AZ-500^Q&As

Microsoft Azure Security Technologies

Pass Microsoft AZ-500 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/az-500.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

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 regenerate the Azure storage account access keys.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Generating new storage account keys will invalidate all SAS\\'s that were based on the previous keys.

QUESTION 2

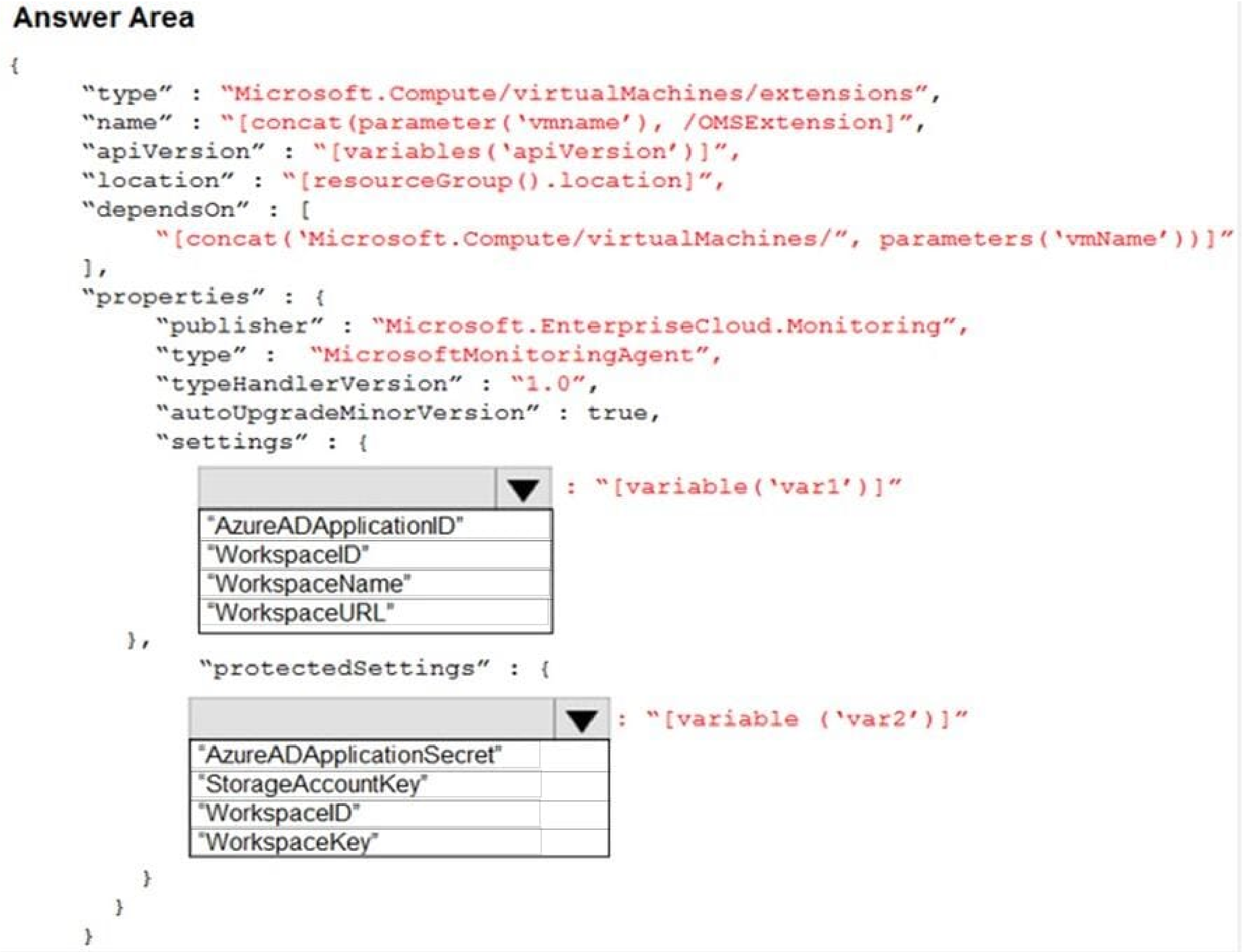
You plan to use Azure Log Analytics to collect logs from 200 servers that run Windows Server 2016.

You need to automate the deployment of the Microsoft Monitoring 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:



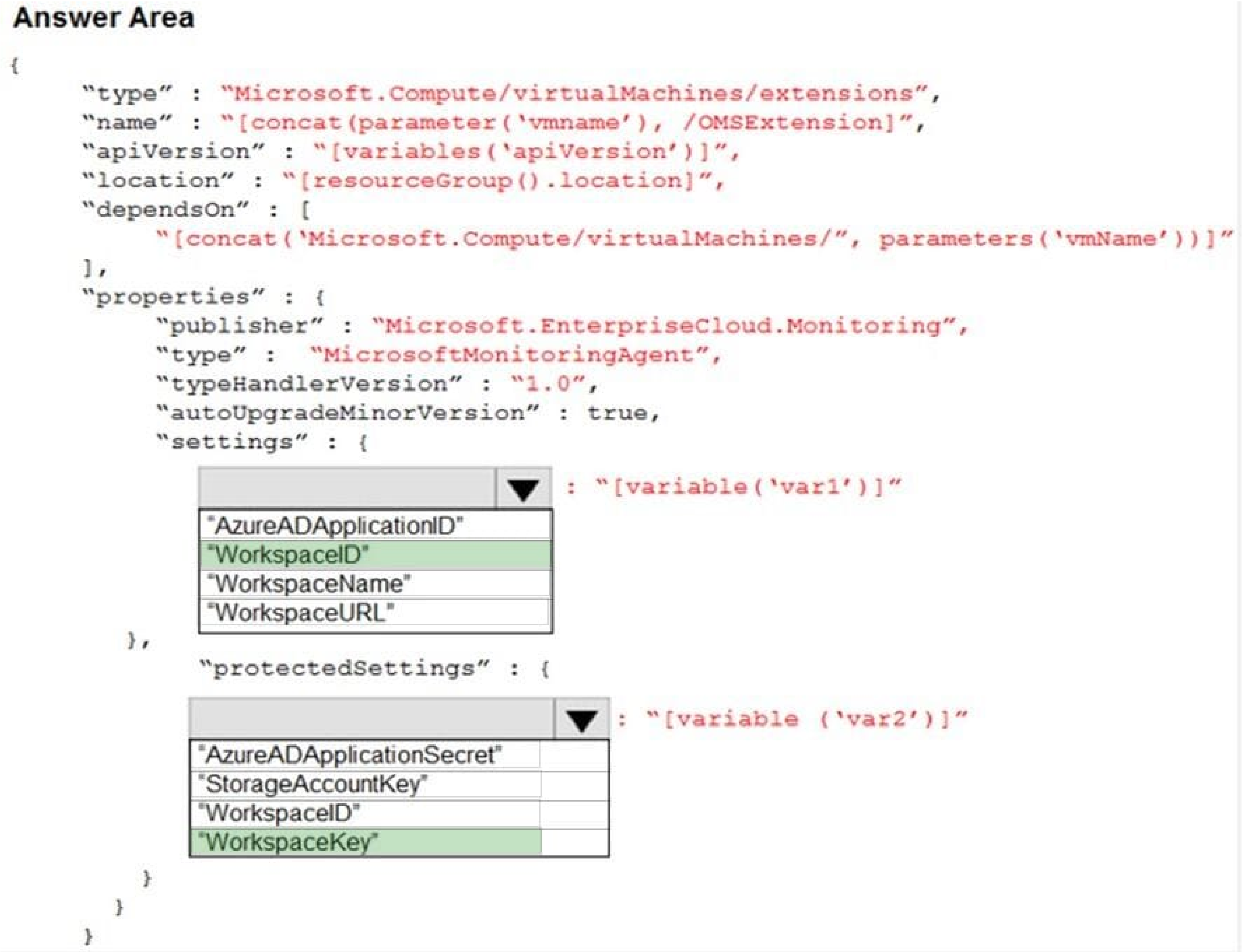
Answer Area

```
{
     "type" : "Microsoft.Compute/virtualMachines/extensions",
     "name" : "[concat(parameter('vmname'), /OMSExtension]",
     "apiVersion" : "[variables('apiVersion')]",
     "location" : "[resourceGroup().location]",
     "dependsOn" : [
          "[concat('Microsoft.Compute/virtualMachines/", parameters('vmName'))]"
     ],
     "properties" : {
          "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
          "type" :  "MicrosoftMonitoringAgent",
          "typeHandlerVersion" : "1.0",
          "autoUpgradeMinorVersion" : true,
          "settings" : {
               [▼] : "[variable('var1')]"
          },
               "protectedSettings" : {
               [▼] : "[variable ('var2')]"
            }
          }
     }
```

First dropdown:
- "AzureADApplicationID"
- "WorkspaceID"
- "WorkspaceName"
- "WorkspaceURL"

Second dropdown:
- "AzureADApplicationSecret"
- "StorageAccountKey"
- "WorkspaceID"
- "WorkspaceKey"

Correct Answer:



Answer Area

```
{
     "type" : "Microsoft.Compute/virtualMachines/extensions",
     "name" : "[concat(parameter('vmname'), /OMSExtension]",
     "apiVersion" : "[variables('apiVersion')]",
     "location" : "[resourceGroup().location]",
     "dependsOn" : [
          "[concat('Microsoft.Compute/virtualMachines/", parameters('vmName'))]"
     ],
     "properties" : {
          "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
          "type" :  "MicrosoftMonitoringAgent",
          "typeHandlerVersion" : "1.0",
          "autoUpgradeMinorVersion" : true,
          "settings" : {
                [▼] : "[variable('var1')]"
                 "AzureADApplicationID"
                 "WorkspaceID"
                 "WorkspaceName"
                 "WorkspaceURL"
          },
                "protectedSettings" : {
               [▼] : "[variable ('var2')]"
                "AzureADApplicationSecret"
                "StorageAccountKey"
                "WorkspaceID"
                "WorkspaceKey"
                }
            }
       }
```

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

QUESTION 3

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 Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.

Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Solution: You recommend the use of federation with Active Directory Federation Services (AD FS).

Does the solution meet the goal?

A. Yes

B. No

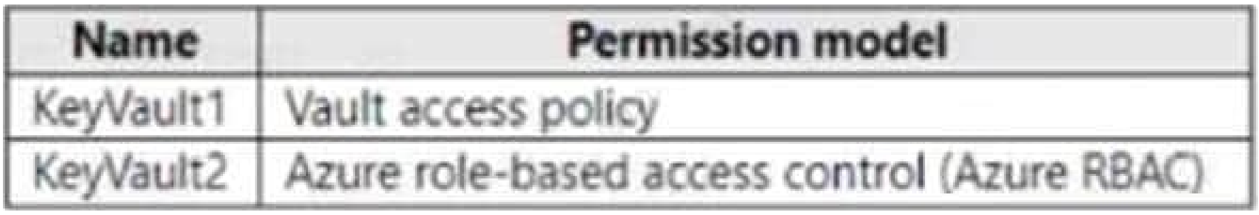
Correct Answer: B

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 4

You have an Azure subscription that contains a managed identity named Identity1 and the Azure key vaults shown in the following table.



Name	Permission model
KeyVault1	Vault access policy
KeyVault2	Azure role-based access control (Azure RBAC)

KeyVault1 contains an access policy that grants Identity1 the following key permissions:

Get List Wrap Unwrap

You need to provide Identity1 with the same permissions for KeyVault2. The solution must use the principle of least privilege.

Which role should you assign to Identity1?

A. Key Vault Crypto Service Encryption User

B. Key Vault Crypto User

C. Key Vault Reader

D. Key Vault Crypto Officer

Correct Answer: D

Key Vault Crypto Officer - Perform any action on the keys of a key vault, except manage permissions. Only works for key vaults that use the \\'Azure role-based access control\\' permission model. Incorrect:

*

Key Vault Crypto Service Encryption User

Read metadata of keys and perform wrap/unwrap operations. Only works for key vaults that use the \\'Azure role-based access control\\' permission model.

*

Key Vault Crypto User

Perform cryptographic operations using keys. Only works for key vaults that use the \\'Azure role-based access control\\' permission model.

*

Key Vault Reader

Read metadata of key vaults and its certificates, keys, and secrets. Cannot read sensitive values such as secret contents or key material. Only works for key vaults that use the \\'Azure role-based access control\\' permission model.

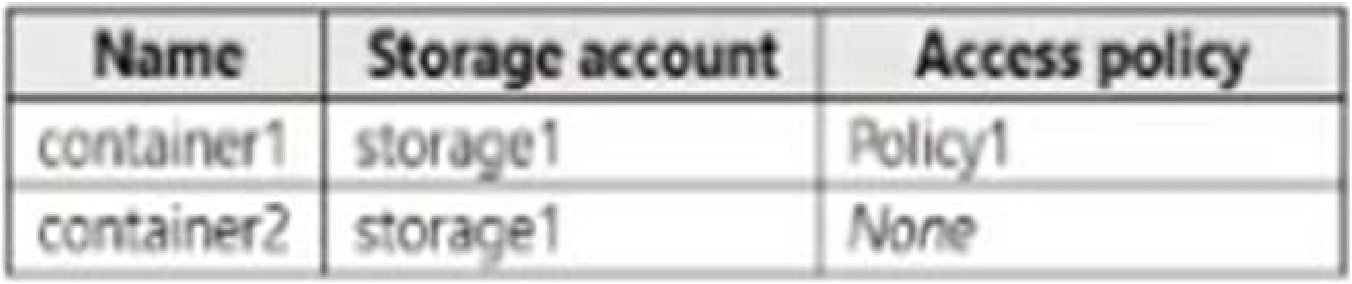
Reference:

https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide

QUESTION 5

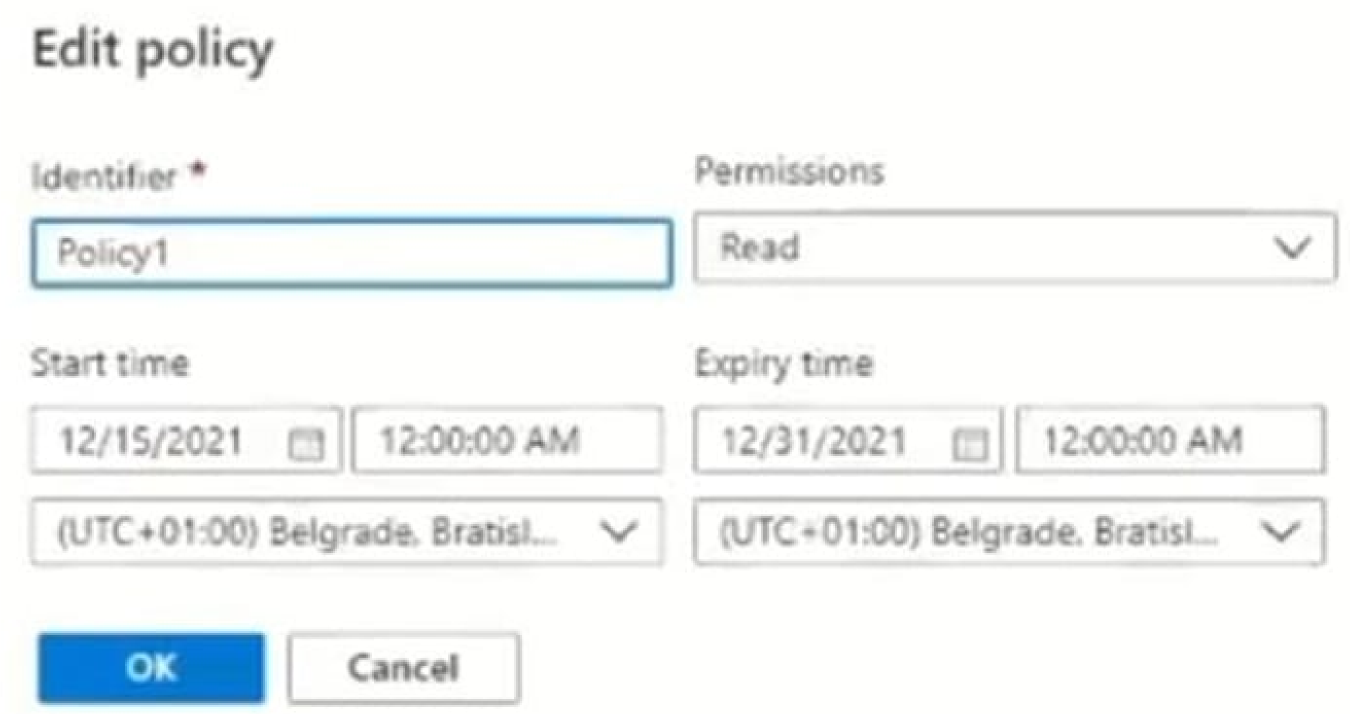
HOTSPOT

You have an Azure subscription that contains two users named User1 and User2 and the blob containers shown in the following table.



Name	Storage account	Access policy
container1	storage1	Policy1
container2	storage1	None

Policy1 is configured as shown in the following exhibit.



Edit policy

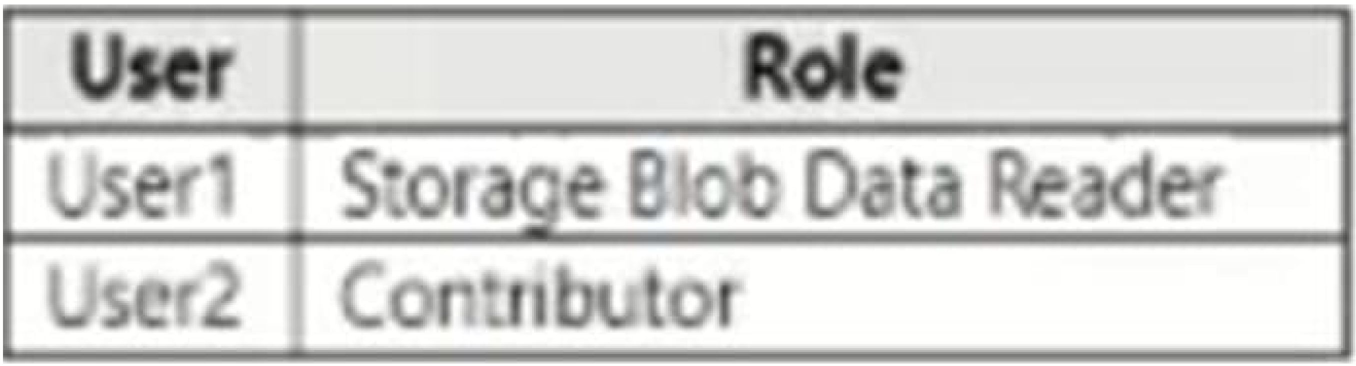
Identifier *
Policy1

Permissions
Read

Start time
12/15/2021 | 12:00:00 AM
(UTC+01:00) Belgrade, Bratisl...

Expiry time
12/31/2021 | 12:00:00 AM
(UTC+01:00) Belgrade, Bratisl...

You assign the roles for storage1 as shown in the following table.



User	Role
User1	Storage Blob Data Reader
User2	Contributor

The storage1 account has the following shared access signature (SAS) named SAS1:

Allowed services: Blob Allowed resource types: Container Allowed permissions: Read, Write, List, Add, Create Blob versioning permissions: enables deletion of versions Allowed blob index permissions: Read/Write Starr and expiry date/time:

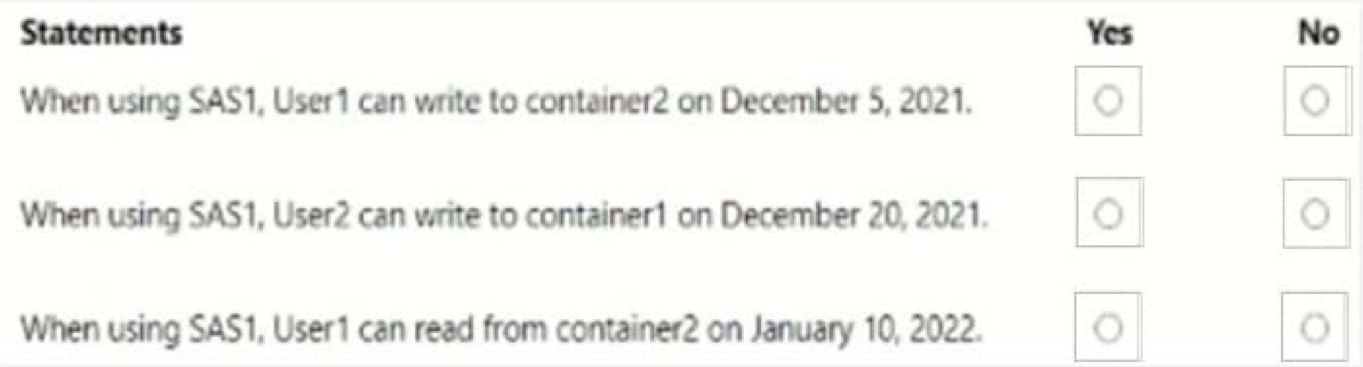
-Start: 12/1/2021

-End: 12/31/2021

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

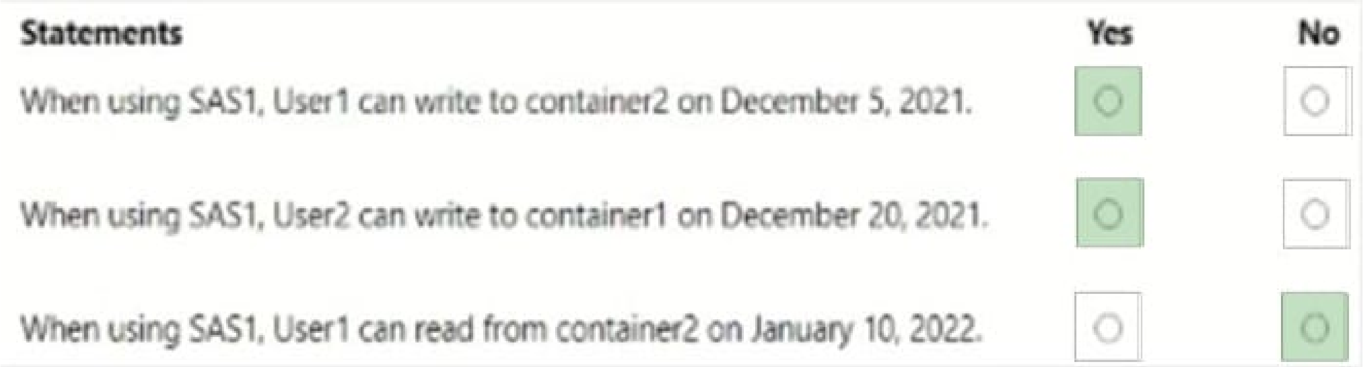
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
When using SAS1, User1 can write to container2 on December 5, 2021.	○	○
When using SAS1, User2 can write to container1 on December 20, 2021.	○	○
When using SAS1, User1 can read from container2 on January 10, 2022.	○	○

Correct Answer:



Statements	Yes	No
When using SAS1, User1 can write to container2 on December 5, 2021.	●	○
When using SAS1, User2 can write to container1 on December 20, 2021.	●	○
When using SAS1, User1 can read from container2 on January 10, 2022.	○	●

QUESTION 6

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 a resource graph and an assignment that is scoped to a management group.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously. However, you need to use an initiative, not a resource graph to bundle the policy definitions into a group that can be applied to the management group.

References: https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/

QUESTION 7

SIMULATION

You need to create a new Azure Active Directory (Azure AD) directory named 11641655.onmicrosoft.com and a user named User1 in the new directory. The solution must ensure that User1 is enabled for Azure Multi-Factor Authentication (MFA).

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

A. See the explanation below.

Correct Answer: A

Step 1: Create an Azure Active Directory 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 and an Initial domain name (10598168). Then select Create. Your directory is created.

6.

After directory creation is complete, select the information box to manage your new directory. Next, you\\'re going to add tenant users.

Step 2: Create an Azure Active Directory tenant user

7.

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

8.

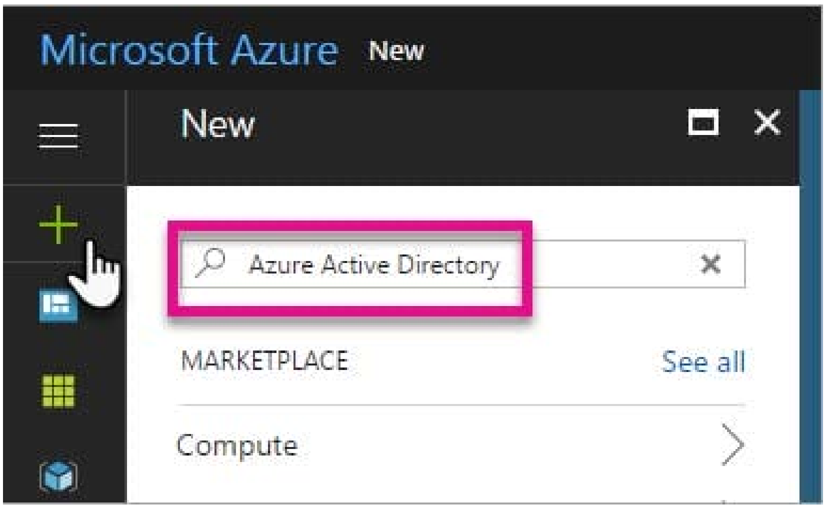
Under Manage, select Users.

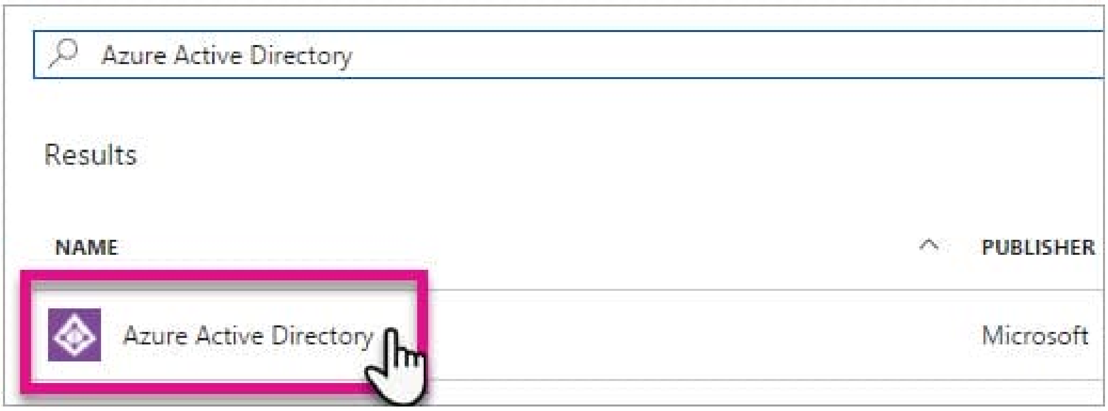
9.

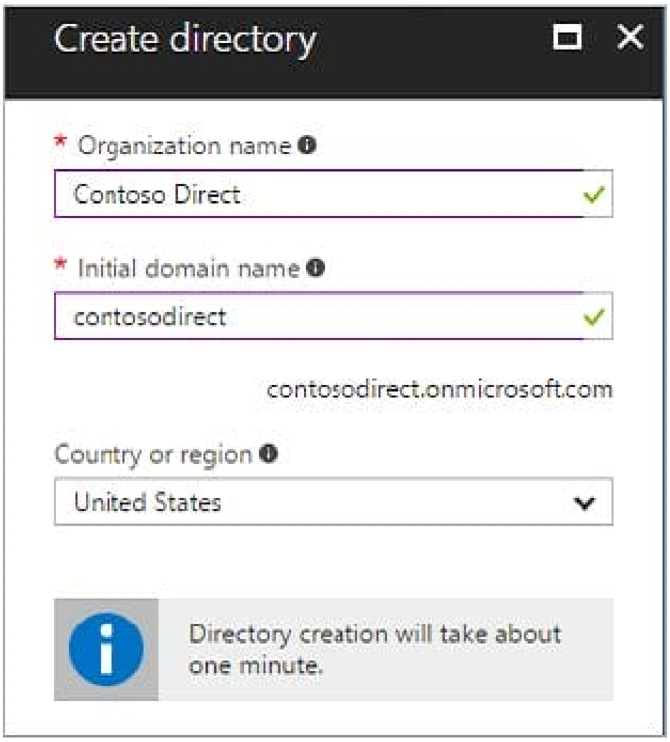
Select All users and then select + New user.

10.

Provide a Name and User name (user1) for the regular user tenant You can also show the temporary password. When you\\'re done, select Create.







Create directory

* Organization name

Contoso Direct

* Initial domain name

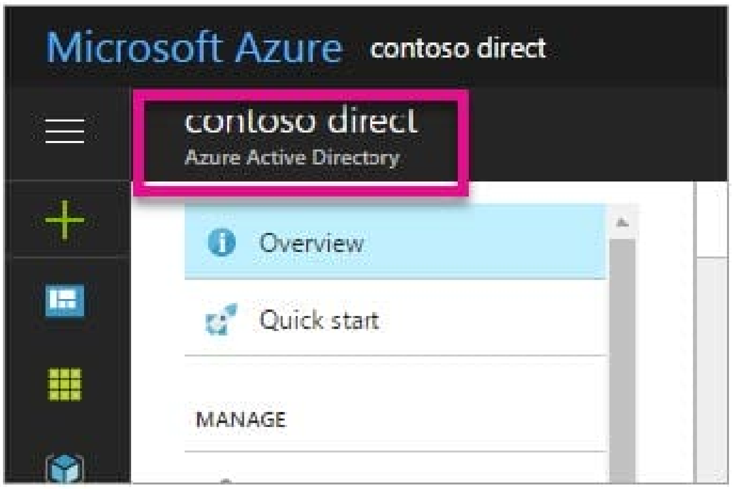
contosodirect

contosodirect.onmicrosoft.com

Country or region

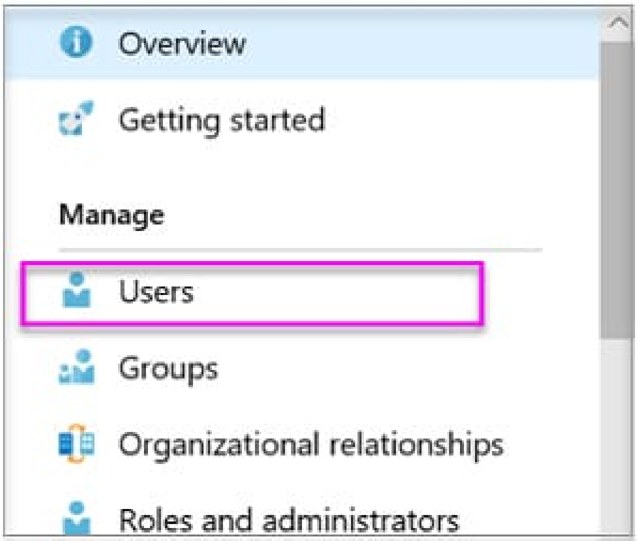
United States

Directory creation will take about one minute.

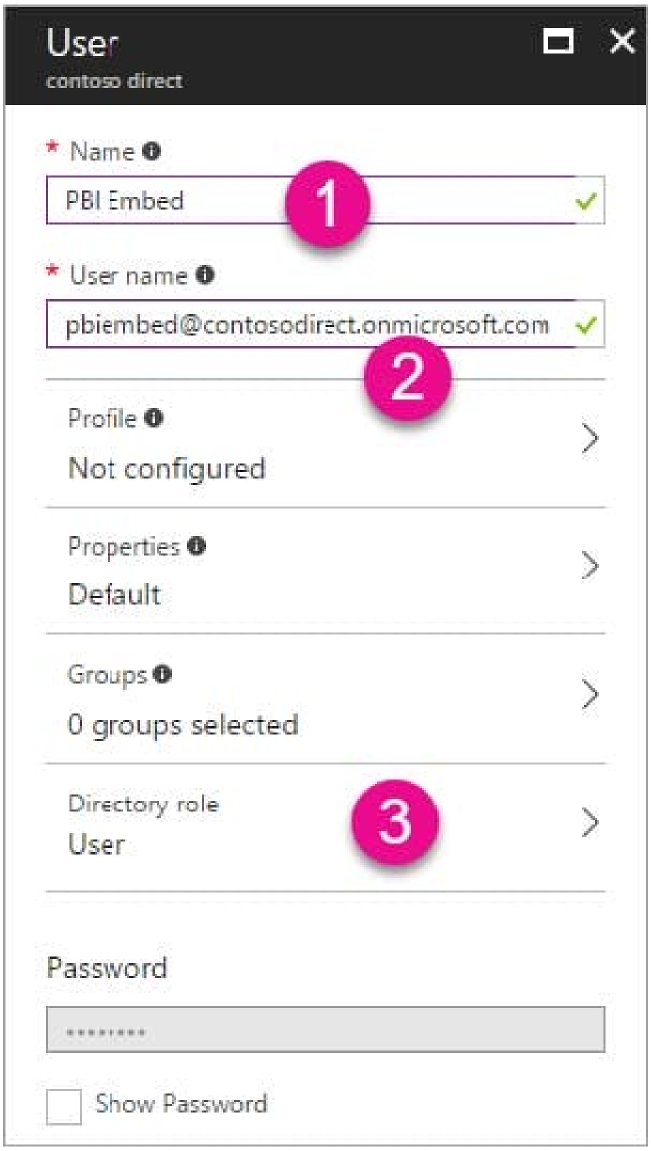


Microsoft Azure contoso direct

contoso direct
Azure Active Directory



Name: user1 User name: user1@10598168.onmicrosoft.com


User
contoso direct

* Name: PBI Embed

* User name: pbiembed@contosodirect.onmicrosoft.com

Profile: Not configured

Properties: Default

Groups: 0 groups selected

Directory role: User

Password: ••••••••

□ Show Password

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

QUESTION 8

SIMULATION

You plan to use Azure Disk Encryption for several virtual machine disks.

You need to ensure that Azure Disk Encryption can retrieve secrets from the KeyVault11641655 Azure key vault.

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 Key Vaults in the search box, select Key Vaults from the search results then select KeyVault11641655. Alternatively, browse to Key Vaults in the left navigation pane.

2.

In the Key Vault properties, scroll down to the Settings section and select Access Policies.

3.

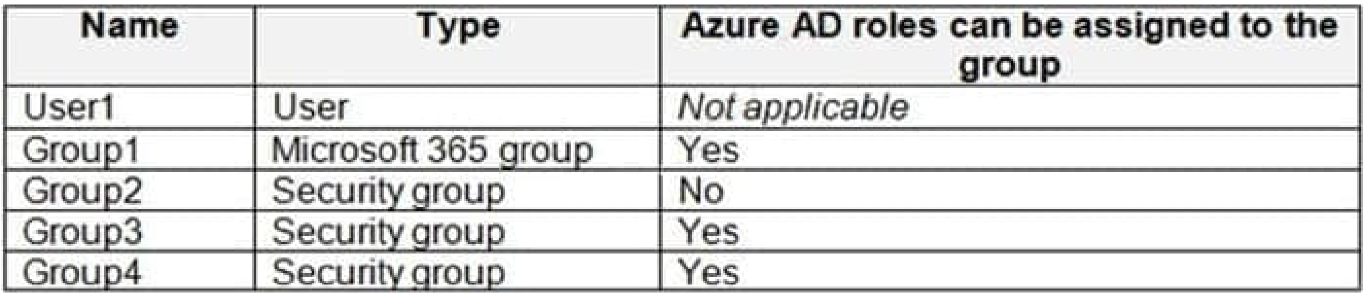
Select the Azure Disk Encryption for volume encryption

4.

Click Save to save the changes.

QUESTION 9

You have an Azure subscription that contains a resource group named RG1 and the identities shown in the following table.



Name	Type	Azure AD roles can be assigned to the group
User1	User	*Not applicable*
Group1	Microsoft 365 group	Yes
Group2	Security group	No
Group3	Security group	Yes
Group4	Security group	Yes

You assign Group4 the Contributor role for RG1. Which identities can you add to Group4 as members?

A. User1 only

B. User1 and Group3 only

C. User1, Group1, and Group3 only

D. User1, Group2, and Group3 only

E. User1, Group1, Group2, and Group3

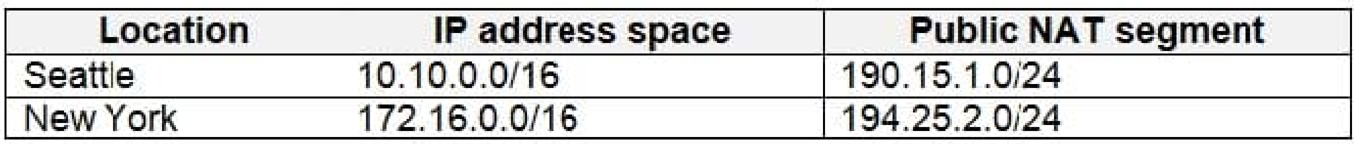
Correct Answer: B

Limitation of using managed identities for authorization Using Azure AD groups for granting access to services is a great way to simplify the authorization process. The idea is simple – grant permissions to a group and add identities to the group so that they inherit the same permissions. This is a well-established pattern from various on-premises systems and works well when the identities represent users.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identity-best-practice-recommendations

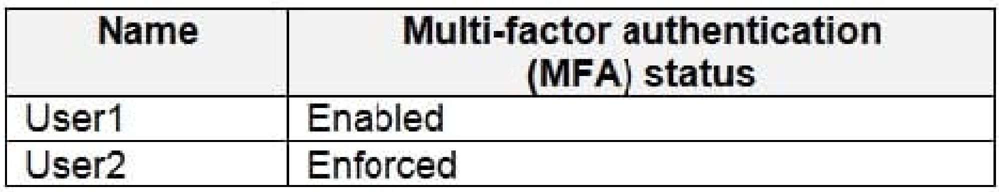
QUESTION 10

Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.



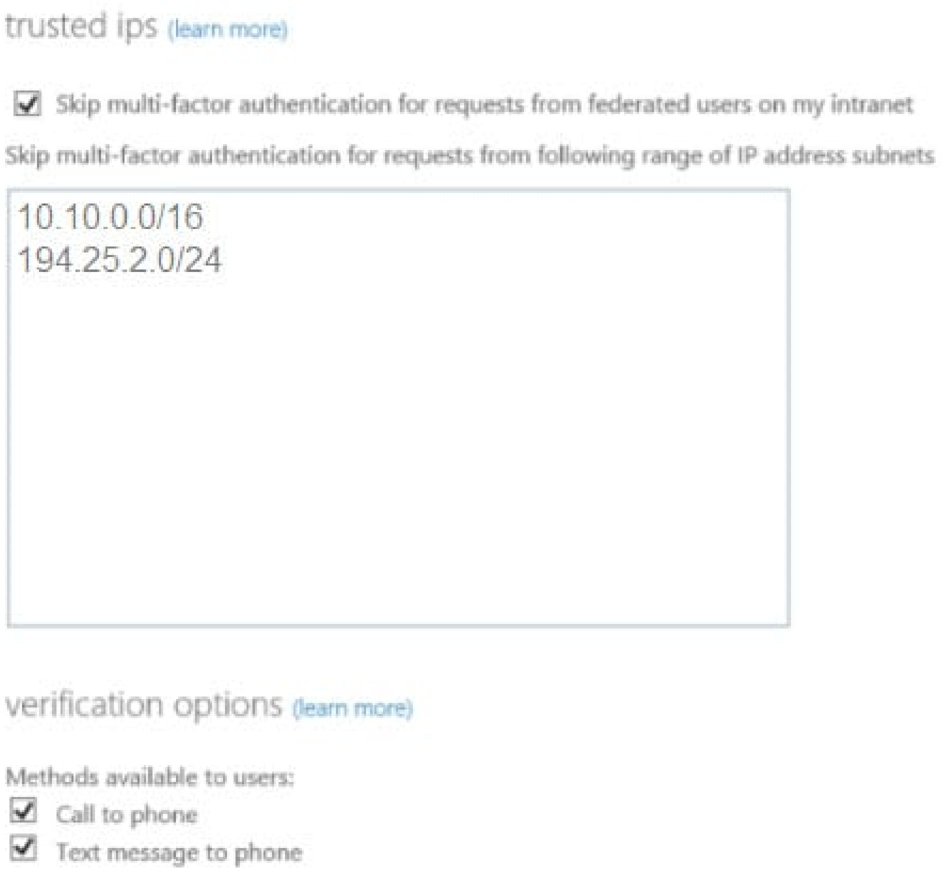
Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

The company has an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.



Name	Multi-factor authentication (MFA) status
User1	Enabled
User2	Enforced

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)



trusted ips (learn more)

☑ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

```
10.10.0.0/16
194.25.2.0/24
```

verification options (learn more)

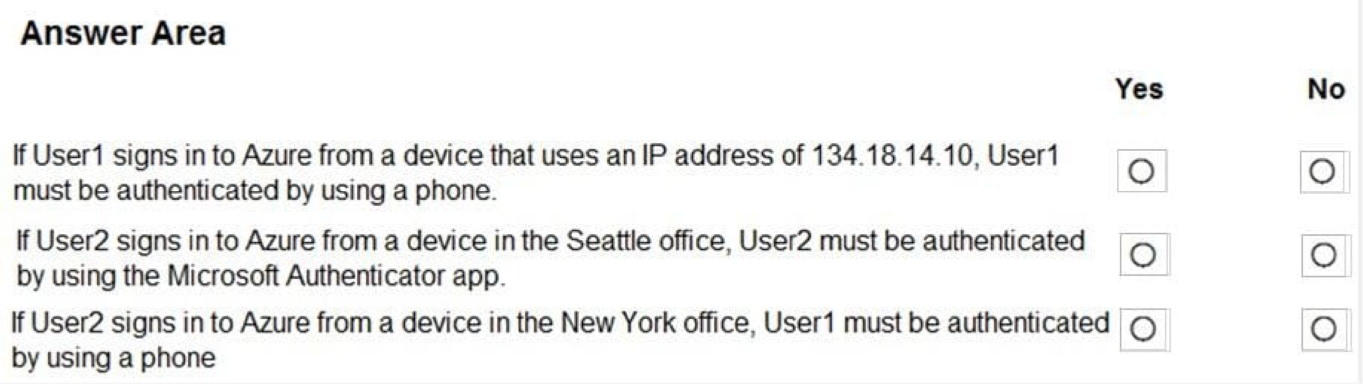
Methods available to users:

☑ Call to phone

☑ Text message to phone

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

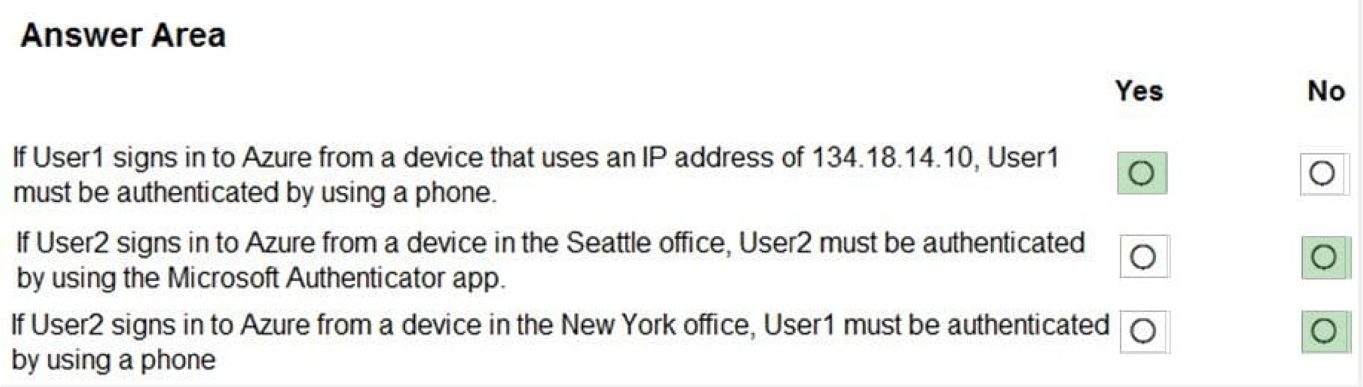
Hot Area:



Answer Area

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	○	○
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	○	○
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	○	○

Correct Answer:



Answer Area

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	[✓ ○]	○
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	○	[✓ ○]
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	○	[✓ ○]

Box 2: No

Use of Microsoft Authenticator is not required.

Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process.

Box 3: No

The New York IP address subnet is included in the "skip multi-factor authentication for request.

References:

https://www.cayosoft.com/difference-enabling-enforcing-mfa/

QUESTION 11

You need to ensure that you can meet the security operations requirements. What should you do first?

A. Turn on Auto Provisioning in Security Center.

B. Integrate Security Center and Microsoft Cloud App Security.

C. Upgrade the pricing tier of Security Center to Standard.

D. Modify the Security Center workspace configuration.

Correct Answer: C

The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds

advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.

Scenario: Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

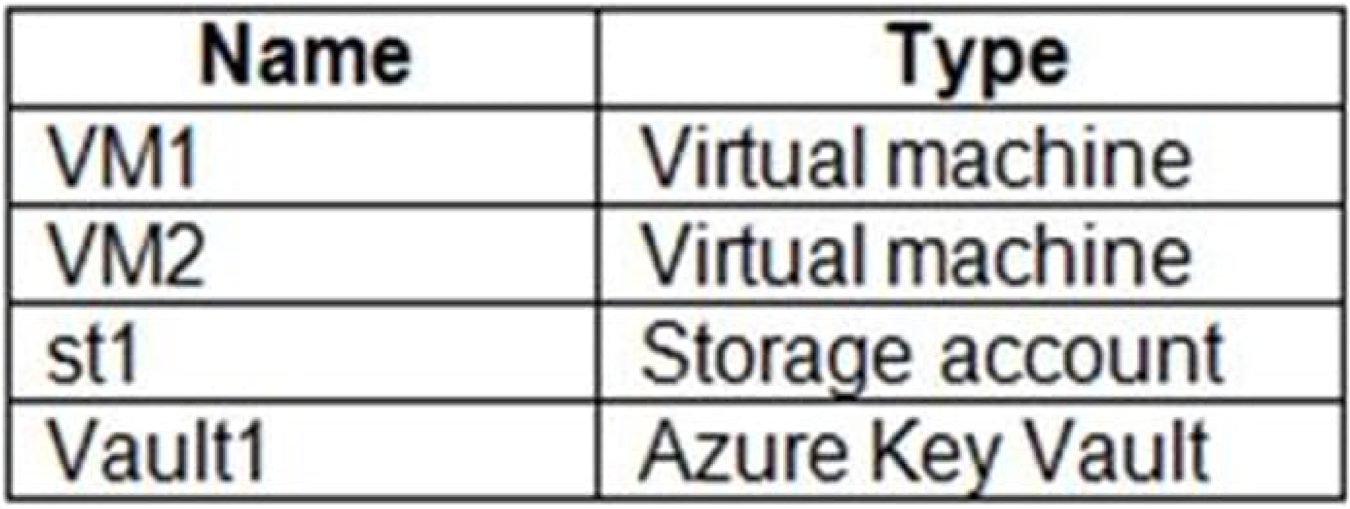
References:

https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing

QUESTION 12

DRAG DROP

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



Name	Type
VM1	Virtual machine
VM2	Virtual machine
st1	Storage account
Vault1	Azure Key Vault

You plan to perform the following actions:

Deploy a new app named App1 that will require access to Vault1.

Configure a shared identity for VM1 and VM2 to access st1.

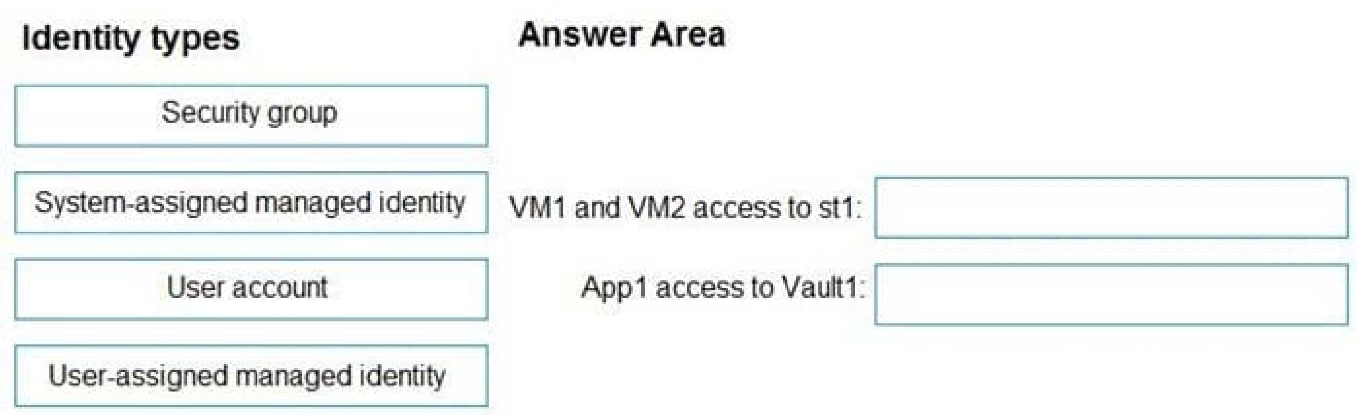
You need to configure identities for each requirement. The solution must minimize administrative effort.

Which type of identity should you configure for each requirement? To answer, drag the appropriate identity types to the correct requirements. Each identity type 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.

Select and Place:



Identity types

Security group

System-assigned managed identity

User account

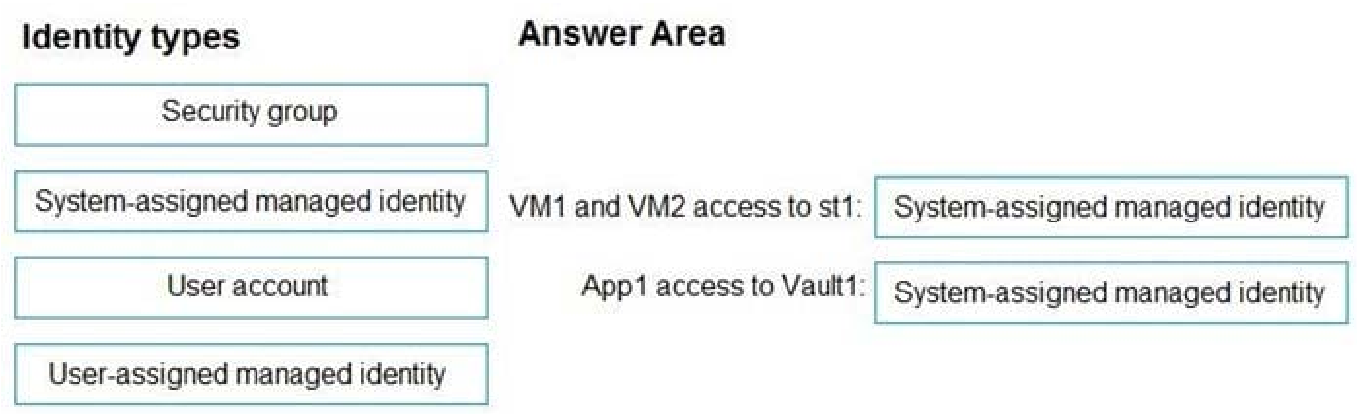
User-assigned managed identity

Answer Area

VM1 and VM2 access to st1:

App1 access to Vault1:

Correct Answer:



Identity types

Security group

System-assigned managed identity

User account

User-assigned managed identity

Answer Area

VM1 and VM2 access to st1: System-assigned managed identity

App1 access to Vault1: System-assigned managed identity

QUESTION 13

You have an Azure subscription that contains a user named Admin1 and a virtual machine named VM1. VM1 runs Windows Server 2019 and was deployed by using an Azure Resource Manager template. VM1 is the member of a backend

pool of a public Azure Basic Load Balancer.

Admin1 reports that VM1 is listed as Unsupported on the Just in time VM access blade of Azure Security Center.

You need to ensure that Admin1 can enable just in time (JIT) VM access for VM1.

What should you do?

A. Create and configure an additional public IP address for VM 1.

B. Replace the Basic Load Balancer with an Azure Standard Load Balancer.

C. Assign an Azure Active Directory Premium Plan 1 license to Admin1.

D. Create and configure a network security group (NSG).

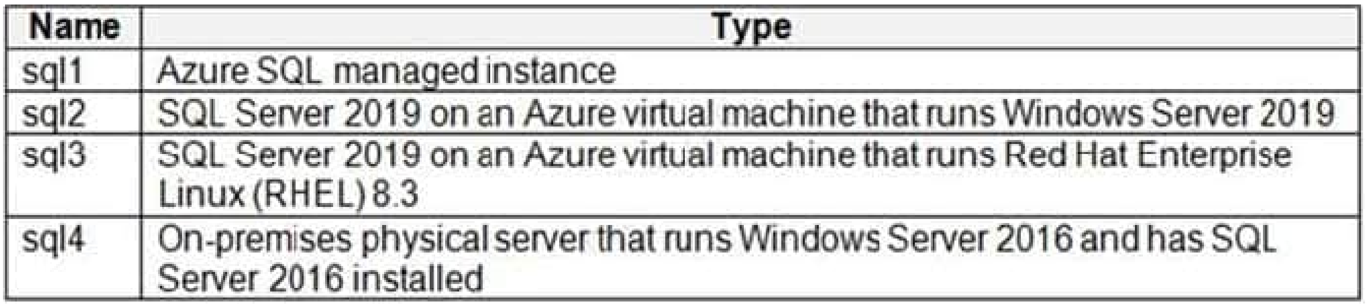
Correct Answer: D

Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-request-asc

QUESTION 14

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, and sql3 only

C. sql1, sql2, and sql4 only

D. sql1, sql2, sql3, and sql4

Correct Answer: D

Microsoft Defender for SQL protected versions:

1.

Azure SQL Managed Instance (sql1)

2.

SQL on Azure virtual machines

SQL Server on Windows Azure Virtual Machines (sql2)

SQL Server on Linux Azure Virtual Machines including Red Hat Enterprise Linux (RHEL) 8 (sql3)

1.

On-premises SQL servers on Windows machines without Azure Arc (sql4)

2.

Azure SQL single databases and elastic pools

3.

SQL Server on Azure Arc-enabled servers

4.

Azure Synapse Analytics (formerly SQL DW) dedicated SQL pool

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-sql-introduction

https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/sql-server-on-azure-vm-iaas-what-is-overview

https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/linux/sql-server-on-linux-vm-what-is-iaas-overview

QUESTION 15

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.

You plan to publish several apps in the tenant.

You need to ensure that User1 can grant admin consent for the published apps.

Which two possible user roles can you assign to User1 to achieve this goal? Each correct answer presents 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

Correct Answer: CE

Reference: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent