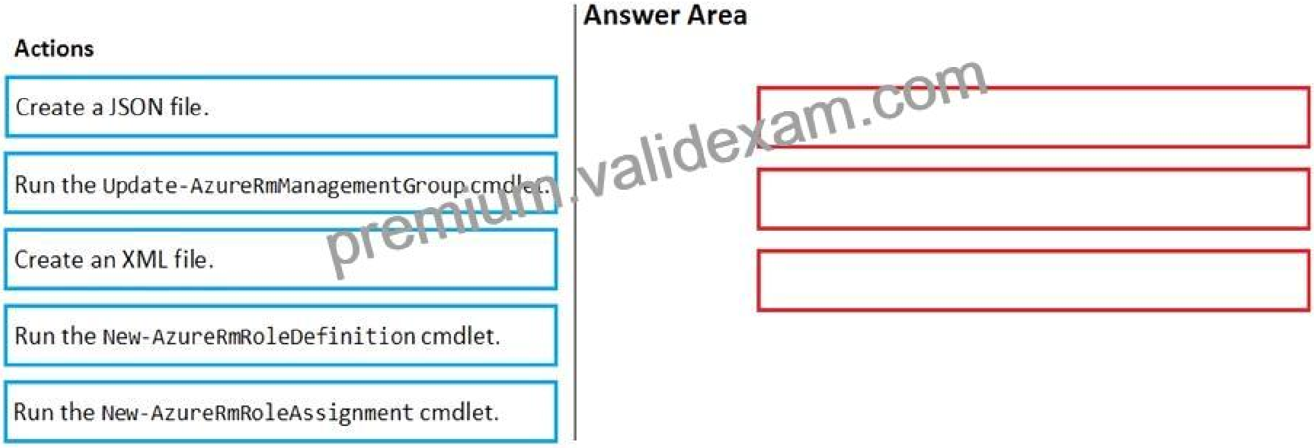
Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	[✓ ○]	○
User2 can request to activate the Password Administrator role.	[✓ ○]	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	[✓ ○]

NO.167 You have an Azure subscription named Sub1.

You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.

You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1. The solution must use the principle of least privilege.

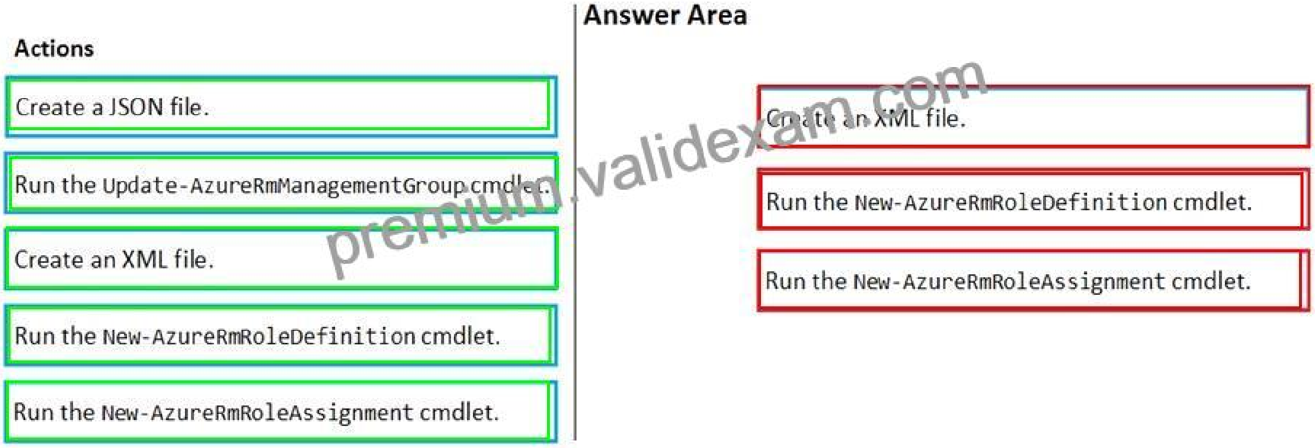
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

- Create a JSON file.
- Run the Update-AzureRmManagementGroup cmdlet.
- Create an XML file.
- Run the New-AzureRmRoleDefinition cmdlet.
- Run the New-AzureRmRoleAssignment cmdlet.

Answer Area



Actions

- Create a JSON file.
- Run the Update-AzureRmManagementGroup cmdlet.
- Create an XML file.
- Run the New-AzureRmRoleDefinition cmdlet.
- Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

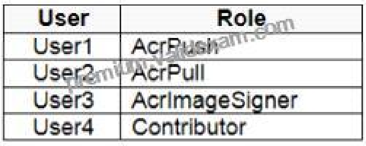
- Create an XML file.
- Run the New-AzureRmRoleDefinition cmdlet.
- Run the New-AzureRmRoleAssignment cmdlet.

References:

https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure

NO.168 You have an Azure Container Registry named Registry1.

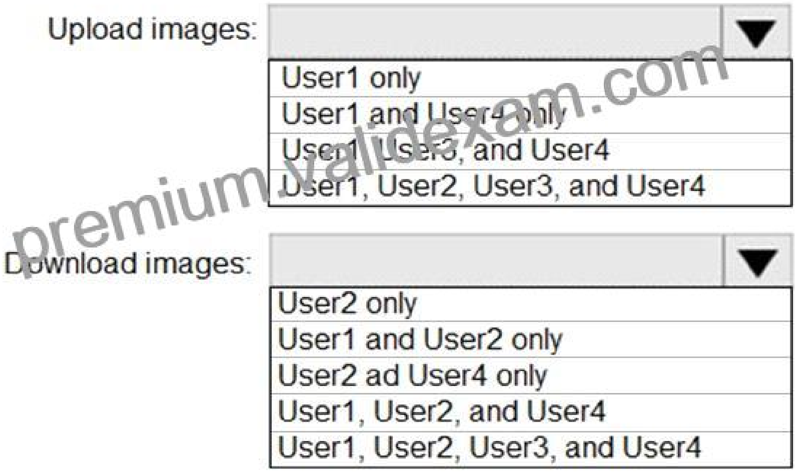
You add role assignment for Registry1 as shown in the following table.



User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

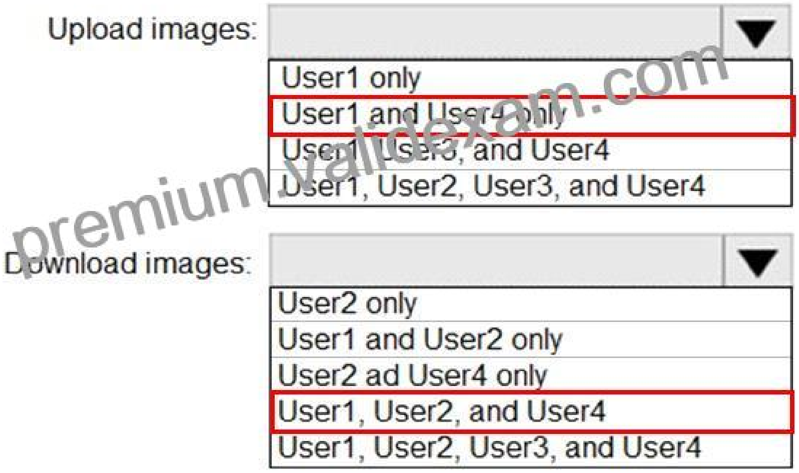


Upload images:

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

Download images:

User2 only
User1 and User2 only
User2 ad User4 only
User1, User2, and User4
User1, User2, User3, and User4



Upload images:

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

Download images:

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

Reference:

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

NO.169 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.
* Turn on the system-assigned managed identity for Contoso1812.
* Add a hostname to Contoso1812.
* Scale out the App Service plan of Contoso1812.
* Add a deployment slot to Contoso1812.
* Scale up the App Service plan of Contoso1812.
* Upload a PFX file to Contoso1812
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 &#8220;A&#8221; record pointing to contoso.com

A root &#8220;TXT&#8221; record for verification

A &#8220;CNAME&#8221; record for the www name that points to the A record

F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.

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

NO.170 You have an Azure subscription that contains an Azure key vault named Vault1.

In Vault1, you create a secret named Secret1.

An application developer registers an application in Azure Active Directory (Azure AD).

You need to ensure that the application can use Secret1.

What should you do?
* In Azure AD, create a role.
* In Azure Key Vault, create a key.
* In Azure Key Vault, create an access policy.
* In Azure AD, enable Azure AD Application Proxy.
Azure Key Vault provides a way to securely store credentials and other keys and secrets, but your code needs to authenticate to Key Vault to retrieve them.

Managed identities for Azure resources overview makes solving this problem simpler, by giving Azure services an automatically managed identity in Azure Active Directory (Azure AD). You can use this identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without having any credentials in your code.

Example: How a system-assigned managed identity works with an Azure VM

After the VM has an identity, use the service principal information to grant the VM access to Azure resources.

To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault.

References:

https://docs.microsoft.com/en-us/azure/key-vault/quick-create-net

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview