Microsoft

AZ-303 Exam

Microsoft Azure Architect Technologies Exam

Product Questions: 111/2Case Study Version: 5.1

Case Study: 1

Contoso, Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.
- Ensure that all the virtual machines for App1 are protected by backups.
- Copy the blueprint files to Azure over the Internet.
- Ensure that the blueprint files are stored in the archive storage tier.
- Ensure that partner access to the blueprint files is secured and temporary.
- Prevent user passwords or hashes of passwords from being stored in Azure.
- Use unmanaged standard storage for the hard disks of the virtual machines.
- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:
Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
Designate a new user named Admin1 as the service administrator of the Azure subscription.
Ensure that a new user named User3 can create network objects for the Azure subscription

Question: 1

You need to meet the user requirement for Admin1.
What should you do?

A. From the Subscriptions blade, select the subscription, and then modify the Properties.
B. From the Subscriptions blade, select the subscription, and then modify the Access control (IAM) settings.
C. From the Azure Active Directory blade, modify the Properties.
D. From the Azure Active Directory blade, modify the Groups.

Answer: A

Explanation:
Change the Service administrator for an Azure subscription
• Sign in to Account Center as the Account administrator.
• Select a subscription.
• On the right side, select Edit subscription details.
Scenario: Designate a new user named Admin1 as the service administrator of the Azure subscription.
References:
https://docs.microsoft.com/en-us/azure/billing/billing-add-change-azure-subscription-administrator

Question: 2

You need to move the blueprint files to Azure.
What should you do?

A. Generate a shared access signature (SAS). Map a drive, and then copy the files by using File Explorer.
B. Use the Azure Import/Export service.
C. Generate an access key. Map a drive, and then copy the files by using File Explorer.
D. Use Azure Storage Explorer to copy the files.

Answer: D

Explanation:
Azure Storage Explorer is a free tool from Microsoft that allows you to work with Azure Storage data on Windows, macOS, and Linux. You can use it to upload and download data from Azure blob storage.

Scenario:
Planned Changes include: move the existing product blueprint files to Azure Blob storage.
Technical Requirements include: Copy the blueprint files to Azure over the Internet.
References:
https://docs.microsoft.com/en-us/azure/machine-learning/team-data-science-process/move-data-to-azure-blob-using-azure-storage-explorer

Question: 3

You need to implement a backup solution for App1 after the application is moved.
What should you create first?

A. a recovery plan
B. an Azure Backup Server
C. a backup policy
D. a Recovery Services vault

Answer: D

Explanation:
A Recovery Services vault is a logical container that stores the backup data for each protected resource, such as Azure VMs. When the backup job for a protected resource runs, it creates a recovery point inside the Recovery Services vault.
Scenario:
There are three application tiers, each with five virtual machines.
Move all the virtual machines for App1 to Azure.
Ensure that all the virtual machines for App1 are protected by backups.
References:
https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-portal

Question: 4

HOTSPOT
You need to recommend a solution for App1. The solution must meet the technical requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Number of virtual networks: [▼]
- 1
- 2
- 3

Number of subnets per virtual network: [▼]
- 1
- 2
- 3

Answer:

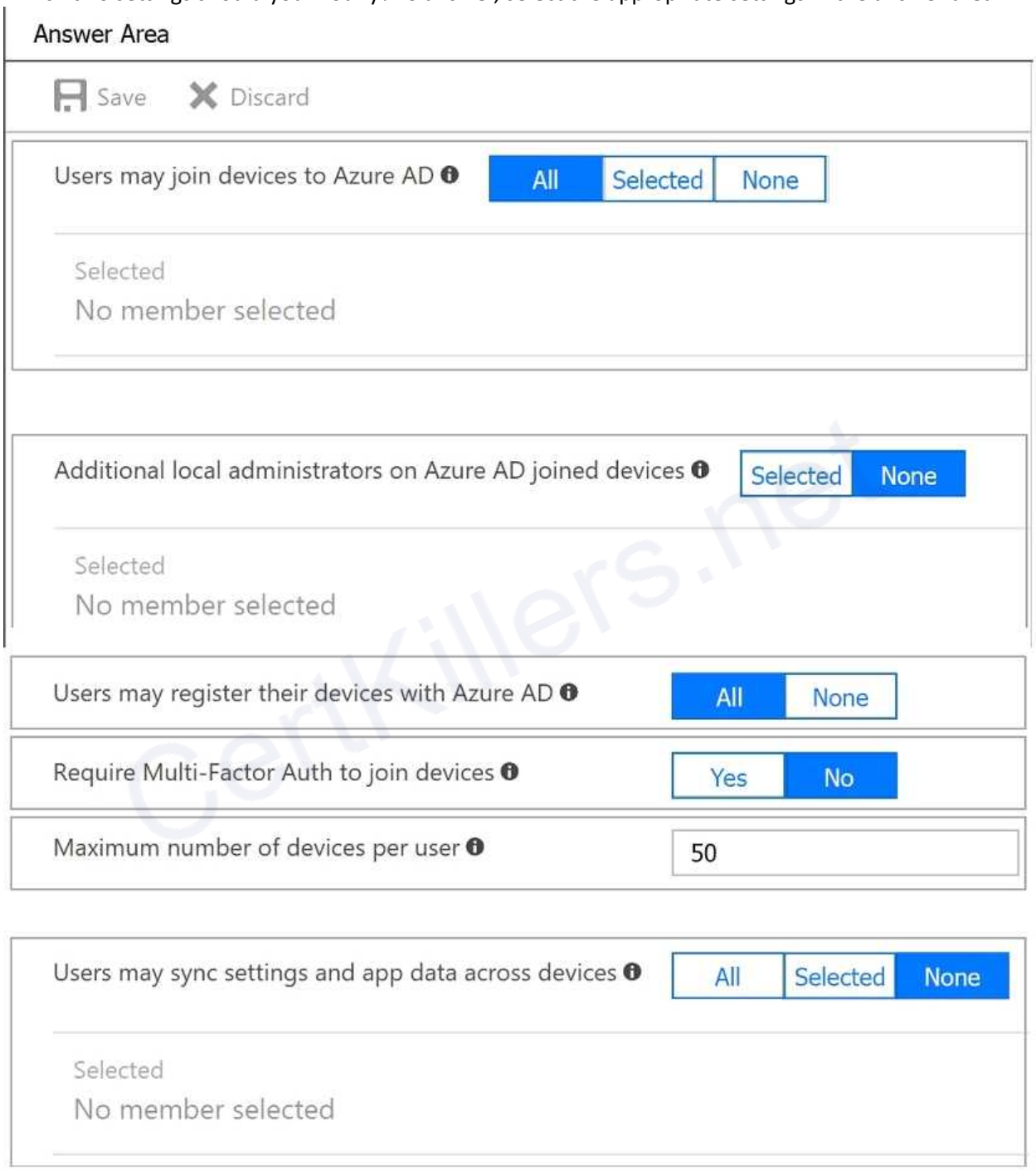
Number of virtual networks: [▼]
- 1
- 2
- 3 (selected)

Number of subnets per virtual network: [▼]
- 1 (selected)
- 2
- 3

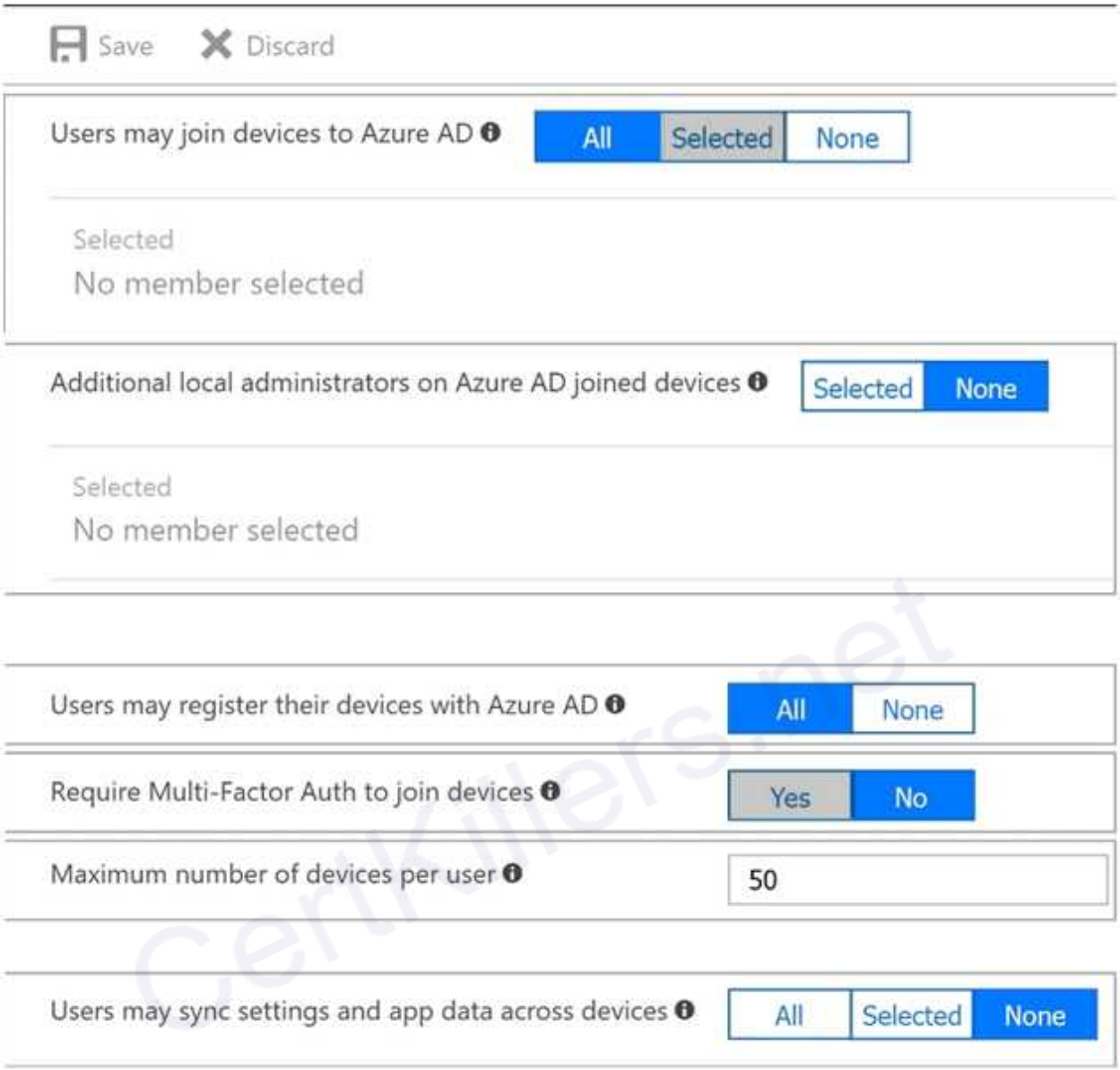
Explanation:
Box 1: 3
One virtual network for every tier
Box 2: 1
Only one subnet for each tier, to minimize the number of open ports.
Scenario: You have a public-facing application named App1. App1 is comprised of the following three tiers:
• A SQL database
• A web front end
• A processing middle tier
Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.
Technical requirements:
• Move all the virtual machines for App1 to Azure.
• Minimize the number of open ports between the App1 tiers.

Question: 5

HOTSPOT
You need to configure the Device settings to meet the technical requirements and the user requirements.
Which two settings should you modify? To answer, select the appropriate settings in the answer area.



Answer:



Explanation:
Box 1: Selected
Only selected users should be able to join devices
Box 2: Yes
Require Multi-Factor Auth to join devices.
From scenario:
• Ensure that only users who are part of a group named Pilot can join devices to Azure AD
• Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Question: 6

You need to recommend an identify solution that meets the technical requirements.
What should you recommend?

A. federated single-on (SSO) and Active Directory Federation Services (AD FS)
B. password hash synchronization and single sign-on (SSO)
C. cloud-only user accounts
D. Pass-through Authentication and single sign-on (SSO)

Answer: D

Explanation:
Active Directory Federation Services is a feature and web service in the Windows Server Operating System that allows sharing of identity information outside a company's network.
Scenario: Technical Requirements include:
Prevent user passwords or hashes of passwords from being stored in Azure.
References:
https://www.sherweb.com/blog/active-directory-federation-services/

Question: 7

You are planning the move of App1 to Azure.
You create a network security group (NSG).
You need to recommend a solution to provide users with access to App1.
What should you recommend?

A. Create an outgoing security rule for port 443 from the Internet. Associate the NSG to all the subnets.
B. Create an incoming security rule for port 443 from the Internet. Associate the NSG to all the subnets.
C. Create an incoming security rule for port 443 from the Internet. Associate the NSG to the subnet that contains the web servers.
D. Create an outgoing security rule for port 443 from the Internet. Associate the NSG to the subnet that contains the web servers.

Answer: C

Explanation:
As App1 is public-facing we need an incoming security rule, related to the access of the web servers.
Scenario: You have a public-facing application named App1. App1 is comprised of the following three tiers: a SQL database, a web front end, and a processing middle tier.
Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Question: 8

HOTSPOT
You need to identify the storage requirements for Contoso.
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
Contoso requires a storage account that supports Blob storage.	○	○
Contoso requires a storage account that supports Azure Table storage.	○	○
Contoso requires a storage account that supports Azure File Storage.	○	○

Answer:

Statements	Yes	No
Contoso requires a storage account that supports Blob storage.	●	○
Contoso requires a storage account that supports Azure Table storage.	○	●
Contoso requires a storage account that supports Azure File Storage.	○	●

Explanation:
Box 1: Yes
Contoso is moving the existing product blueprint files to Azure Blob storage.
Use unmanaged standard storage for the hard disks of the virtual machines. We use Page Blobs for these.
Box 2: No
Box 3: No

Case Study: 2
Mix Questions

Question: 9

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.
Your company is deploying an on-premises application named Appl. Users will access App1 by using a URL of https://app1.contoso.com. You register App1 in Azure Active Directory (Azure AD) and publish Appl by using the Azure AD Application Proxy. You need to ensure that Appl appears in the My Apps portal for all the users.

Solution: You configure the delegated permission for Appl in Azure AD. Does this meet the goal?

A. Yes
B. No

Answer: A

Question: 10

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.
Your company is deploying an on-premises application named Appl. Users will access App1 by using a URL of https://app1.contoso.com. You register App1 in Azure Active Directory (Azure AD) and publish Appl by using the Azure AD Application Proxy. You need to ensure that Appl appears in the My Apps portal for all the users.
Solution: You create an offer for App1 and publish the offer to Azure Marketplace.

A. Yes
B. No

Answer: A

Question: 11

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.
Your company is deploying an on-premises application named Appl. Users will access App1 by using a URL of https://app1.contoso.com. You register App1 in Azure Active Directory (Azure AD) and publish Appl by using the Azure AD Application Proxy. You need to ensure that Appl appears in the My Apps portal for all the users.
Solution: You create a conditional access policy for App1.

A. Yes
B. No

Answer: B

Question: 12

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 Active Directory {Azure AD) tenant named contoso.com.
A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin 1 discovers that all the other Identity Governance settings are available.
Admin1 is assigned The User administrator. Compliance administrator, and Security administrator roles.
You need to ensure that Admin1 can create access reviews in contoso.com. .
Solution: You assign the Global administrator role to Admin1.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use Azure AD Privileged Identity Management.
Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include:
Conduct access reviews to ensure users still need roles
References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Question: 13

Note: This question is part of 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 Active Directory (Azure AD) tenant named contoso.com.
A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other Identity Governance settings are available.
Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.
You need to ensure that the Admin1 can create access reviews in contoso.com.
Solution: You purchase an Azure Directory Premium P2 license for contoso.com.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use Azure AD Privileged Identity Management.
Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include:
• Conduct access reviews to ensure users still need roles
References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Question: 14

Note: This question is part of 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 Active Directory (Azure AD) tenant named contoso.com.
A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other Identity Governance settings are available.
Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.
You need to ensure that Admin1 can create access reviews in contoso.com.
Solution: You create an access package.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
You do not use access packages for Identity Governance. Instead use Azure AD Privileged Identity Management.
Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include:
Conduct access reviews to ensure users still need roles
References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview

Question: 15

Note: This question is part of 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 Active Directory (Azure AD) tenant named contoso.com.
A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other Identity Governance settings are available.
Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.
You need to ensure that Admin1 can create access reviews in contoso.com.
Solution: You assign the Service administrator role to Admin1.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use Azure AD Privileged Identity Management.
Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include:
• Conduct access reviews to ensure users still need roles
References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Question: 16

You have an Azure SQL database named Db1 that runs on an Azure SQL server named SQLserver1.
You need to ensure that you can use the query editor on the Azure portal to query Db1.
What should you do?

A. Modify the Advanced Data Security settings of Db1
B. Configure the Firewalls and virtual networks settings for SQLserver1
C. Copy the ADO.NET connection string of Db1 and paste the string to the query editor
D. Approve private endpoint connections for SQLserver1

Answer: B

Reference:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-connect-query-portal

Question: 17

HOTSPOT
You have an Azure subscription that contains the Azure SQL servers shown in the following table.

Name	Region	In resource group
Sql1	West US	RG1
Sql2	West US	RG1

The subscription contains the elastic pool shown in the following table.

Name	On Azure SQL server
Pool1	Sql1
Pool2	Sql1
Pool3	Sql2

The subscription contains the Azure SQL databases shown in the following table.

Name	On Azure SQL server	Pool
DB1	Sql1	Pool1
DB2	Sql1	Pool2
DB3	Sql1	*None*

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
DB1 can be removed from Pool1 and added to Pool2.	○	○
DB2 can be removed from Pool2 and added to Pool3.	○	○
DB3 can be added to Pool1.	○	○

Answer:

Statements	Yes	No
DB1 can be removed from Pool1 and added to Pool2	○	○
DB2 can be removed from Pool2 and added to Pool3	○	○
DB3 can be added to Pool1	○	○

Explanation:
Note: You cannot add databases from different servers into the same pool
Box 1: Yes
Pool2 contains DB2 but DB1 and DB2 are on Sql1. DB1 can thus be added to Pool2.
Box 2: Yes
Pool3 is empty.
Box 3: Yes
Pool1 contains DB1 but DB3 and DB1 are on Sql1. DB3 can thus be added to Pool1.
References:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-elastic-pool

Question: 18

HOTSPOT
You have the Azure SQL Database servers shown in the following table.

Name	Elastic pool
sqlserver1	Pool1
sqlserver2	Pool1, Pool2

You have the Azure SQL databases shown in the following table.

Name	Azure SQL Database server	Elastic pool
DB1	sqlserver1	*None*
DB2	sqlserver1	Pool1
DB3	sqlserver2	Pool1
DB4	sqlserver2	Pool2

You create a failover group named failover1 that has the following settings:
- Primary server: sqlserver1
- Secondary server: sqlserver2
- Read/Write failover policy: Automatic
- Read/Write grace period (hours): 1 hour

Statements	Yes	No
You can add DB1 to failover1.	○	○
You can add DB3 to failover1.	○	○
Sqlserver1 and sqlserver2 are in the same Azure region.	○	○

Answer:

Statements	Yes	No
You can add DB1 to failover1.	○	○
You can add DB3 to failover1.	○	○
Sqlserver1 and sqlserver2 are in the same Azure region.	○	○

Question: 19

Your company plans to develop an application that will use a NoSQL database. The database will be used to store transactions and customer information by using JSON documents. Which two Azure Cosmos DB APIs can developers use for the application? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Cassandra
B. Gremlin (graph)
C. MongoDB
D. Azure Table
E. Core (SQL)

Answer: DE

Question: 20

You have two Azure SQL Database managed instances in different Azure regions.
You plan to configure the managed instances in an instance failover group.
What should you configure before you can add the managed instances to the instance failover group?

A. Azure Private Link that has endpoints on two virtual networks
B. an internal Azure Load Balancer instance that has managed instance endpoints in a backend pool
C. an Azure Application Gateway that has managed instance endpoints in a backend pool

D. a Site-to-Site VPN between the virtual networks that contain the instances

Answer: D

Explanation:
For two managed instances to participate in a failover group, there must be either ExpressRoute or a gateway configured between the virtual networks of the two managed instances to allow network communication.
You create the two VPN gateways and connect them.
• Create the gateway for the virtual network of your primary managed instance using the Azure portal.
• Create the gateway for the virtual network of your secondary managed instance using the Azure portal.
• Create a bidirectional connection between the two gateways of the two virtual networks.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/failover-group-add-instance-tutorial?tabs=azure-portal#4---create-a-primary-gateway

Question: 21

You have an Azure Cosmos DB account named Account1. Account1 includes a database named DB1 that contains a container named Container 1. The partition key tor Container1 is set to /city.
You plan to change the partition key for Container1
What should you do first?

A. Delete Container1
B. Create a new container in DB1
C. Regenerate the keys for Account1.
D. Implement the Azure CosmosDB.NET SDK

Answer: B

Explanation:
The good news is that there are two features, the Change Feed Processor and Bulk Executor Library, in Azure Cosmos DB that can be leveraged to achieve a live migration of your data from one container to another. This allows you to re-distribute your data to match the desired new partition key scheme, and make the relevant application changes afterwards, thus achieving the effect of "updating your partition key".
Reference:
https://devblogs.microsoft.com/cosmosdb/how-to-change-your-partition-key/

Question: 22

HOTSPOT
From Azure Cosmos DB, you create the containers shown in the following table.

Container ID	Partition key	Unique key
Container1	/category	*None*
Container2	/id	/importance

You add the following item to Container1.

```
{
    "id": "1",
    "category": "personal",
    "name": "Name1",
    "description": "Description1"
}
```

You plan to add items to Azure Cosmos DB as shown in the following table.

Name	Content
Item1	{ "id": "1", "category": "personal", "name": "Name1", "description": "Description1" }
Item2	{ "category": "business", "name": "Name2", "description": "Description2" "importance": "High" }
Item3	{ "id": "3", "name": "Name3", "description": "Description3" }
Item4	{ "id": "4", "importance": "Low" }

You need to identify which items can be added successfully to Container1 and Container2.
What should you identify for each container? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Container1:

- Item2 only
- Item1 and Item2 only
- Item3 and Item4 only
- Item2, Item3, and Item4 only
- Item1, Item2, Item3, and Item4

Container2:

- Item4 only
- Item2 and Item4 only
- Item1, Item3, and Item4 only
- Item1, Item2, Item3, and Item4

Answer:

Container1:

- Item2 only
- Item1 and Item2 only
- Item3 and Item4 only
- Item2, Item3, and Item4 only
- **Item1, Item2, Item3, and Item4**

Container2:

- Item4 only
- **Item2 and Item4 only**
- Item1, Item3, and Item4 only
- Item1, Item2, Item3, and Item4

Question: 23

You have the virtual machines shown in the following table.

Name	Operating system	Connected to
VM1	Red Hat Enterprise Linux 7.7	VNET1
VM2	Windows Server 2019	VNET2
VM3	Windows Server 2019	VNET3

You deploy an Azure bastion named Bastion1 to VNET1.
To which virtual machines can you connect by using Bastion1?

A. VM1 only
B. VM1 and VM2 only
C. VM2 and VM3 only
D. VM1, VM2, and VM3

Answer: C

Question: 24

You have an Azure subscription.
You create a custom role in Azure by using the following Azure Resource Manager template.

```
{
  "Name": "Role1",
  "Id": "88888888-8888-8888-888888888888",
  "IsCustom" : true,
  "Description" : "Role1 Description",
  "Actions" : [
     "Microsoft.Storage/*/read",
     "Microsoft.Network/*/read",
     "Microsoft.Compute/*/read",
     "Microsoft.Compute/virtualMachines/start/action",
     "Microsoft.Compute/virtualMachines/restart/action",
     "Microsoft.Authorization/*/read",
     "Microsoft.ResourceHealth/availabilityStatuses/read",
     "Microsoft.Resources/subscriptions/resourceGroups/read",
     "Microsoft.Insights/alertRules/*",
     "Microsoft.Insights/diagnosticSettings/*",
     "Microsoft.Support/*"
 ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions" : [],
  "AssignableScopes" : [
     "/subscriptions/981dd4bc-8cf4-46fc-9513-0c599648b44b
 ]
}
```

You assign the role to a user named User1.
Which action can User1 perform?

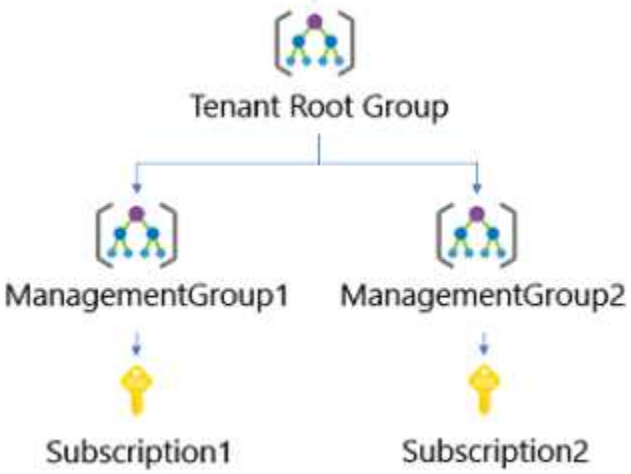
A. Delete virtual machines.
B. Create resource groups.
C. Create virtual machines.
D. Create support requests

Answer: D

Explanation:
The "Microsoft.Support/*" operation will allow the user to create support tickets.
References:
https://docs.microsoft.com/en-us/azure/role-based-access-control/tutorial-custom-role-powershell

Question: 25

HOTSPOT
You have a hierarchy of management groups and Azure subscriptions as shown in the following table.



You create the Azure resources shown in the following table.

Name	Type	Created in
RG1	Resource group	Subscription1
RG2	Resource group	Subscription2
VM2	Virtual machine	RG2

You assign roles to users as shown in the following table.

User name	Role	On resource
User1	Contributor	ManagementGroup1
User2	Contributor	ManagementGroup2
User3	Reader	Tenant Root Group

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
You can remove User1 from the Contributor role for RG1.	○	○
User2 can delete VM2.	○	○
You can add User3 as a Contributor for RG1.	○	○

Answer:

Statements	Yes	No
You can remove User1 from the Contributor role for RG1.	○	○
User2 can delete VM2.	○	○
You can add User3 as a Contributor for RG1.	○	○

Question: 26

You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.

Name	Operating system	Resource group	Location
VM1	Windows Server 2012 R2	RG1	East US
VM2	Windows Server 2016	RG1	West US
VM3	Windows Server 2019	RG2	West US
VM4	Red Hat Enterprise Linux 7.7	RG2	West US
VM5	Ubuntu Server 18.04 LTS	RG1	East US
VM6	CentOS-based 7.7	RG1	East US

You need to ensure that all critical and security updates are applied to each virtual machine every month. What is the minimum number of update deployments you should create?

A. 4
B. 6
C. 1
D. 2

Answer: A

Question: 27

You have an Azure Active Directory (Azure AD) tenant linked to an Azure subscription. The tenant contains a group named Admins.
You need to prevent users, except for the members of Admins, from using the Azure portal and Azure PowerShell to access the subscription.
What should you do?

A. From Azure AD, configure the User settings.
B. From the Azure subscription, assign an Azure policy.
C. From Azure AD, create a conditional access policy.

D. From the Azure subscription, configure Access control (IAM).

Answer: D

Question: 28

HOTSPOT
You have an Azure subscription that contains a resource group named RG1.
You have a group named Group1 that is assigned the Contributor role for RG1.
You need to enhance security for the virtual machines in RG1 to meet the following requirements:
• Prevent Group1 from assigning external IP addresses to the virtual machines.
• Ensure that Group1 can establish an RDP connection to the virtual machines through a shared external IP address.
What should you use to meet each requirement? To answer, select the appropriate options in the answer are
a. NOTE: Each correct selection is worth one point.

Prevent Group1 from assigning external IP addresses to the virtual machines:

- Azure Policy
- Azure Bastion
- Virtual network service endpoints
- Azure Firewall
- Azure Web Application Firewall (WAF)

Ensure that Group1 can establish an RDP connection to the virtual machines through a shared external IP address:

- Azure Policy
- Azure Bastion
- Virtual network service endpoints
- Azure Firewall
- Azure Web Application Firewall (WAF)

Answer:

Prevent Group1 from assigning external IP addresses to the virtual machines:

- Azure Policy
- Azure Bastion
- **Virtual network service endpoints**
- Azure Firewall
- Azure Web Application Firewall (WAF)

Ensure that Group1 can establish an RDP connection to the virtual machines through a shared external IP address:

- **Azure Policy**
- Azure Bastion
- Virtual network service endpoints
- Azure Firewall
- Azure Web Application Firewall (WAF)

Question: 29

You have Azure virtual machines deployed to three Azure regions. Each region contains a single virtual network that has four virtual machines on the same subnet. Each virtual machine runs an application named App1. App1 is accessible by using HTTPS. Currently, the virtual machines are inaccessible from the internet.
You need to use Azure Front Door to load balance requests for App1 across all the virtual machines.
Which additional Azure service should you provision?

A. a public Azure Load Balancer
B. Azure Traffic Manager
C. an internal Azure Load Balancer
D. Azure Private Link

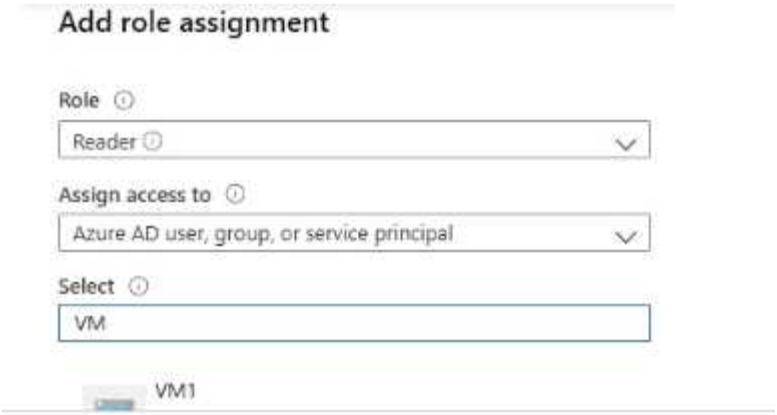
Answer: A

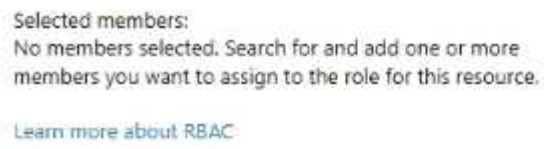
Question: 30

You create the Azure resources shown in the following table.

Name	Resource type
VM1	Virtual machine
VM2	Virtual machine
Managed1	Managed identity
Managed2	Managed identity

You attempt to add a role assignment to a resource group as shown in the following exhibit.





What should you do to ensure that you can assign VM2 the Reader role for the resource group?

A. Modify the Reader role at the subscription level.
B. Configure just in time (JIT) VM access on VM2.
C. Configure Access control (IAM) on VM2.
D. Assign a managed identity to VM2.

Answer: D

Question: 31

You have SQL Server on an Azure virtual machine named SQL1.
You need to automate the backup of the databases on SQL1 by using Automated Backup v2 for the virtual machines. The backups must meet the following requirements:
- Meet a recovery point objective (RPO) of 15 minutes.
- Retain the backups for 30 days.
- Encrypt the backups at rest.

What should you provision as part of the backup solution?

A. Azure Key Vault
B. an Azure Storage account
C. a Recovery Services vault
D. Elastic Database jobs

Answer: B

Explanation:
An Azure storage account is used for storing Automated Backup files in blob storage. A container is created at this location to store all backup files. The backup file naming convention includes the date, time, and database GUID.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/automated-backup

Question: 32

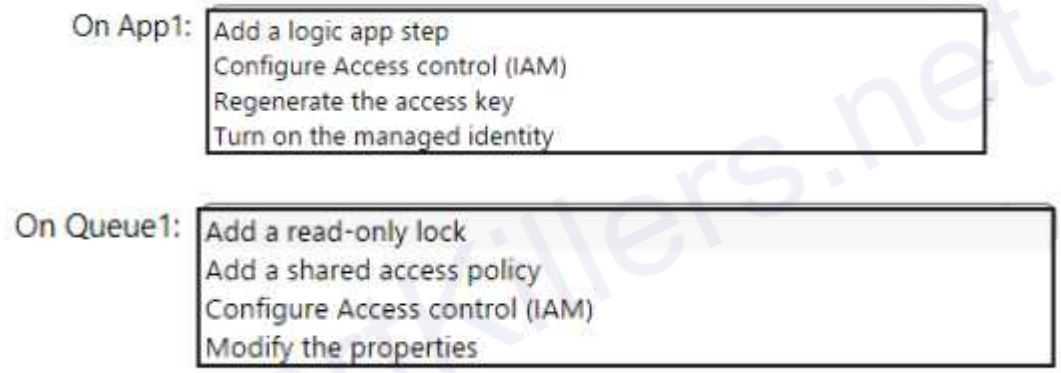
You have an Azure Container Registry and an Azure container instance.
You pull an image from the registry, and then update the local copy of the image.
You need to ensure that the updated image can be deployed to the container instance. The solution must ensure that you can deploy the updated image or the previous version of the image.
What should you do?

A. Run the docker image push command and specify the tag parameter.
B. Run the az image copy command and specify the tag parameter. Run the az aks update command and specify the attach-acr parameter.
C. Run the kubect1 apply command and specify the dry-run parameter.

Answer: B

Question: 33

HOTSPOT
You have an Azure logic app named App1 and an Azure Service Bus queue named Queue1.
You need to ensure that App1 can read messages from Queue1. App1 must authenticate by using Azure Active Directory (Azure AD).
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

On App1:

Add a logic app step
Configure Access control (IAM)
Regenerate the access key
Turn on the managed identity

On Queue1:

Add a read-only lock
Add a shared access policy
Configure Access control (IAM)
Modify the properties

Explanation:
On App1: Turn on the managed identity
To use Service Bus with managed identities, you need to assign the identity the role and the appropriate scope. The procedure in this section uses a simple application that runs under a managed identity and accesses Service Bus resources.
Once the application is created, follow these steps:
• Go to Settings and select Identity.
• Select the Status to be On.
• Select Save to save the setting.
On Queue1: Configure Access Control (IAM)
Azure Active Directory (Azure AD) authorizes access rights to secured resources through role-based access control (RBAC). Azure Service Bus defines a set of built-in RBAC roles that encompass common sets of permissions used to access Service Bus entities and you can also define custom roles for accessing the data.
Assign RBAC roles using the Azure portal
In the Azure portal, navigate to your Service Bus namespace. Select Access Control (IAM) on the left menu to display access control settings for the namespace. If you need to create a Service Bus namespace.
Select the Role assignments tab to see the list of role assignments. Select the Add button on the toolbar and then select Add role assignment.
Reference:
https://docs.microsoft.com/en-us/azure/service-bus-messaging/authenticate-application
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-managed-service-identity

Question: 34

You have an Azure Kubernetes Service (AKS) cluster named Clus1 in a resource group named RG1.
An administrator plans to manage Clus1 from an Azure AD-joined device.

You need to ensure that the administrator can deploy the YAML application manifest file for a container application.
You install the Azure CLI on the device.
Which command should you run next?

A. kubectl get nodes
B. az aks install-cli
C. kubectl apply –f app1.yaml
D. az aks get-credentials --resource-group RG1 --name Clus1

Answer: C

Explanation:
kubectl apply –f appl.yaml applies a configuration change to a resource from a file or stdin.
References:
https://kubernetes.io/docs/reference/kubectl/overview/
https://docs.microsoft.com/en-us/cli/azure/aks

Question: 35

You create a container image named Image1 on a developer workstation.
You plan to create an Azure Web App for Containers named WebAppContainer that will use Image1.
You need to upload Image1 to Azure. The solution must ensure that WebAppContainer can use Image1.
To which storage type should you upload Image1?

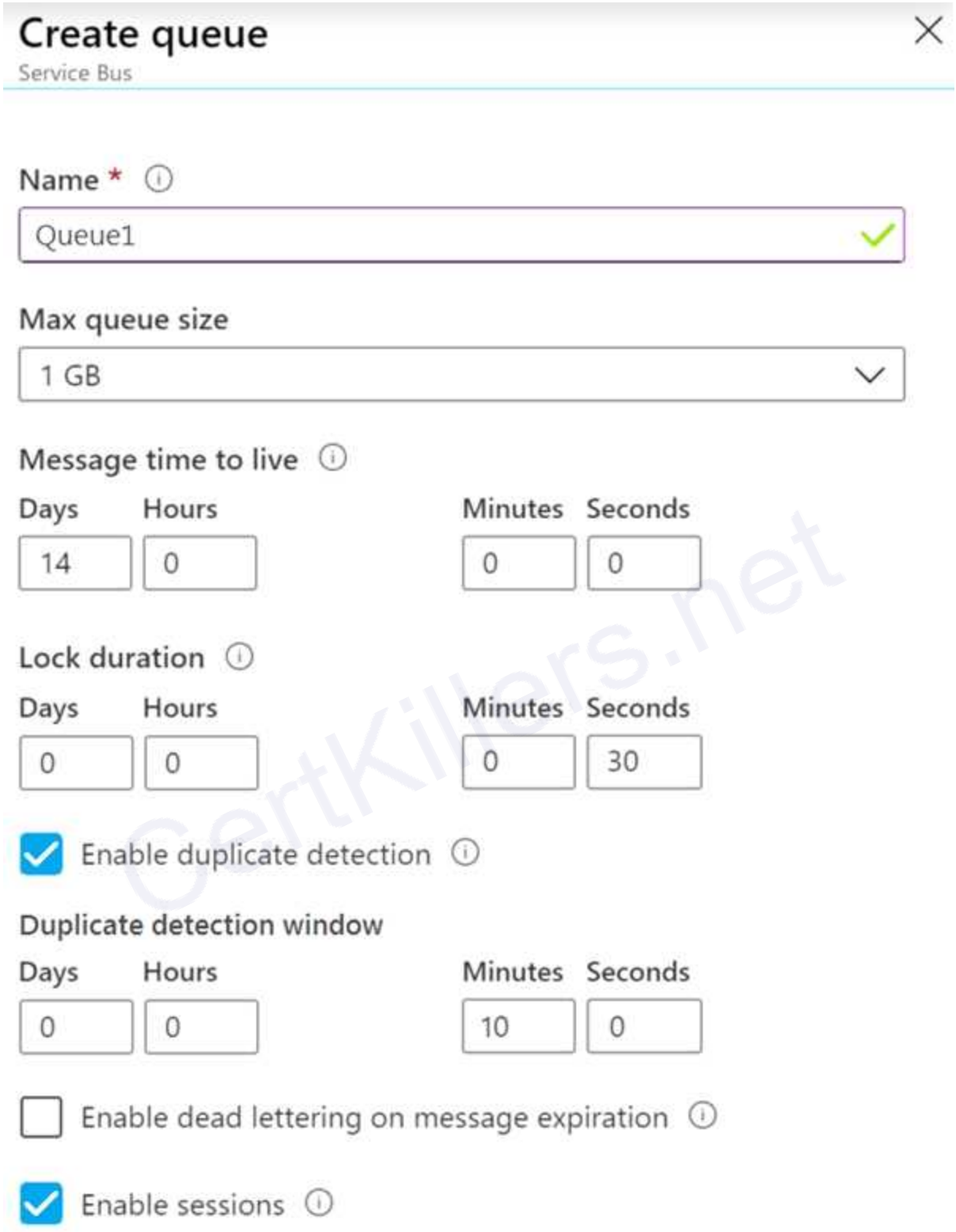
A. Azure Container Registry
B. an Azure Storage account that contains a blob container
C. an Azure Storage account that contains a file share
D. Azure Container Instances

Answer: A

Explanation:
Configure registry credentials in web app.
App Service needs information about your registry and image to pull the private image. In the Azure portal, go to Container settings from the web app and update the Image source, Registry and save.
References:
https://docs.microsoft.com/en-us/azure/devops/pipelines/targets/webapp-on-container-linux

Question: 36

You have an Azure Service Bus and two clients named Client1 and Client2.
You create a Service Bus queue named Queue1 as shown in the exhibit. (Click the Exhibit tab.)



Client1 sends messages to Queue1 as shown in the following table.

Time hh:mm:ss	Message
12:01:01	M3
12:01:02	M2
12:01:03	M1
12:01:04	M3

Client2 reads the messages from Queue1 at 12:01:05.
How will the messages be presented to Client2?

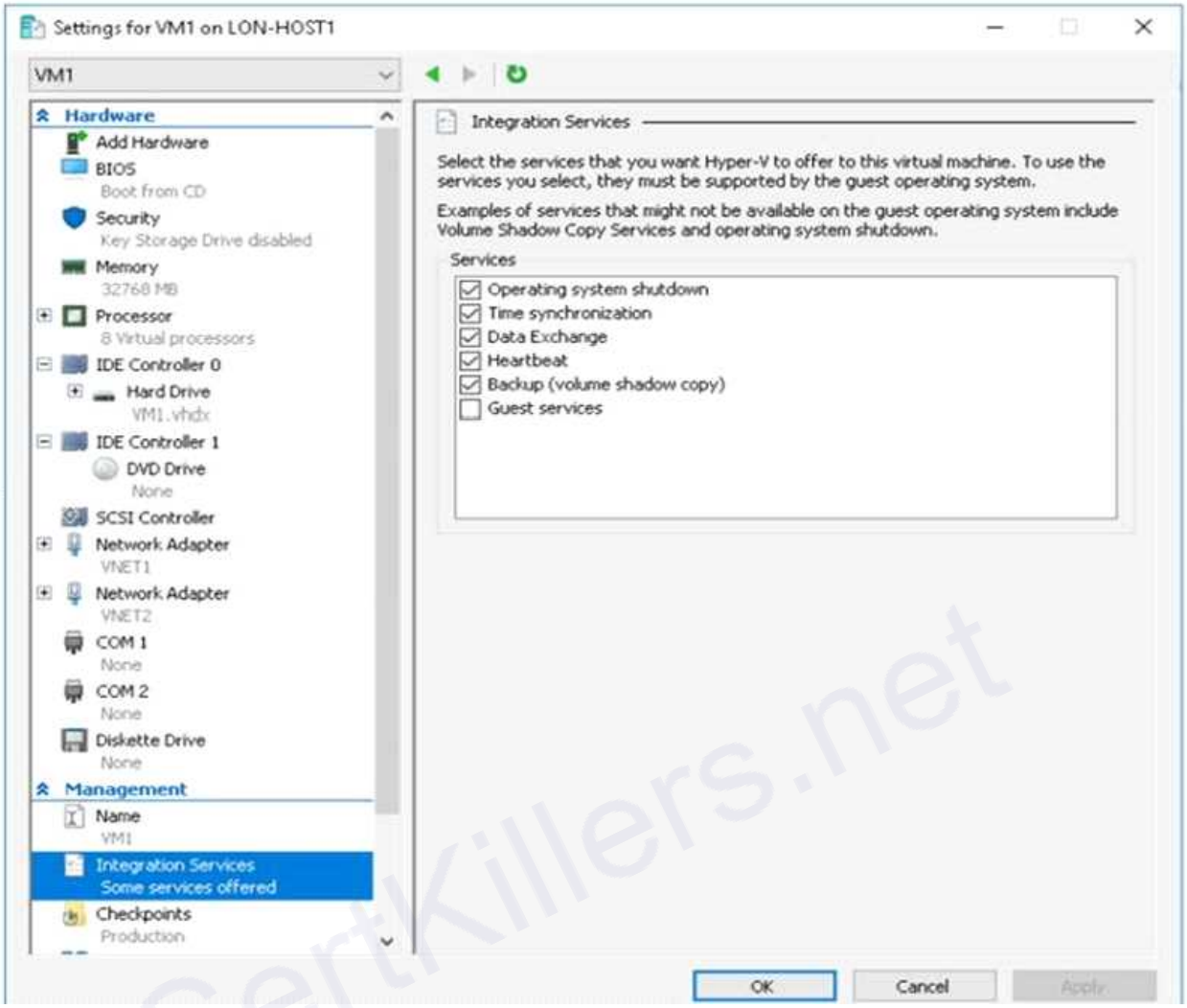
A. Client2 will read four messages in the following order: M3, M2, M1, and then M3.
B. Client2 will read three messages in the following order: M3, M2, and then M1.
C. Client2 will read four messages in the following order; M3, M1, M2, and then M3.
D. Client2 will read three messages in the following order: M1, M2. and then M3
E. Client2 will read three messages in the following order: M3, M1, and then M2.

Answer: B

Explanation:
Duplicate is enabled, and the duplication detection window is set to 10 minutes. The second M3 message in the queue will be discarded.
Note 1: Duplicate detection enables the sender resend the same message, and the queue or topic discards any duplicate copies.
Note 2: Queues offer First In, First Out (FIFO) message delivery to one or more competing consumers. That is, receivers typically receive and process messages in the order in which they were added to the queue, and only one message consumer receives and processes each message.
References:
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-queues-topics-subscriptions
https://docs.microsoft.com/en-us/azure/service-bus-messaging/duplicate-detection

Question: 37

You have an on-premises virtual machine named VM1 configured as shown in the following exhibit.



VM is started.

You need to create a new virtual machine image in Azure from VM1.

Which three actions should you perform before you create the new image? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Remove the Backup (volume shadow copy) integration service
B. Generalize VM1
C. Run Add-AzureRmVhd and specify a blob service container as the destination
D. Run Add-AzureRmVhd and specify a file share as the destination
E. Reduce the amount of memory to 16 GB
F. Convert the disk type to VHD

Answer: BCF

Question: 38

HOTSPOT
You have an Azure subscription that contains the resource groups shown in the following table.

Name	Region
RG1	East US
RG2	West US

RG1 contains the virtual machines shown in the following table.

Name	Region
VM1	West US
VM2	West US
VM3	West US
VM4	West US

RG2 contains the virtual machines shown in the following table.

Name	Region
VM5	East US 2
VM6	East US 2
VM7	West US
VM8	West US 2

All the virtual machines are configured to use premium disks and are accessible from the Internet.
VM1 and VM2 are in an available set named AVSET1. VM3 and VM4 are in the same availability zone and are in an availability set named AVSET2. VM5 and VM6 are in different availability zones.
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
VM1 is eligible for a Service Level Agreement (SLA) of 99,95 percent.	○	○
VM3 is eligible for a Service Level Agreement (SLA) of 99,99 percent.	○	○
VM5 is eligible for a Service Level Agreement (SLA) of 99,99 percent.	○	○

Answer:

Statements	Yes	No
VM1 is eligible for a Service Level Agreement (SLA) of 99,95 percent.	○	○
VM3 is eligible for a Service Level Agreement (SLA) of 99,99 percent.	○	○
VM5 is eligible for a Service Level Agreement (SLA) of 99,99 percent.	○	○

Explanation:
Box 1: Yes
VM1 and VM2 are in an available set named AVSET1.
For all Virtual Machines that have two or more instances deployed in the same Availability Set, we [Microsoft] guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.95% of the time.
Box 2: No
VM3 and VM4 are in the same availability zone and are in an availability set named AVSET2.
Box 3: Yes
VM5 and VM6 are in different availability zones.
For all Virtual Machines that have two or more instances deployed across two or more Availability Zones in the same Azure region, we [Microsoft] guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.99% of the time.
References:
https://azure.microsoft.com/en-us/support/legal/sla/virtual-machines/v1_8/

Question: 39

HOTSPOT
Your network contains an on-premises Active Directory domain named contoso.com that contains a user named User1. The domain syncs to Azure Active Directory (Azure AD). You have the Windows 10 devices shown in the following table.

Name	Joined to
Device1	On-premises Active Directory
Device2	Azure AD
Device3	Workgroup

The User Sign-In settings are configured as shown in the following exhibit.

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Disabled	0 agents

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 accessing the Azure portal from Device1, User1 will sign in automatically by using SSO.	○	○
When accessing the Azure portal from Device2, User1 will sign in automatically by using SSO.	○	○
When accessing the Azure portal from Device3, User1 will sign in automatically by using SSO.	○	○

Answer:

Statements	Yes	No
When accessing the Azure portal from Device1, User1 will sign in automatically by using SSO.	○	○
When accessing the Azure portal from Device2, User1 will sign in automatically by using SSO.	○	○
When accessing the Azure portal from Device3, User1 will sign in automatically by using SSO.	○	○

Question: 40

You have an Azure subscription named Subscription1 that contains an Azure virtual network named VNet1. VNet1 connects to your on-premises network by using Azure ExpressRoute.
You need to connect VNet1 to the on-premises network by using a site-to-site VPN. The solution

must minimize cost.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Create a VPN gateway that uses the VpnGw1 SKU.
B. Create a connection.
C. Create a local site VPN gateway.
D. Create a gateway subnet.
E. Create a VPN gateway that uses the Basic SKU.

Answer: ABC

Explanation:
References:
https://docs.microsoft.com/en-za/archive/blogs/canitpro/step-by-step-configuring-a-site-to-site-vpn-gateway-between-azure-and-on-premise

Question: 41

You plan to create an Azure Storage account named storage! that will store blobs and be accessed by Azure Databricks.
You need to ensure that you can set permissions for individual blobs by using Azure Active Directory (Azure AD) authentication.
Which Advanced setting should you enable for storage1?

A. Hierarchical namespace
B. Large file shares
C. Blob soft delete
D. NFSv3

Answer: C

Question: 42

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	Member of
User1	Domain Admins
User2	Domain Users
User3	ADSyncAdmins
User4	Account Operators

You plan to install Azure AD Connect and enable SSO.
You need to specify which user to use to enable SSO. The solution must use the principle of least privilege.

Which user should you specify?

A. User4
B. User1
C. User3
D. User2

Answer: C

Question: 43

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

Name	Type	Region	Resource group
RG1	Resource group	Central US	*Not applicable*
RG2	Resource group	West US	*Not applicable*
VM1	Virtual machine	East US	RG2
VNET1	Virtual network	East US	RG1

In RG2, you need to create a new virtual machine named VM2 that will connect to VNET1. VM2 will use a network interface named VM2_Interface.
In which region should you create VM2 and VM2_Interface? To answer, drag the appropriate regions to the correct targets. Each region 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.

Regions

Central US

East US

West US

Answer Area

VM2:

VM2_Interface:

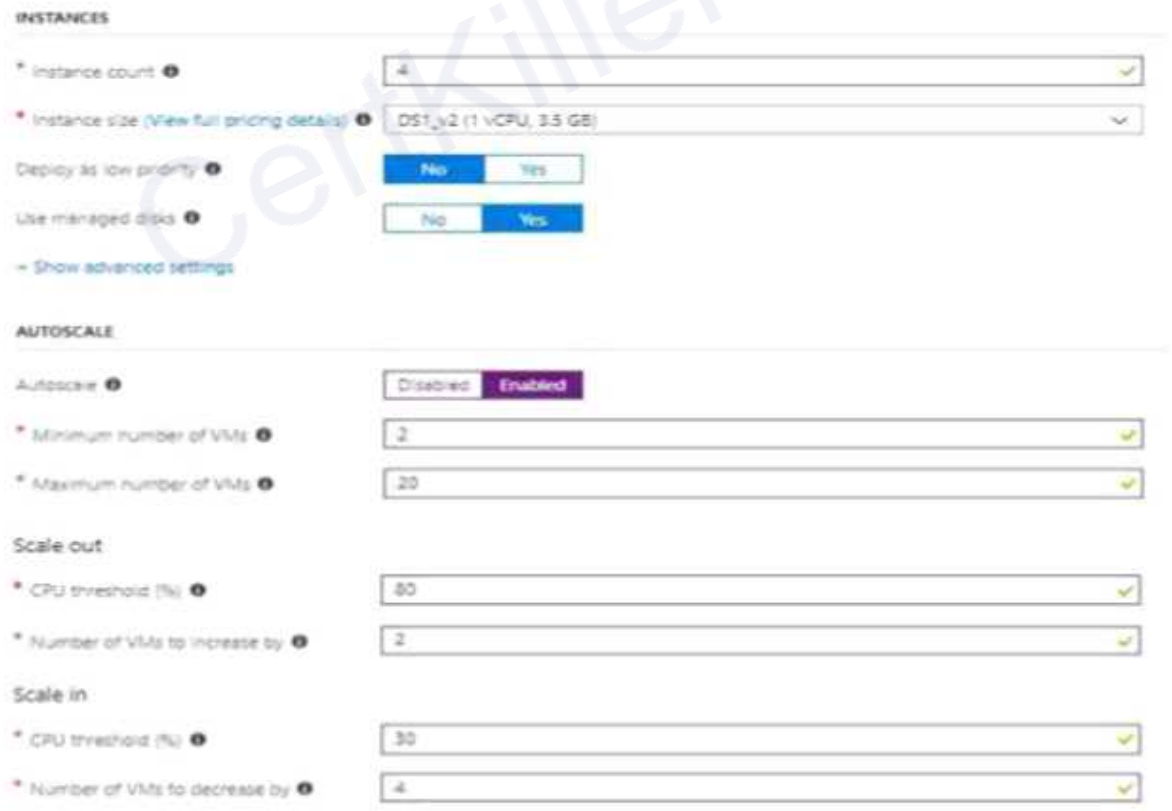
Answer:

VM2:	West US
VM2_Interface:	East US

Explanation:
VM2: West US
In RG2, which is in West US, you need to create a new virtual machine named VM2.
VM2_interface: East US
VM2 will use a network interface named VM2_Interface to connect to VNET1, which is in East US.
References:
https://docs.microsoft.com/en-us/azure/virtual-network/associate-public-ip-address-vm

Question: 44

HOTSPOT
You create a virtual machine scale set named Scale1. Scale1 is configured as shown in the following exhibit.
The subscription contains the Azure SQL databases shown in the following table.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

If Scale1 is utilized at 85 percent for six minutes, Scale1 will be running **[answer choice].**

- 2 virtual machines
- 4 virtual machines
- 6 virtual machines
- 8 virtual machines
- 10 virtual machines

If Scale1 is first utilized at 25 percent for six minutes, and then utilized at 50 percent for six minutes, Scale1 will be running **[answer choice].**

- 2 virtual machines
- 4 virtual machines
- 6 virtual machines
- 8 virtual machines
- 10 virtual machines

Answer:

If Scale1 is utilized at 85 percent for six minutes, Scale1 will be running **[answer choice].**

- 2 virtual machines
- 4 virtual machines
- **6 virtual machines**
- 8 virtual machines
- 10 virtual machines

If Scale1 is first utilized at 25 percent for six minutes, and then utilized at 50 percent for six minutes, Scale1 will be running **[answer choice].**

- **2 virtual machines**
- 4 virtual machines
- 6 virtual machines
- 8 virtual machines
- 10 virtual machines

Explanation:
Box 1:
The Autoscale scale out rule increases the number of VMs by 2 if the CPU threshold is 80% or higher.
The initial instance count is 4 and rises to 6 when the 2 extra instances of VMs are added.
Box 2:
The Autoscale scale in rule decreases the number of VMs by 4 if the CPU threshold is 30% or lower.
The initial instance count is 4 and thus cannot be reduced to 0 as the minimum instances is set to 2.
Instances are only added when the CPU threshold reaches 80%.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-overview
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-best-practices
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-common-scale-patterns

Question: 45

You have an Azure subscription named Subscription1 that is used by several departments at your company. Subscription1 contains the resources in the following table.

Name	Type
Storage1	Storage account
RG1	Resource group
Container1	Blob container
Share1	File share

Another administrator deploys a virtual machine named VM1 and an Azure Storage account named Storage2 by using a single Azure Resource Manager template.
You need to view the template used for the deployment.
From which blade can you view the template that was used for the deployment?

A. Container1
B. VM1
C. Storage2
D. RG1

Answer: D

Question: 46

A company plans to use third-party application software to perform complex data analysis processes. The software will use up to 500 identical virtual machines (VMs) based on an Azure Marketplace VM image.
You need to design the infrastructure for the third-party application server. The solution must meet the following requirements:
• The number of VMs that are running at any given point in time must change when the user workload changes.
• When a new version of the application is available in Azure Marketplace it must be deployed without causing application downtime.
• Use VM scale sets.
• Minimize the need for ongoing maintenance.
Which two technologies should you recommend? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. single storage account
B. autoscale
C. single placement group
D. managed disks

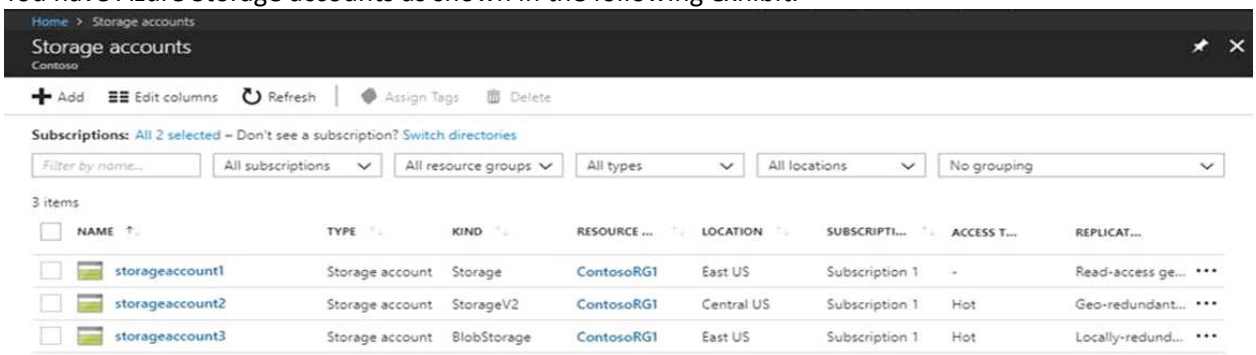
Answer: BD

Explanation:
Introduction to Azure managed disks https://docs.microsoft.com/en-us/azure/virtual-machines/windows/managed-disks-overview "Using managed disks, you can create up to 50,000 VM disks of a type in a subscription per region, allowing you to create thousands of VMs in a single

subscription. This feature also further increases the scalability of virtual machine scale sets by allowing you to create up to 1,000 VMs in a virtual machine scale set using a Marketplace image."

Question: 47

HOTSPOT
You have Azure Storage accounts as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

You can use **[answer choice]** for Azure Table Storage.

- storageaccount1 only
- storageaccount2 only
- storageaccount3 only
- storageaccount1 and storageaccount2 only
- storageaccount2 and storageaccount3 only

You can use **[answer choice]** for Azure Blob storage.

- storageaccount3 only
- storageaccount2 and storageaccount3 only
- storageaccount1 and storageaccount3 only
- all the storage accounts

Answer:

You can use **[answer choice]** for Azure Table Storage.

- storageaccount1 only
- storageaccount2 only
- storageaccount3 only
- storageaccount1 and storageaccount2 only
- storageaccount2 and storageaccount3 only

You can use **[answer choice]** for Azure Blob storage.

- storageaccount3 only
- storageaccount2 and storageaccount3 only
- storageaccount1 and storageaccount3 only
- all the storage accounts

Explanation:
Note: The three different storage account options are: General-purpose v2 (GPv2) accounts, General-purpose v1 (GPv1) accounts, and Blob storage accounts.
• General-purpose v2 (GPv2) accounts are storage accounts that support all of the latest features for blobs, files, queues, and tables.
• Blob storage accounts support all the same block blob features as GPv2, but are limited to supporting only block blobs.
• General-purpose v1 (GPv1) accounts provide access to all Azure Storage services, but may not have the latest features or the lowest per gigabyte pricing.
References:
https://docs.microsoft.com/en-us/azure/storage/common/storage-account-options

Question: 48

DRAG DROP
You have virtual machines (VMs) that run a mission-critical application.
You need to ensure that the VMs never experience down time.
What should you recommend? To answer, drag the appropriate solutions to the correct scenarios. Each solution 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.

Solutions

- Fault Domain
- Availability Zone
- Availability Set
- Scale Sets

Answer area

Scenario	Solution
Maintain application performance across identical VMs.	Solution
Maintain application availability when an Azure datacenter fails.	Solution
Maintain application performance across different VMs.	Solution

Answer:

Scenario	Solution
Maintain application performance across identical VMs.	Scale Sets
Maintain application availability when an Azure datacenter fails.	Availability Set
Maintain application performance across different VMs.	Fault Domain

Explanation:
Box 1: Scale set
A virtual machine scale set allows you to deploy and manage a set of identical, autoscaling virtual machines.
Box 2: Availability Set
An Availability Set is a logical grouping capability for isolating VM resources from each other when they're deployed. Azure makes sure that the VMs you place within an Availability Set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or software failure happens, only a subset of your VMs are impacted and your overall solution stays operational. Availability Sets are essential for building reliable cloud solutions.
Box 3: Fault domain
A fault domain is a logical group of underlying hardware that share a common power source and network switch, similar to a rack within an on-premises datacenter. As you create VMs within an availability set, the Azure platform automatically distributes your VMs across these fault domains. This approach limits the impact of potential physical hardware failures, network outages, or power interruptions.
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-create-vmss
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets

Question: 49

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

Name	Type	Address space
VNET1	Virtual network	10.1.1.0/24
Subnet1	Subnet	10.1.1.0/24
VM1	Virtual machine	*Not applicable*

Subnet1 is on VNET1. VM1 connects to Subnet1.
You plan to create a virtual network gateway on VNET1.
You need to prepare the environment for the planned virtual network gateway.
What are two ways to achieve this goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Create a subnet named GatewaySubnet on VNET1.
B. Delete Subnet1.
C. Modify the address space used by Subnet1.
D. Modify the address space used by VNET1
E. Create a local network gateway.

Answer: AD

Question: 50

Your company has an office in Seattle.
You have an Azure subscription that contains a virtual network named VNET1.
You create a site-to-site VPN between the Seattle office and VNET1.
VNET1 contains the subnets shown in the following table.

Name	IP address space
Subnet1	10.1.1.0/24
GatewaySubnet	10.1.200.0/28

You need to redirect all Internet-bound traffic from Subnet1 to the Seattle office.
What should you create?

A. a route for Subnet1 That uses the virtual network gateway as the next hop
B. a route for GatewaySubnet that uses the virtual network gateway as the next hop
C. a route for GatewaySubnet that uses the local network gateway as the next hop
D. a route for Subnet1 that uses The local network gateway as the next hop

Answer: B

Explanation:
A route with the 0.0.0.0/0 address prefix instructs Azure how to route traffic destined for an IP address that is not within the address prefix of any other route in a subnet's route table. When a subnet is created, Azure creates a default route to the 0.0.0.0/0 address prefix, with the Internet next hop type. We need to create a custom route in Azure to use a virtual network gateway in the Seattle office as the next hop.
References:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

Question: 51

You create an Azure virtual machine named VM1 in a resource group named RG1.
You discover that VM1 performs slower than expected.
You need to capture a network trace on VM1.
What should you do?

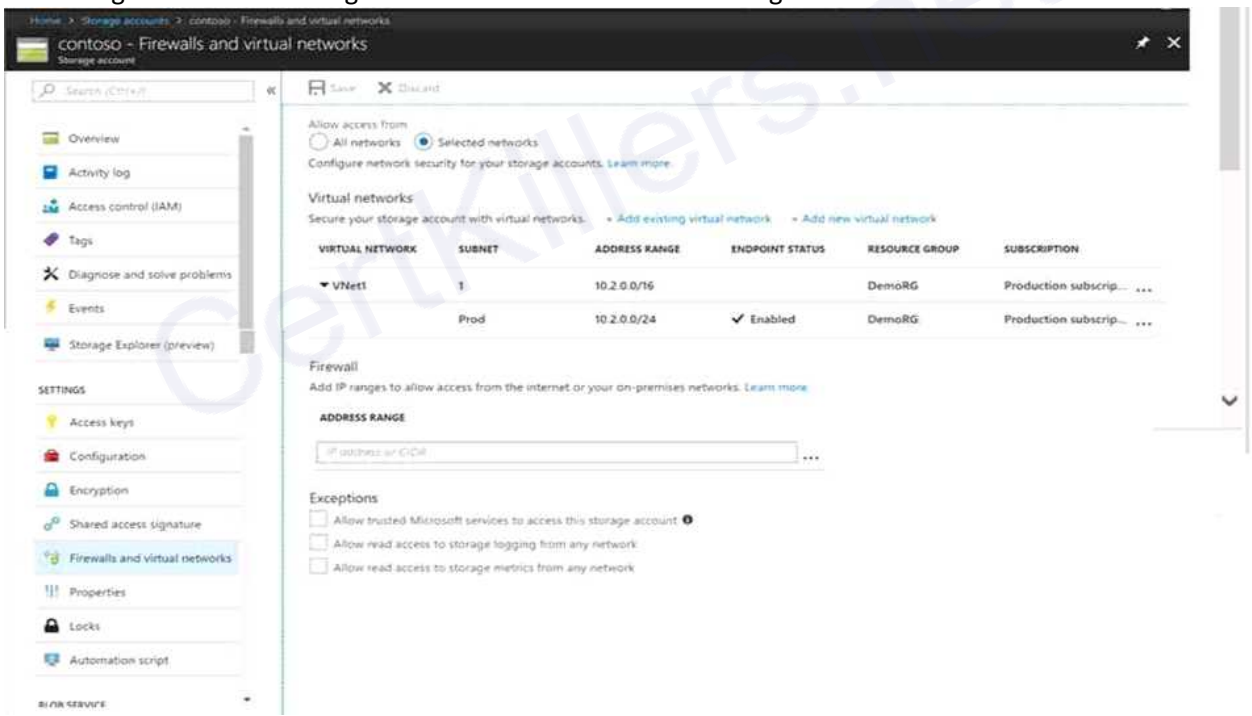
A. From Diagnostic settings for VM1. configure the performance counters to include network counters.
B. From the VM1 blade, configure Connection troubleshoot.
C. From the VM1 blade, install performance diagnostics and run advanced performance analysis
D. From Diagnostic settings for VM1, configure the log level of the diagnostic agent.

Answer: C

Explanation:
The performance diagnostics tool helps you troubleshoot performance issues that can affect a Windows or Linux virtual machine (VM). Supported troubleshooting scenarios include quick checks on known issues and best practices, and complex problems that involve slow VM performance or high usage of CPU, disk space, or memory.
Advanced performance analysis, included in the performance diagnostics tool, includes all checks in the performance analysis, and collects one or more of the traces, as listed in the following sections. Use this scenario to troubleshoot complex issues that require additional traces. Running this scenario for longer periods will increase the overall size of diagnostics output, depending on the size of the VM and the trace options that are selected.
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/performance-diagnostics

Question: 52

HOTSPOT
You have several Azure virtual machines on a virtual network named VNet1.
You configure an Azure Storage account as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

The virtual machines on the 10.2.9.0/24 subnet will have network connectivity to the file shares in the storage account **[answer choice]**.

always
during a backup
never

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account **[answer choice]**.

always
during a backup
never

Answer:

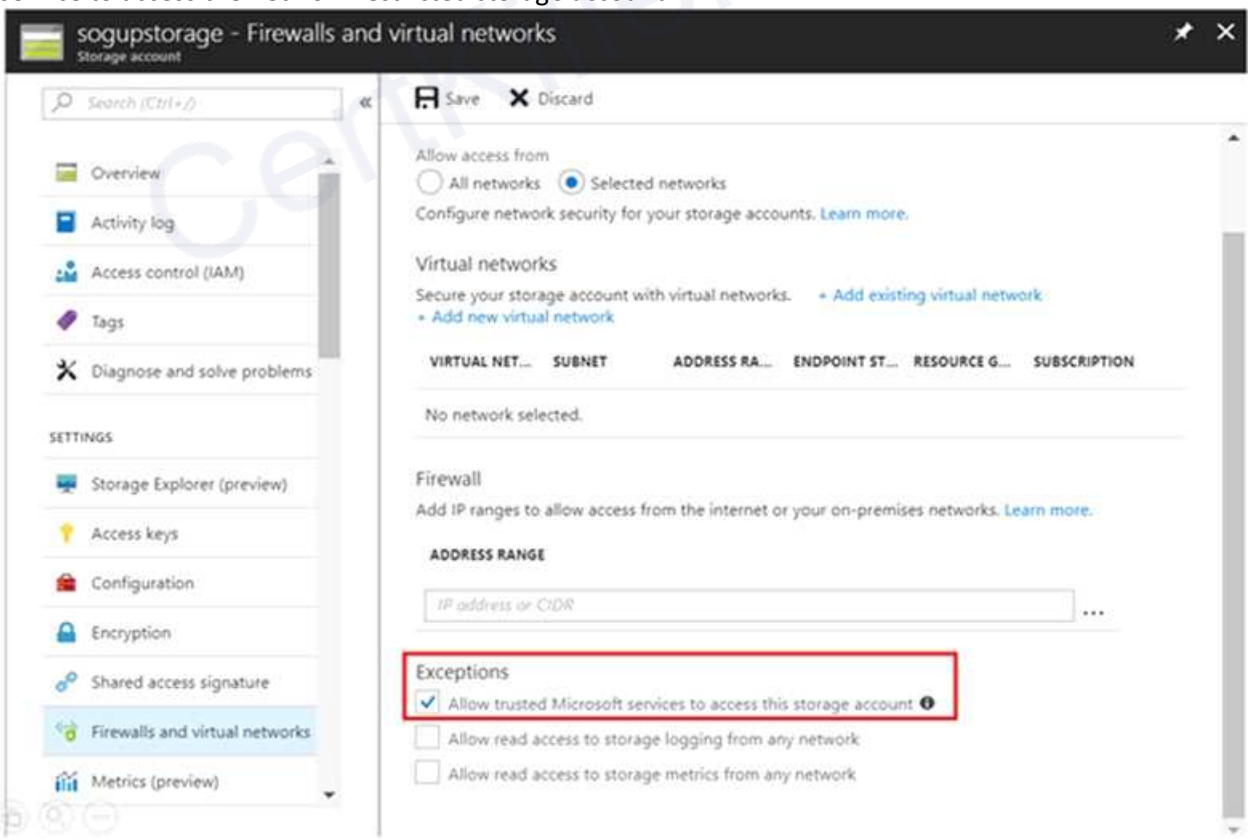
The virtual machines on the 10.2.9.0/24 subnet will have network connectivity to the file shares in the storage account **[answer choice]**.

always
during a backup
never

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account **[answer choice]**.

always
during a backup
never

Explanation:
Box 1: Never
Box 2: Never
After you configure firewall and virtual network settings for your storage account, select Allow trusted Microsoft services to access this storage account as an exception to enable Azure Backup service to access the network restricted storage account.



Reference:
https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows
https://azure.microsoft.com/en-us/blog/azure-backup-now-supports-storage-accounts-secured-with-azure-storage-firewalls-and-virtual-networks/

Question: 53

HOTSPOT
You create and save an Azure Resource Manager template named Template1 that includes the following four sections.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
      "windowsOSVersion": {
            "defaultValue": "2019-Datacenter",
            "allowedValues": [
                "2012-Datacenter",
                "2012-R2-Datacenter",
                "2016-Datacenter",
                "2019-Datacenter"
            ],
            }
       },
```

Section2.

```
    "variables": {
       "windowsOSVersion": "2012-Datacenter",
```

Section3.

```
     },
    "resources": [
      {
      "type": "Microsoft.Compute/virtualMachines",
```

Section4.

```
        "storageProfile": {
            "imageReference": {
                "publisher": "MicrosoftWindowsServer",
                "offer": "WindowsServer",
                "sku": "2012-R2-Datacenter",
                "version": "latest"
                },
```

You deploy template1.
For each of the following statement, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Windows Server 2012 R2 Datacenter will be deployed to the Azure virtual machine.	○	○
A custom image of Windows Server will be deployed.	○	○
During the deployment of Template1, an administrator will be prompted to select a version of Windows Server.	○	○

Answer:

Statements	Yes	No
Windows Server 2012 R2 Datacenter will be deployed to the Azure virtual machine.	○	○
A custom image of Windows Server will be deployed.	○	○
During the deployment of Template1, an administrator will be prompted to select a version of Windows Server.	○	○

Question: 54

A company hosts virtual machines (VMs) in an on-premises datacenter and in Azure. The on-premises and Azure-based VMs communicate using ExpressRoute.
The company wants to be able to continue regular operations if the ExpressRoute connection fails. Failover connections must use the Internet and must not require Multiprotocol Label Switching (MPLS) support.
You need to recommend a solution that provides continued operations.
What should you recommend?

A. Set up a second ExpressRoute connection.
B. Increase the bandwidth of the existing ExpressRoute connection.
C. Increase the bandwidth for the on-premises internet connection.
D. Set up a VPN connection.

Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroutevpn-failover

Question: 55

HOTSPOT
You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Kind	Performance tier	Replication	Location
storage1	StorageV2	Premium	Locally-redundant storage (LRS)	East US
storage2	Storage	Standard	Geo-redundant storage (GRS)	UK West
storage3	BlobStorage	Standard	Locally-redundant storage (LRS)	North Europe

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
storage1 can host Azure file shares.	○	○
There are six copies of the data in storage2.	○	○
storage3 can be converted to a GRS account.	○	○

Answer:

Statements	Yes	No
storage1 can host Azure file shares.	○	●
There are six copies of the data in storage2 stored in Azure datacenters.	●	○
storage3 can be converted to a GRS account.	●	○

Question: 56

You have an Azure subscription that contains an Azure Log Analytics workspace. You have a resource group that contains 100 virtual machines. The virtual machines run Linux. You need to collect events from the virtual machines to the Log Analytics workspace. Which type of data source should you configure in the workspace?

A. Syslog
B. Linux performance counters
C. custom fields

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm
Syslog is an event logging protocol that is common to Linux. Applications will send messages that

may be stored on the local machine or delivered to a Syslog collector. When the Log Analytics agent for Linux is installed, it configures the local Syslog daemon to forward messages to the agent. The agent then sends the message to Azure Monitor where a corresponding record is created.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-custom-logs

Question: 57

HOTSPOT
You have an Azure subscription that includes an Azure key vault named Vault1.
You create the Azure virtual machines shown in the following table.

Name	Operating system disk type	Use managed disks
VM1	Premium SSD	Yes
VM2	Standard HDD	Yes
VM3	Standard SSD	No

You enable Azure Disk Encryption for all the virtual machines and use the –VolumeType All parameter.
You add data disks to the virtual machines as shown in the following table.

Name	Virtual machine	Storage account type
VM1-Disk1	VM1	Premium SSD
VM2-Disk1	VM2	Standard SSD
VM3-Disk1	VM3	Standard HDD

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
VM1-Disk1 is encrypted automatically by using Azure Disk Encryption.	○	○
VM2-Disk1 is encrypted automatically by using Azure Disk Encryption.	○	○
VM3-Disk1 is encrypted automatically by using Azure Disk Encryption.	○	○

Answer:

Statements	Yes	No
VM1-Disk1 is encrypted automatically by using Azure Disk Encryption.	○	○
VM2-Disk1 is encrypted automatically by using Azure Disk Encryption.	○	○
VM3-Disk1 is encrypted automatically by using Azure Disk Encryption.	○	○

Explanation:
Premium and standard, but not basic, account types support disk encryption.
Disk encryption requires managed disks.
References:
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview

Question: 58

You plan to automate the deployment of a virtual machine scale set that uses the Windows Server 2016 Datacenter image. You need to ensure that when the scale set virtual machines are provisioned, they have web server components installed. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Create a new virtual machine scale set in the Azure portal.
B. Create an automation account.
C. Upload a configuration script.
D. Modify the extensionProfile section of the Azure Resource Manager template.
E. Create an Azure policy.

Answer: AD

Explanation:
References:
https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/tutorial-install-apps-template

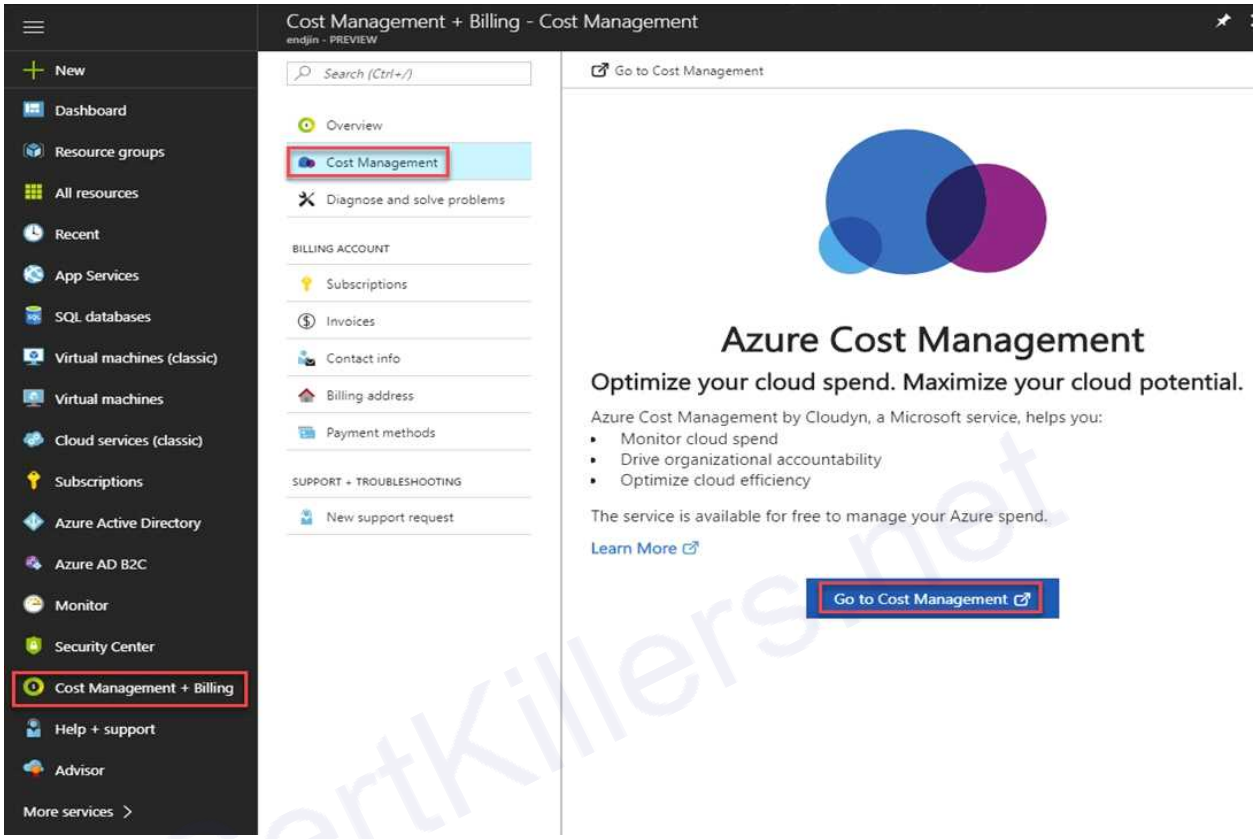
Question: 59

You have an Azure subscription that contains a resource group named RG1. RG1 contains multiple resources.
You need to trigger an alert when the resources in RG1 consume $1,000 USD.
What should you do?

A. From Cost Management + Billing, add a cloud connector.
B. From the subscription, create an event subscription.
C. From Cost Management + Billing create a budget.
D. From RG1, create an event subscription.

Answer: C

Explanation:
Create budgets to manage costs and create alerts that automatically notify you are your stakeholders of spending anomalies and overspending.
To set it up, go to the Azure Portal, select 'Cost Management + Billing' -> 'Cost Management' -> 'Go to Cost Management'.



Note: Cost alerts are automatically generated based when Azure resources are consumed. Alerts show all active cost management and billing alerts together in one place. When your consumption reaches a given threshold, alerts are generated by Cost Management. There are three types of cost alerts: budget alerts, credit alerts, and department spending quota alerts.
Reference:
https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/getting-started

Question: 60

You create a new Azure subscription. You create a resource group named RG1. In RG1. you create the resources shown in the following table.

Name	Type
VNET1	Virtual network
VM1	Virtual machine
GWSN1	Gateway subnet
VPNGW1	Virtual network gateway

You need to configure an encrypted tunnel between your on-premises network and VNET1.

Which two additional resources should you create in Azure? Each correct answer presents part of the solution.

A. a point-to-site configuration
B. a local network gateway
C. a VNet-to-VNet connection
D. a VPN gateway
E. a site-to-site connection

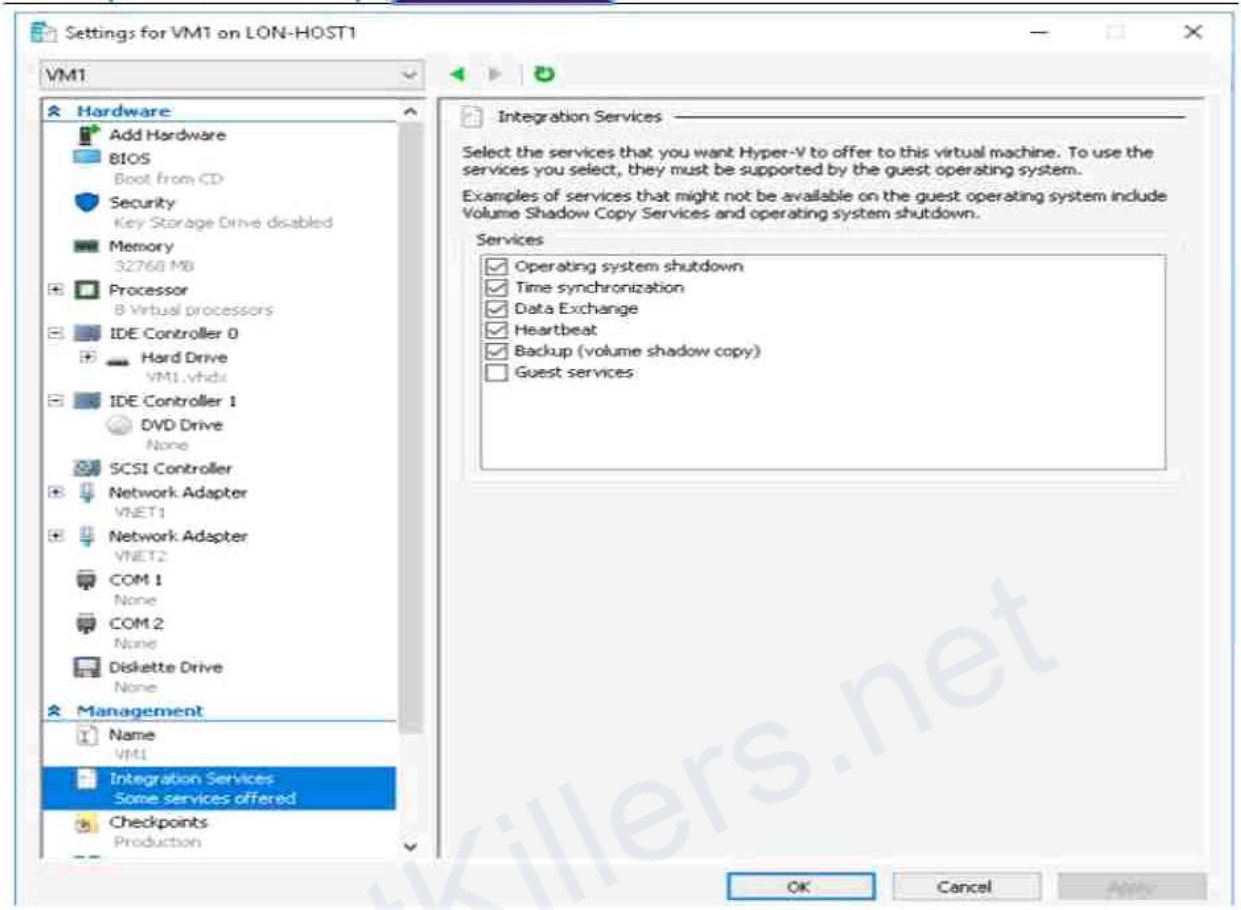
Answer: DE

Explanation:
A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device, a local network gateway, located on-premises that has an externally facing public IP address assigned to it.
Finally, create a Site-to-Site VPN connection between your virtual network gateway and your on-premises VPN device.
References:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

Question: 61

You have an Azure subscription.
You have an on-premises virtual machine named VM1. The settings for VM1 are shown in the exhibit. (Click the Exhibit tab.)

Question Exhibit



You need to ensure that you can use the disks attached to VM1 as a template for Azure virtual machines.
What should you modify on VM1?

A. the hard drive
B. Integration Services
C. the memory
D. the network adapters
E. the processor

Answer: A

Explanation:
From the exhibit we see that the disk is in the VHDX format.
Before you upload a Windows virtual machines (VM) from on-premises to Microsoft Azure, you must prepare the virtual hard disk (VHD or VHDX). Azure supports only generation 1 VMs that are in the VHD file format and have a fixed sized disk. The maximum size allowed for the VHD is 1,023 GB. You can convert a generation 1 VM from the VHDX file system to VHD and from a dynamically expanding disk to fixed-sized.
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-

image?toc=azure virtual-machines windows toc.json

Question: 62

You have an Azure subscription that contains 10 virtual machines on a virtual network.
You need to create a graph visualization to display the traffic flow between the virtual machines.
What should you do from Azure Monitor?

A. From Activity log, use quick insights.
B. From Metrics, create a chart.
C. From Logs, create a new query.
D. From Workbooks, create a workbook.

Answer: C

Explanation:
Navigate to Azure Monitor and select Logs to begin querying the data
Reference:
https://azure.microsoft.com/en-us/blog/analysis-of-network-connection-data-with-azure-monitor-for-virtual-machines/

Question: 63

HOTSPOT
You plan to create an Azure Storage account in the Azure region of East US 2.
You need to create a storage account that meets the following requirements:
• Replicates synchronously
• Remains available if a single data center in the region fails
How should you configure the storage account? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Replication:
- Geo-redundant storage (GRS)
- Locally-redundant storage (LRS)
- Read-access geo-redundant storage (RA GRS)
- Zone-redundant storage (ZRS)

Account kind:
- Blob storage
- Storage (general purpose v1)
- StorageV2 (general purpose v2)

Answer:

Replication:
- Geo-redundant storage (GRS)
- Locally-redundant storage (LRS)
- Read-access geo-redundant storage (RA GRS)
- Zone-redundant storage (ZRS) ✓

Account kind:
- Blob storage
- Storage (general purpose v1)
- StorageV2 (general purpose v2) ✓

Explanation:
Box 1: Zone-redundant storage (ZRS)
Zone-redundant storage (ZRS) replicates your data synchronously across three storage clusters in a single region.
LRS would not remain available if a data center in the region fails
GRS and RA GRS use asynchronous replication.
Box 2: StorageV2 (general purpose V2)
ZRS only support GPv2.
References:
https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy
https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-zrs

Question: 64

HOTSPOT

You play to deploy an Azure virtual machine named VM1 by using an Azure Resource Manager template.

You need to complete the template.

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

NOTE: Each correct selection is worth one point.

```
{
    "type": "Microsoft.Compute/virtualMachines",
    "apiVersion": "2018-10-01",
    "name": "VM1",
    "location": "[parameters('location')]",
    "dependsOn": [
        "[resourceId('Microsoft.Storage/storageAccounts/', variables ('Name3'))]",
        "[resourceId(                                      variables('Name4'))]"
],
```

- 'Microsoft.Network/publicIPAddresses/'
- 'Microsoft.Network/virtualNetworks/'
- 'Microsoft.Network/networkInterfaces/'
- 'Microsoft.Network/virtualNetworks/subnets'
- 'Microsoft.Storage/storageAccounts/'

```
{
    "type": "Microsoft.Network/networkInterfaces",
    "apiVersion": "2018-11-01",
    "name": "NIC1",
    "location": "[parameters('location')]",
    "dependsOn": [
        "[resourceId('Microsoft.Network/publicIPAddresses/', variables ('Name1'))]",
        "[resourceId(                                        variables('Name2'))]"
],
```

- 'Microsoft.Network/publicIPAddresses/'
- 'Microsoft.Network/virtualNetworks/'
- 'Microsoft.Network/networkInterfaces/'
- 'Microsoft.Network/virtualNetworks/subnets'
- 'Microsoft.Storage/storageAccounts/'

Answer:

```
{
    "type": "Microsoft.Compute/virtualMachines",
    "apiVersion": "2018-10-01",
    "name": "VM1",
    "location": "[parameters('location')]",
    "dependsOn": [
        "[resourceId('Microsoft.Storage/storageAccounts/', variables ('Name3'))]",
        "[resourceId(                                      variables('Name4'))]"
],
```

- 'Microsoft.Network/publicIPAddresses/'
- 'Microsoft.Network/virtualNetworks/'
- 'Microsoft.Network/networkInterfaces/' (selected)
- 'Microsoft.Network/virtualNetworks/subnets'
- 'Microsoft.Storage/storageAccounts/'

```
{
    "type": "Microsoft.Network/networkInterfaces",
    "apiVersion": "2018-11-01",
    "name": "NIC1",
    "location": "[parameters('location')]",
    "dependsOn": [
        "[resourceId('Microsoft.Network/publicIPAddresses/', variables ('Name1'))]",
        "[resourceId(                                        variables('Name2'))]"
],
```

- 'Microsoft.Network/publicIPAddresses/'
- 'Microsoft.Network/virtualNetworks/' (selected)
- 'Microsoft.Network/networkInterfaces/'
- 'Microsoft.Network/virtualNetworks/subnets'
- 'Microsoft.Storage/storageAccounts/'

Explanation:

Within your template, the dependsOn element enables you to define one resource as a dependent on one or more resources. Its value can be a comma-separated list of resource names.

Box 1: 'Microsoft.Network/networkInterfaces'

This resource is a virtual machine. It depends on two other resources:

Microsoft.Storage/storageAccounts

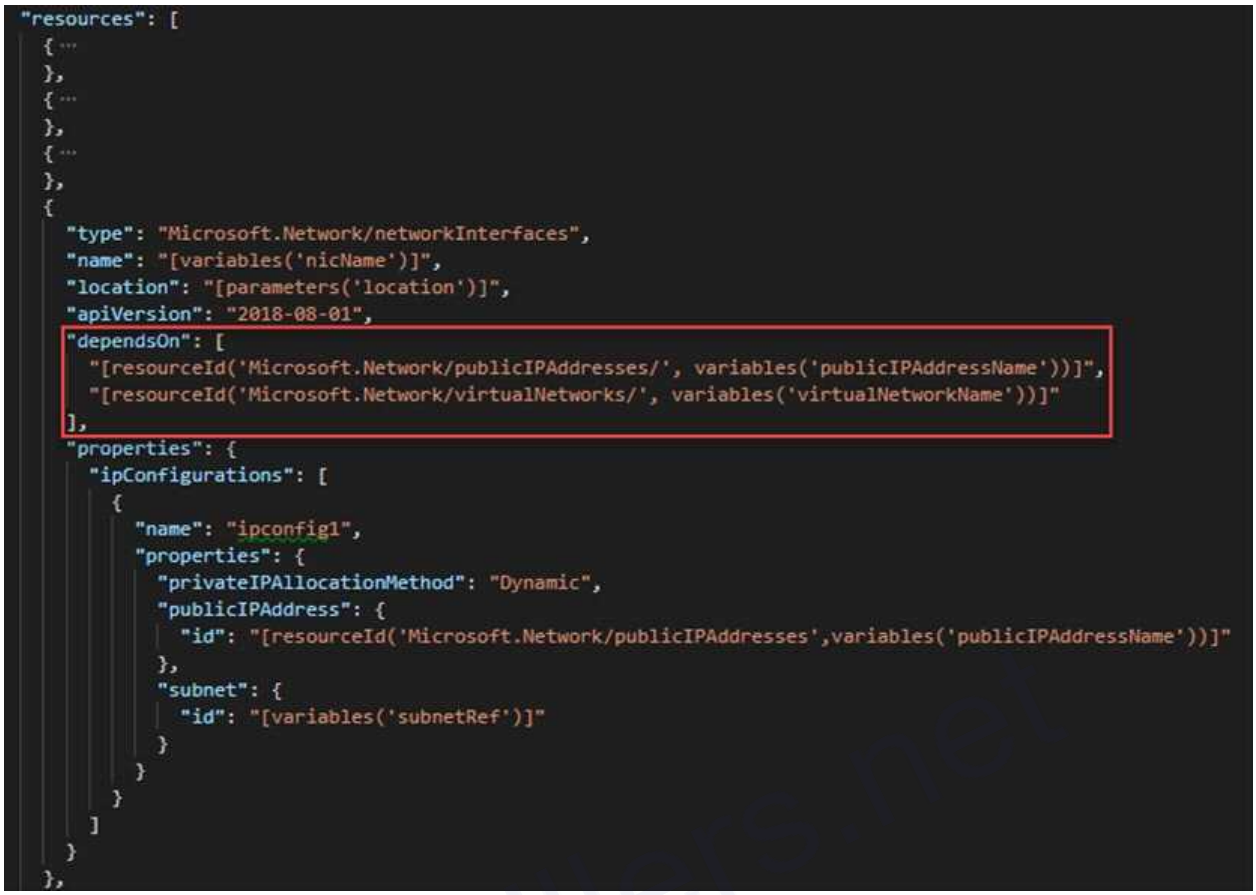
Microsoft.Network/networkInterfaces

Box 2: 'Microsoft.Network/virtualNetworks/'

The dependsOn element enables you to define one resource as a dependent on one or more resources. The resource depends on two other resources:

Microsoft.Network/publicIPAddresses

Microsoft.Network/virtualNetworks



References:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-tutorial-create-templates-with-dependent-resources

Question: 65

HOTSPOT

You network contains an Active Directory domain named adatum.com and an Azure Active Directory (Azure AD) tenant named adatum.onmicrosoft.com.

Adatum.com contains the user accounts in the following table.

Name	Member of
User1	Domain Admins
User2	Schema Admins
User3	Incoming Forest Trust Builders
User4	Replicator
User5	Enterprise Admins

Adatum.onmicrosoft.com contains the user accounts in the following table.

Name	Role
UserA	Global administrator
UserB	User administrator
UserC	Security administrator
UserD	Service administrator

You need to implement Azure AD Connect. The solution must follow the principle of least privilege. Which user accounts should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Adatum.com:

- User1
- User2
- User3
- User4
- User5

Adatum.onmicrosoft.com:

- UserA
- UserB
- UserC
- UserD

Answer:

Adatum.com:

- User1
- User2
- User3
- User4
- User5 (selected)

Adatum.onmicrosoft.com:

- UserA (selected)
- UserB
- UserC
- UserD

Explanation:
Box 1: User5
In Express settings, the installation wizard asks for the following:
AD DS Enterprise Administrator credentials
Azure AD Global Administrator credentials
The AD DS Enterprise Admin account is used to configure your on-premises Active Directory. These credentials are only used during the installation and are not used after the installation has completed. The Enterprise Admin, not the Domain Admin should make sure the permissions in Active Directory can be set in all domains.
Box 2: UserA
Azure AD Global Admin credentials are only used during the installation and are not used after the installation has completed. It is used to create the Azure AD Connector account used for synchronizing changes to Azure AD. The account also enables sync as a feature in Azure AD.
References:
https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions

Question: 66

You have an Azure subscription that contains 100 virtual machines.
You have a set of Pester tests in PowerShell that validate the virtual machine environment.
You need to run the tests whenever there is an operating system update on the virtual machines. The solution must minimize implementation time and recurring costs.
D18912E1457D5D1DDCBD40AB3BF70D5D
Which three resources should you use to implement the tests? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Azure Automation runbook
B. an alert rule
C. an Azure Monitor query
D. a virtual machine that has network access to the 100 virtual machines
E. an alert action group

Answer: ABE

Reference:
https://docs.microsoft.com/en-us/azure/automation/automation-create-alert-triggered-runbook
https://techsnips.io/snips/how-to-create-and-test-azure-monitor-alerts/?page=13

Question: 67

HOTSPOT
You have an Azure subscription that contains the resource groups shown in the following table.

Name	Location
RG1	West US
RG2	East US

You create an Azure Resource Manager template named Template1 as shown in the following exhibit.

```
{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "name": {
            "type": "String"
        },
        "location": {
           "defaultValue": "westus",
            "type": "String"
        }
    },
    "variables": {
             "location": "[resourceGroup().location]"
       },
    "resources": [
        {
            "type": "Microsoft.Network/publicIPAddresses",
            "apiVersion": "2019-11-01",
            "name": "[parameters('name')]",
            "location": "[variables('location')]",
            "sku": {
                "name": "Basic"
            },
            "properties": {
                "publicIPAddressVersion": "IPv4",
                "publicIPAllocationMethod": "Dynamic",
                "idleTimeoutInMinutes": 4,
                "ipTags": []
             }
         }
    ]
}
```

From the Azure portal, you deploy Template1 four times by using the settings shown in the following table.

Resource group	Name	Location
RG1	IP1	westus
RG1	IP2	westus
RG2	IP1	westus
RG2	IP3	westus

What is the result of the deployment? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Number of public IP addresses in West US: [▼]
- 1
- 2
- 3
- 4

Total number of public IP addresses created: [▼]
- 1
- 2
- 3
- 4

Answer:

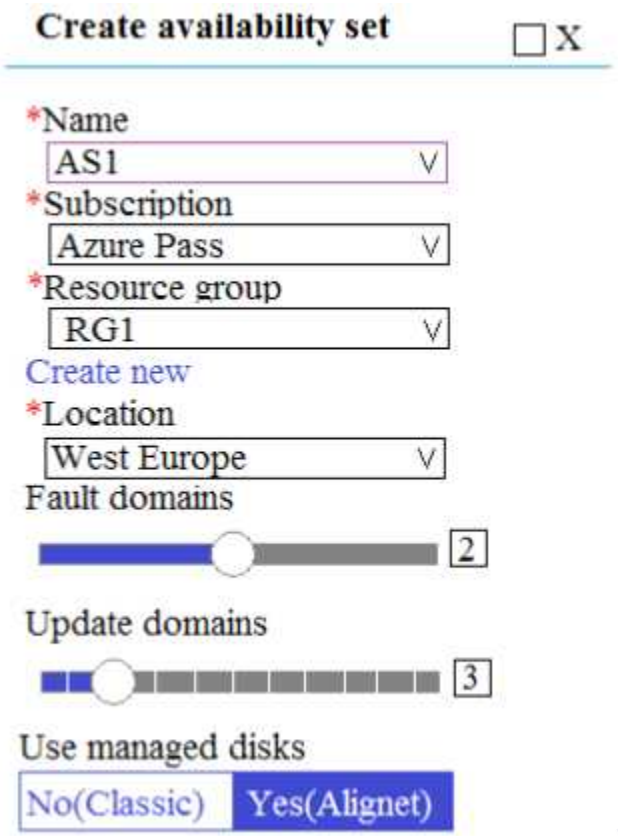
Number of public IP addresses in West US: [▼]
- 1
- 2
- 3
- 4

Total number of public IP addresses created: [▼]
- 1
- 2
- 3
- 4

Question: 68

HOTSPOT

You have an Azure subscription that contains multiple resource groups. You create an availability set as shown in the following exhibit.



You deploy 10 virtual machines to AS1.
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

During planned maintenance, at least **[answer choice]** 4 / 5 / 6 / 8 virtual machines will be available.

To add another virtual machines to AS1, the virtual machines must'be added to **[answer choice].** any region and the RG1 resource group / the West Europe region and any resource group / the West Europe region and the RG1 resource group

Answer:

During planned maintenance, at least **[answer choice]** 4 / 5 / **6** / 8 virtual machines will be available.

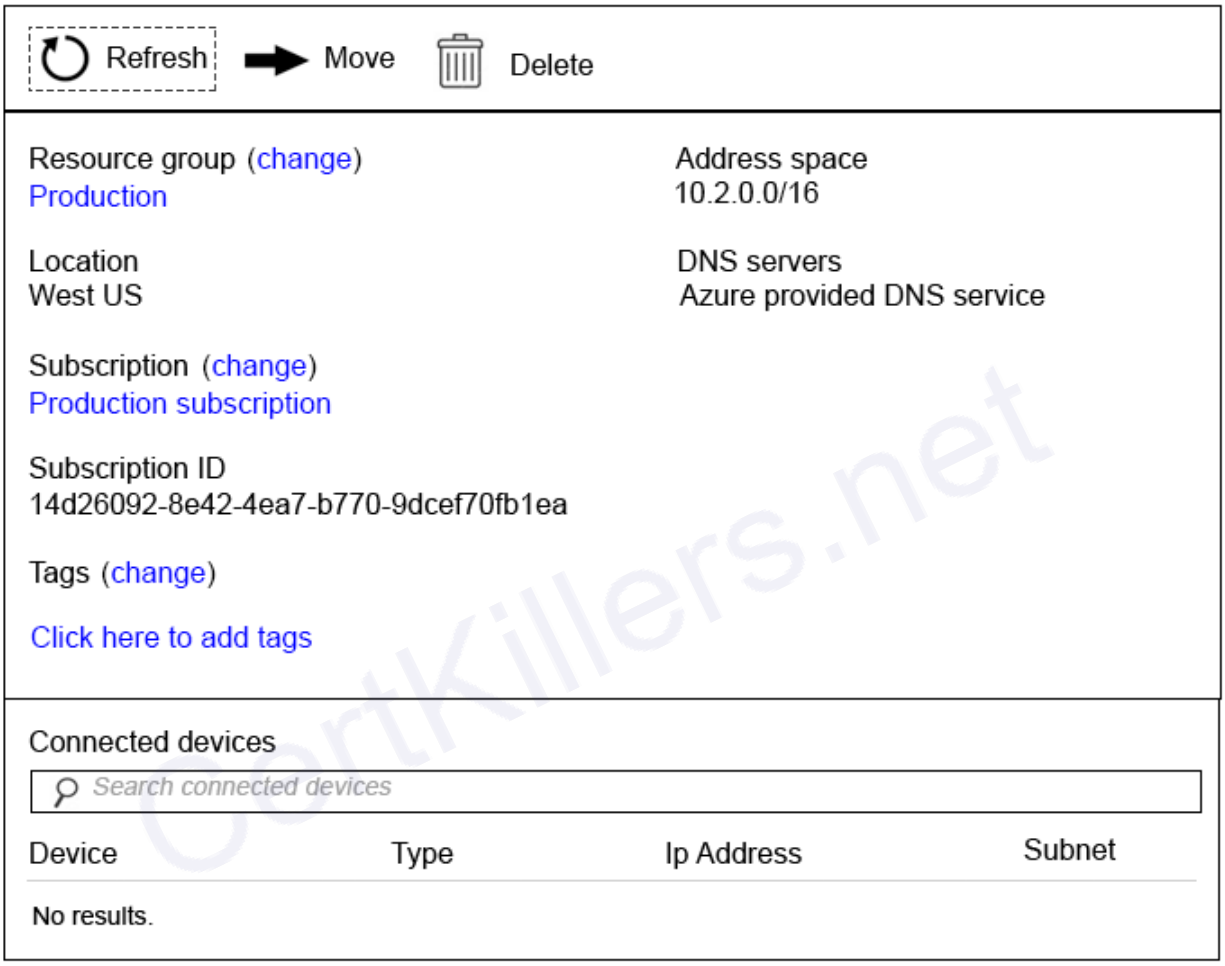
To add another virtual machines to AS1, the virtual machines must'be added to **[answer choice].** any region and the RG1 resource group / the West Europe region and any resource group / **the West Europe region and the RG1 resource group**

Explanation:
Box 1: 6
Two out of three update domains would be available, each with at least 3 VMs.
An update domain is a group of VMs and underlying physical hardware that can be rebooted at the same time.
As you create VMs within an availability set, the Azure platform automatically distributes your VMs across these update domains. This approach ensures that at least one instance of your application

always remains running as the Azure platform undergoes periodic maintenance.
Box 2: the West Europe region and the RG1 resource group
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/regions-and-availability

Question: 69

You have a virtual network named VNet1 as shown in the exhibit.



No devices are connected to VNet1.
You plan to peer VNet1 to another virtual network named Vnet2 in the same region. VNet2 has an address space of 10.2.0.0/16.
You need to create the peering.
What should you do first?

A. Modify the address space of VNet1.
B. Configure a service endpoint on VNet2
C. Add a gateway subnet to VNet1.
D. Create a subnet on VNet1 and VNet2.

Answer: A

Explanation:
The virtual networks you peer must have non-overlapping IP address spaces.
References:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints

Question: 70

HOTSPOT
You have an Azure Resource Manager template for a virtual machine named Template1. Template1 has the following parameters section.

```
"parameters": {
    "adminUsername": {
        "type": "string"
    },
    "adminPassword": {
        "type": "securestring"
    },
    "dnsLabelPrefix": {
        "type": "string"
    },
    "windowsOSVersion": {
        "type": "string"
        "defaultValue": "2016-Datacenter",
        "allowedValues": [
            "2016-Datacenter",
            "2019-Datacenter"
        ]
    },
    "location": {
        "type": "String",
        "allowedValues": [
            "eastus",
            "centralus",
            "westus" ]
    }
},
```

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 you deploy Template1, you are prompted for a resource group.	○	○
When you deploy Template1, you are prompted for the Windows operating system version.	○	○
When you deploy Template1, you are prompted for a location.	○	○

Answer:

Statements	Yes	No
When you deploy Template1, you are prompted for a resource group.	○	○
When you deploy Template1, you are prompted for the Windows operating system version.	○	○
When you deploy Template1, you are prompted for a location.	○	○

Explanation:
Box 1: Yes
The Resource group is not specified.
Box 2: No
The default value for the operating system is Windows 2016 Datacenter.
Box 3: Yes
Location is no default value.
References:
https://docs.microsoft.com/bs-latn-ba/azure/virtual-machines/windows/ps-template

Question: 71

You have an Azure subscription.
You have 100 Azure virtual machines.
You need to quickly identify underutilized virtual machines that can have their changed to a less expensive offering.
Which Wade should you use?

A. Metrics
B. Monitor
C. Customer insights
D. Advisor

Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations

Question: 72

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

Name	Member of
User1	Group1
User2	Group2

The tenant contains computers that run Windows 10. The computers are configured as shown in the following table.

Name	Member of
Computer1	GroupA
Computer2	GroupA
Computer3	GroupB

You enable Enterprise State Roaming in contoso.com for Group1 and GroupA.
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
If User1 modifies the desktop background of Computer1, User1 will see the changed background when signing in to Computer3.	○	○
If User2 modifies the desktop background of Computer1, User2 will see the changed background when signing in to Computer2.	○	○
If User1 modifies the desktop background of Computer3, User1 will see the changed background when signing in to Computer2.	○	○

Answer:

Statements	Yes	No
If User1 modifies the desktop background of Computer1, User1 will see the changed background when signing in to Computer3.	○	○
If User2 modifies the desktop background of Computer1, User2 will see the changed background when signing in to Computer2.	○	○
If User1 modifies the desktop background of Computer3, User1 will see the changed background when signing in to Computer2.	○	○

Explanation:
Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.
Box 1: Yes
Box 2: No
Box 3: Yes
References:
https://docs.microsoft.com/en-us/azure//////active-directory/devices/enterprise-state-roaming-overview

Question: 73

HOTSPOT
You have an Azure Resource Manager template named Template1 in the library as shown in the following exhibit.

ARM Template

template1

```
{
    "$schema": "https:/schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {},
    "resources": [
      {
        "apiVersion": "2016-01-01",
        "type": "Microsoft.Storage/storageAccounts",
        "name": "[concat(copyIndex(),'storage',uniqueString(resourceGroup().id))]",
        "location": "[resourceGroup().location]",
        "sku": {
          "name": "Premium_LRS"
        },
        "kind": "Storage",
        "properties": {},
        "copy": {
          "name": "storagecopy",
          "count": 3,
          "mode": "Serial",
          "batchSize": 1
        }
      }

    ]
}
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

During the deployment of Template1, you can specify **[answer choice]**.

- the number of resources to deploy
- the name of the resources to deploy
- the resource group to which to deploy the resources
- the permissions for the resources that will be deployed

Template1 deploys **[answer choice]**.

- a single storage account in one resource group
- three storage accounts in one resource group
- three resource groups that each has one storage account
- three resource groups that each has three storage accounts

Answer:

During the deployment of Template1, you can specify **[answer choice]**.

- the number of resources to deploy
- the name of the resources to deploy
- the resource group to which to deploy the resources
- the permissions for the resources that will be deployed

Template1 deploys **[answer choice]**.

- a single storage account in one resource group
- three storage accounts in one resource group
- three resource groups that each has one storage account
- three resource groups that each has three storage accounts

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-syntax

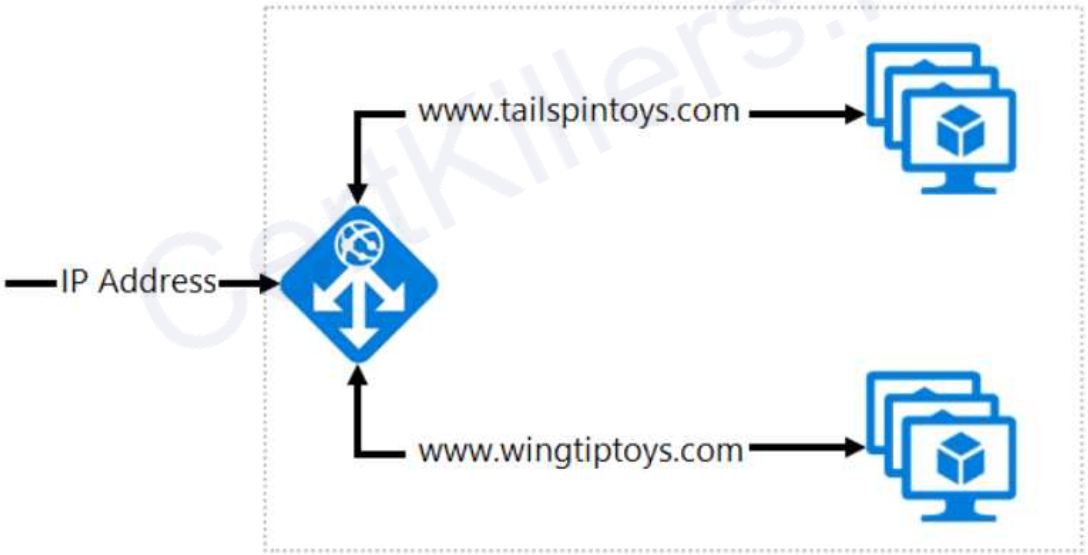
Question: 74

HOTSPOT

Your company hosts multiple websites by using Azure virtual machine scale sets (VMSS) that run Internet Information Server (IIS).

All network communications must be secured by using end to end Secure Socket Layer (SSL) encryption. User sessions must be routed to the same server by using cookie-based session affinity.

The image shown depicts the network traffic flow for the websites to the VMSS.



Use the drop-down menus to select the answer choice that answers each question.

NOTE: Each correct selection is worth one point.

Which Azure solution should you create to route the web application traffic to the VMSS?

- Azure VPN Gateway
- Azure Application Gateway
- Azure ExpressRoute
- Azure Network Watcher

What should you configure to make sure web traffic arrives at the appropriate server in the VMSS?

- Routing rules and backend listeners
- CNAME and A records
- Routing method and DNS time to live (TTL)
- Path-based redirection and WebSockets

Answer:

Which Azure solution should you create to route the web application traffic to the VMSS?

- Azure VPN Gateway
- **Azure Application Gateway**
- Azure ExpressRoute
- Azure Network Watcher

What should you configure to make sure web traffic arrives at the appropriate server in the VMSS?

- Routing rules and backend listeners
- CNAME and A records
- Routing method and DNS time to live (TTL)
- **Path-based redirection and WebSockets**

Explanation:
Box 1: Azure Application Gateway
You can create an application gateway with URL path-based redirection using Azure PowerShell.
Box 2: Path-based redirection and Websockets
Reference:
https://docs.microsoft.com/bs-latn-ba/azure//application-gateway/tutorial-url-redirect-powershell

Question: 75

DRAG DROP
You have an Azure subscription that contains two virtual networks named VNet1 and VNet2. Virtual machines connect to the virtual networks.
The virtual networks have the address spaces and the subnets configured as shown in the following table.

Virtual network	Address space	Subnet	Peering
VNet1	10.1.0.0/16	10.1.0.0/24 10.1.1.0/26	VNet2
VNet2	10.2.0.0/16	10.2.0.0/24	VNet1

You need to add the address space of 10.33.0.0/16 to VNet1. The solution must ensure that the hosts on VNet1 and VNet2 can communicate.
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	Answer Area
Remove peering between VNet1 and VNet2.	
Recreate peering between VNet1 and VNet2.	
On the peering connection in VNet1, allow gateway transit.	
Add the 10.33.0.0/16 address space to VNet1.	
On the peering conenction in VNet2, allow gateway transit.	
Create a new virtual network named VNet1.	
Remove VNet1.	

Answer:

Remove peering between VNet1 and VNet2.

Add the 10.33.0.0/16 address space to VNet1.

Recreate peering between VNet1 and VNet2.

Explanation:
Step 1: Remove peering between Vnet1 and VNet2.
You can't add address ranges to, or delete address ranges from a virtual network's address space once a virtual network is peered with another virtual network. To add or remove address ranges, delete the peering, add or remove the address ranges, then re-create the peering.
Step 2: Add the 10.44.0.0/16 address space to VNet1.
Step 3: Recreate peering between VNet1 and VNet2
References:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering

Question: 76

You have an Azure App Service app.
You need to implement tracing for the app. The tracing information must include the following:

• Usage trends
• AJAX call responses
• Page load speed by browser
• Server and browser exceptions
What should you do?

A. Configure IIS logging in Azure Log Analytics.
B. Configure a connection monitor in Azure Network Watcher.
C. Configure custom logs in Azure Log Analytics.
D. Enable the Azure Application Insights site extension.

Answer: D

Explanation:
For web pages, Application Insights JavaScript SDK automatically collects AJAX calls as dependencies.
Note: Some of the things you can track or collect are:
What are the most popular webpages in your application, at what time of day and where is that traffic coming from?
Dependency rates or response times and failure rates to find out if there's an external service that's causing performance issues on your app, maybe a user is using a portal to get through to your application and there are response time issues going through there for instance.
Exceptions for both server and browser information, as well as page views and load performance from the end users' side.
Reference:
https://azure.microsoft.com/en-us/blog/ajax-collection-in-application-insights/
https://blog.pragmaticworks.com/what-is-application-insights

Question: 77

HOTSPOT
You have an Azure subscription named Subscription1. Subscription1 contains the resources in the following table:

Name	Type
RG1	Resource group
RG2	Resource group
VNet1	Virtual network
VNet2	Virtual network

VNet1 is in RG1. VNet2 is in RG2. There is no connectivity between VNet1 and VNet2. An administrator named Admin1 creates an Azure virtual machine VM1 in RG1. VM1 uses a disk named Disk1 and connects to VNet1. Admin1 then installs a custom application in VM1.
You need to move the custom application to VNet2. The solution must minimize administrative effort.
Which two actions should you perform? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

First action:

- Create a network interface in RG2.
- Detach a network interface.
- Delete VM1.
- Move a network interface to RG2.

Second action:

- Attach a network interface.
- Create a network interface in RG2.
- Create a new virtual machine.
- Move VM1 to RG2.

Answer:

First action: Create a network interface in RG2. / Detach a network interface. / **Delete VM1.** / Move a network interface to RG2.

Second action: Attach a network interface. / Create a network interface in RG2. / **Create a new virtual machine.** / Move VM1 to RG2.

Explanation:
We cannot just move a virtual machine between networks. What we need to do is identify the disk used by the VM, delete the VM itself while retaining the disk, and recreate the VM in the target virtual network and then attach the original disk to it.
Reference:
https://blogs.technet.microsoft.com/canitpro/2014/06/16/step-by-step-move-a-vm-to-a-different-

vnet-on-azure/
https://4sysops.com/archives/move-an-azure-vm-to-another-virtual-network-vnet/#migrate-an-azure-vm-between-vnets

Question: 78

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

Name	Contains
Storagecontoso1	A blob service and a table service
Storagecontoso2	A blob service and a file service
Storagecontoso3	A queue service
Storagecontoso4	A file service and a queue service
Storagecontoso5	A table service

You enable Azure Advanced Threat Protection (ATP) for all the storage accounts.
You need to identify which storage accounts will generate Azure ATP alerts.
Which two storage accounts should you identify? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

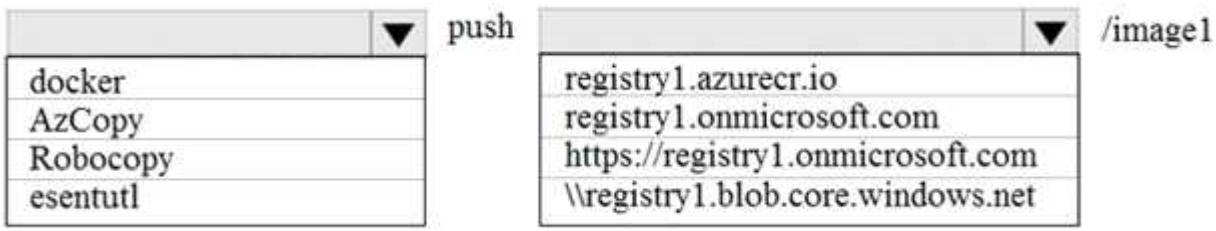
A. storagecontoso1
B. storagecontoso2
C. storagecontoso3
D. storagecontoso4
E. storaaecontoso5

Answer: AB

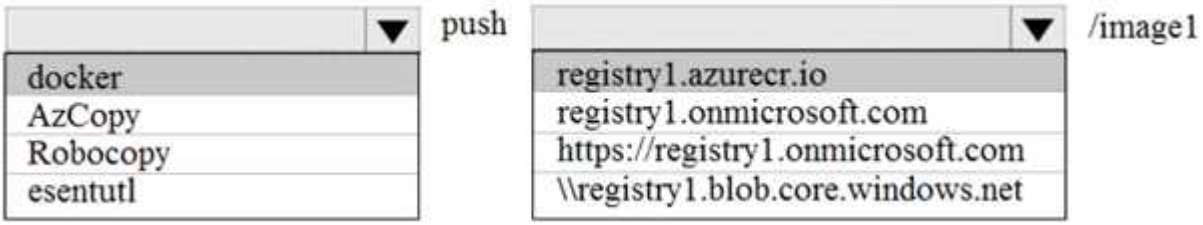
Explanation:
Advanced threat protection for Azure Storage is currently available only for Blob Storage.
https://docs.microsoft.com/en-us/azure/storage/common/storage-advanced-threat-protection?tabs=azure-portal

Question: 79

HOTSPOT
Your company has an Azure Container Registry named Registry1.
You have an Azure virtual machine named Server1 that runs Windows Server 2019.
From Server1, you create a container image named image1.
You need to add image1 to Registry1.
Which command should you run on Server1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
An Azure container registry stores and manages private Docker container images, similar to the way Docker Hub stores public Docker images. You can use the Docker command-line interface (Docker CLI) for login, push, pull, and other operations on your container registry.
Reference:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-get-started-docker-cli
https://docs.docker.com/engine/reference/commandline/push/

Question: 80

HOTSPOT

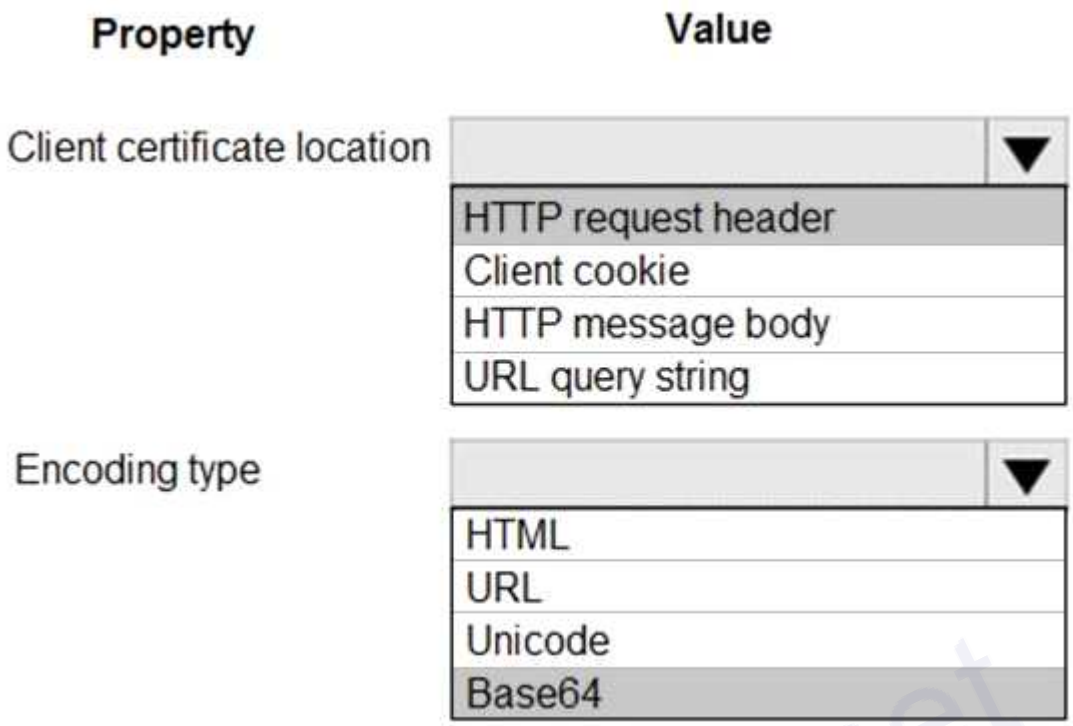
You are developing an Azure Web App. You configure TLS mutual authentication for the web app.

You need to validate the client certificate in the web app. To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Property	Value
Client certificate location	HTTP request header Client cookie HTTP message body URL query string
Encoding type	HTML URL Unicode Base64

Answer:



Question: 81

DRAG DROP

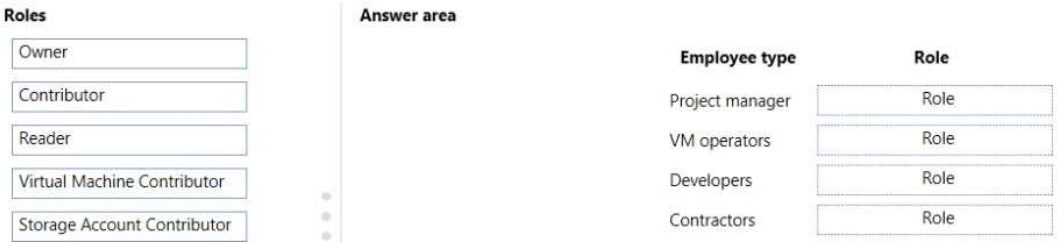
You are designing a solution to secure a company's Azure resources. The environment hosts 10 teams. Each team manages a project and has a project manager, a virtual machine (VM) operator, developers, and contractors.

Project managers must be able to manage everything except access and authentication for users. VM operators must be able to manage VMs, but not the virtual network or storage account to which they are connected. Developers and contractors must be able to manage storage accounts.

You need to recommend roles for each member.

What should you recommend? To answer, drag the appropriate roles to the correct employee types. Each role 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.



Answer:

Employee type	Role
Project manager	Contributor
VM operators	Virtual Machine Contributor
Developers	Storage Account Contributor
Contractors	Storage Account Contributor

Question: 82

You have an Azure virtual machine named VM1 and an Azure Active Directory (Azure AD) tenant named adatum.com.
D18912E1457D5D1DDCBD40AB3BF70D5D
VM1 has the following settings:
• IP address: 10.10.0.10
• System-assigned managed identity: On
You need to create a script that will run from within VM1 to retrieve the authentication token of VM1.
Which address should you use in the script?

A. vm1.adatum.com.onmicrosoft.com
B. 169.254.169.254
C. 10.10.0.10
D. vm1.adatum.com

Answer: B

Explanation:
Your code that's running on the VM can request a token from the Azure Instance Metadata Service identity endpoint, accessible only from within the VM: http://169.254.169.254/metadata/identity/oauth2/token
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

Question: 83

HOTSPOT
Your company has a virtualization environment that contains the virtualization hosts shown in the

following table.

Name	Hypervisor	Guest
Server1	VMware	VM1, VM2, VM3
Server2	Hyper-V	VMA, VMB, VMC

The virtual machines are configured as shown in the following table.

Name	Generation	Memory	Operating system (OS)	OS disk	Data disk
VM1	*Not applicable*	4 GB	Windows Server 2016	200 GB	800 GB
VM2	*Not applicable*	12 GB	Red Hat Enterprise Linux 7.2	3 TB	200 GB
VM3	*Not applicable*	32 GB	Windows Server 2012 R2	200 GB	1 TB
VMA	1	8 GB	Windows Server 2012	100 GB	2 TB
VMB	1	16 GB	Red Hat Enterprise Linux 7.2	150 GB	3 TB
VMC	2	24 GB	Windows Server 2016	200 GB	6 TB

All the virtual machines use basic disks. VM1 is protected by using BitLocker Drive Encryption (BitLocker).
You plan to migrate the virtual machines to Azure by using Azure Site Recovery.
You need to identify which virtual machines can be migrated.
Which virtual machines should you identify for each server? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

The virtual machines that can be migrated from Server1.

- VM1 only
- VM2 only
- VM3 only
- VM1 and VM2 only
- VM1 and VM3 only
- VM1, VM2, and VM3

The virtual machines that can be migrated from Server2.

- VMA only
- VMB only
- VMC only
- VMA and VMB only
- VMA and VMC only
- VMA, VMB, and VMC

Answer:

The virtual machines that can be migrated from Server1.	
	VM1 only
	VM2 only
	VM3 only
	VM1 and VM2 only
	VM1 and VM3 only
	VM1, VM2, and VM3

The virtual machines that can be migrated from Server2.	
	VMA only
	VMB only
	VMC only
	VMA and VMB only
	VMA and VMC only
	VMA, VMB, and VMC

Explanation:
Incorrect Answers:
VM1 cannot be migrates as it has BitLocker enabled.
VM2 cannot be migrates as the OS disk on VM2 is larger than 2TB.
VMC cannot be migrates as the Data disk on VMC is larger than 4TB.
References:
https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-support-matrix#azure-vm-requirements

Question: 84

You are designing an Azure solution.
The solution must meet the following requirements:
* Distribute traffic to different pools of dedicated virtual machines (VMs) based on rules
* Provide SSL offloading capabilities
You need to recommend a solution to distribute network traffic.
Which technology should you recommend?

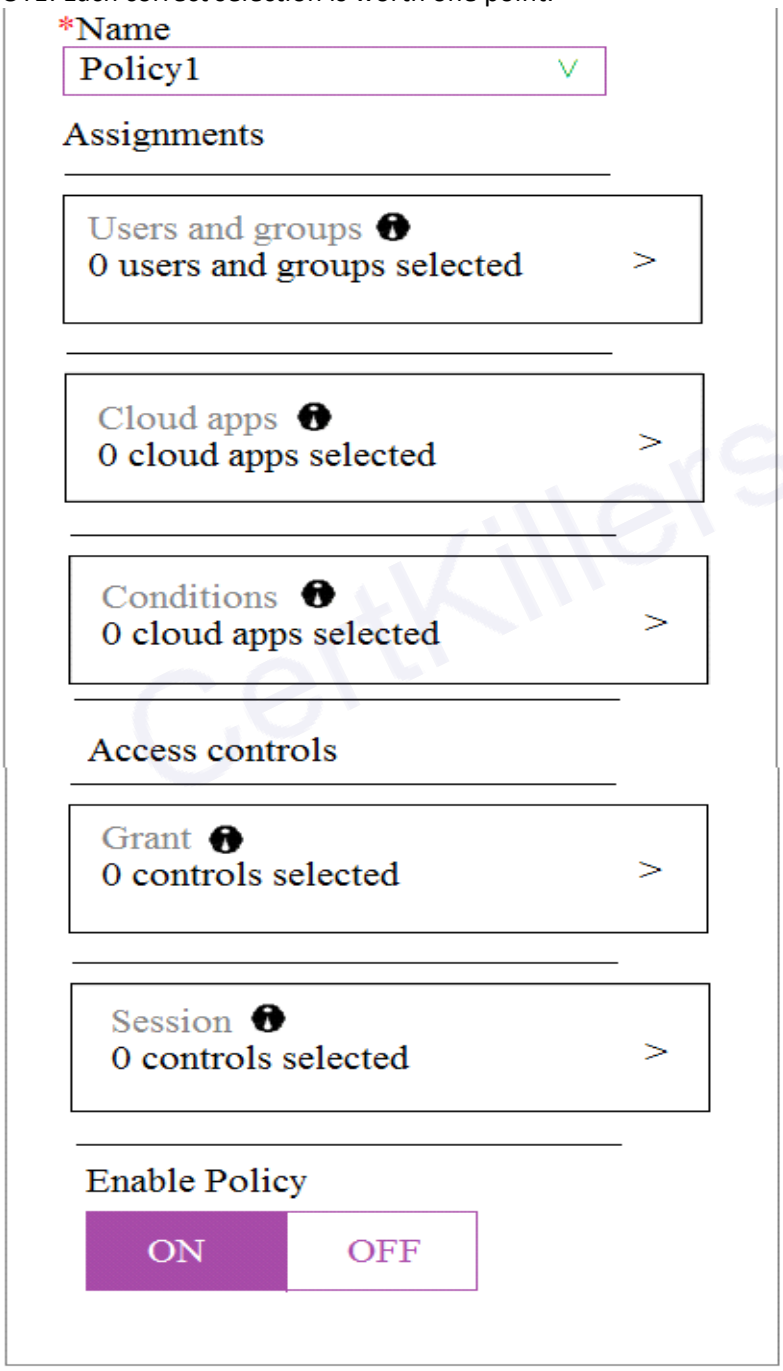
A. server-level firewall rules
B. Azure Application Gateway
C. Azure Traffic Manager
D. Azure Load Balancer

Answer: B

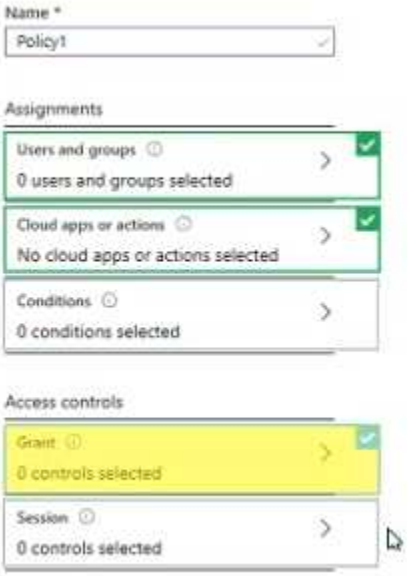
Explanation:
If you require "SSL offloading", application layer treatment, or wish to delegate certificate management to
Azure, you should use Azure's layer 7 load balancer Application Gateway instead of the Load Balanacer.
References:
https://docs.microsoft.com/en-us/azure/application-gateway/overview

Question: 85

HOTSPOT
You have an Azure Active Directory (Azure AD) tenant.
You need to create a conditional access policy that requires all users to use multi-factor authentication when they access the Azure portal.
Which three settings should you configure? To answer, select the appropriate settings to the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies

Question: 86

You are implementing authentication for applications in your company. You plan to implement self-service password reset (SSPR) and multifactor authentication (MFA) in Azure Active Directory (Azure AD).
You need to select authentication mechanisms that can be used for both MFA and SSPR.
Which two authentication methods should you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Short Message Service (SMS) messages
B. Authentication app
C. Email addresses
D. Security questions
E. App passwords

Answer: AB

Explanation:
References:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

Question: 87

Your company has the groups shown in the following table.

Group	Number of members
Managers	10
Sales	100
Development	15

The company has an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com.
An administrator named Admin1 attempts to enable Enterprise State Roaming for all the users in the Managers group.
Admin1 reports that the options for Enterprise State Roaming are unavailable from Azure AD.
You verify that Admin1 is assigned the Global administrator role.
You need to ensure that Admin1 can enable Enterprise State Roaming.
What should you do?

A. Enforce Azure Multi-Factor Authentication (MFA) for Admin1.
B. Purchase an Azure AD Premium P1 license for each user in the Managers group.
C. Assign an Azure AD Privileged Identity Management (PIM) role to Admin1.
D. Purchase an Azure Rights Management (Azure RMS) license for each user in the Managers group.

Answer: B

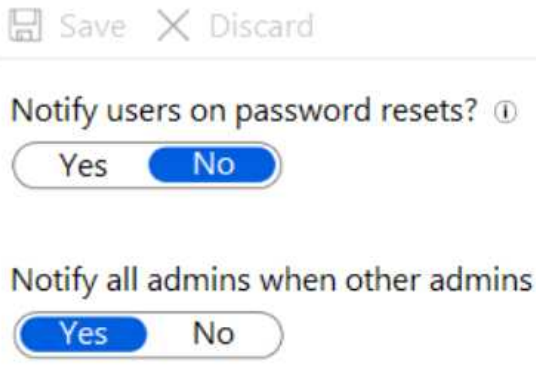
Explanation:
Enterprise State Roaming is available to any organization with an Azure AD Premium or Enterprise Mobility + Security (EMS) license.
References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/devices/enterprise-state-roaming-enable

Question: 88

HOTSPOT
You have an Azure Active Directory (Azure AD) tenant that contains the user groups shown in the following table.

Name	Role	Member of
User1	Global administrator	*None*
User2	User administrator	Group1
User3	Password administrator	Group1
User4	*None*	Group1

You enable self-service password reset (SSPR) for Group1.
You configure the Notifications settings 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.

Statements	Yes	No
User1 gets a notification when User3 resets her password by using SSPR.	○	○
User3 gets a notification when User3 resets her password by using SSPR.	○	○
User1 gets a notification when User2 resets the password of User4.	○	○

Answer:

Statements	Yes	No
User1 gets a notification when User3 resets her password by using SSPR.	○	○
User3 gets a notification when User3 resets her password by using SSPR.	○	○
User1 gets a notification when User2 resets the password of User4.	○	○

Explanation:
Box 1: Yes
Notify all admins when other admins reset their passwords: Yes.
Box 2: No
Notify users on password resets: No.
Box 3: No
• Notify users on password resets

If this option is set to Yes, then users resetting their password receive an email notifying them that their password has been changed. The email is sent via the SSPR portal to their primary and alternate email addresses that are on file in Azure AD. No one else is notified of the reset event.
• Notify all admins when other admins reset their passwords
If this option is set to Yes, then all administrators receive an email to their primary email address on file in Azure AD. The email notifies them that another administrator has changed their password by using SSPR.
Example: There are four administrators in an environment. Administrator A resets their password by using SSPR. Administrators B, C, and D receive an email alerting them of the password reset.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr

Question: 89

Your company has an Azure subscription.
You enable multi-factor authentication (MFA) for all users.
The company's help desk reports an increase in calls from users who receive MFA requests while they work from the company's main office.
You need to prevent the users from receiving MFA requests when they sign in from the main office.
What should you do?

A. From Azure Active Directory (Azure AD), configure organizational relationships.
B. From the MFA service settings, create a trusted IP range.
C. From Conditional access in Azure Active Directory (Azure AD), create a custom control.
D. From Conditional access in Azure Active Directory (Azure AD), create a named location.

Answer: B

Explanation:
The first thing you may want to do, before enabling Multi-Factor Authentication for any users, is to consider configuring some of the available settings. One of the most important features is a trusted IPs list. This will allow you to whitelist a range of IPs for your network. This way, when users are in the office, they will not get prompted with MFA, and when they take their devices elsewhere, they will. Here's how to do it:
Log in to your Azure Portal.
Navigate to Azure AD > Conditional Access > Named locations.
From the top toolbar select Configure MFA trusted IPs.
References:
https://www.kraftkennedy.com/implementing-azure-multi-factor-authentication/

Question: 90

You have an application named App1 that does not support Azure Active Directory (Azure AD) authentication.
You need to ensure that App1 can send messages to an Azure Service Bus queue. The solution must prevent Appl from listening to the queue.

What should you do?

A. Modify the locks of the Queue
B. Configure Access control (IAM) for the Service Bus
C. Configure Access control (IAM) for the queue.
D. Add a shared access policy to the queue

Answer: D

Explanation:
There are two ways to authenticate and authorize access to Azure Service Bus resources: Azure Activity Directory (Azure AD) and Shared Access Signatures (SAS).
Each Service Bus namespace and each Service Bus entity has a Shared Access Authorization policy made up of rules.
Reference:
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-authentication-and-authorization
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-sas

Question: 91

An administrator plans to create a function app in Azure that will have the following settings:
• Runtime stack: .NET Core
• Operating System: Linux
• Plan type: Consumption
• Enable Application Insights: Yes
You need to ensure that you can back up the function app.
Which settings should you recommend changing before creating the function app?
D18912E1457D5D1DDCBD40AB3BF70D5D

A. Runtime stack
B. Enable Application Insights
C. Operating System
D. Plan type

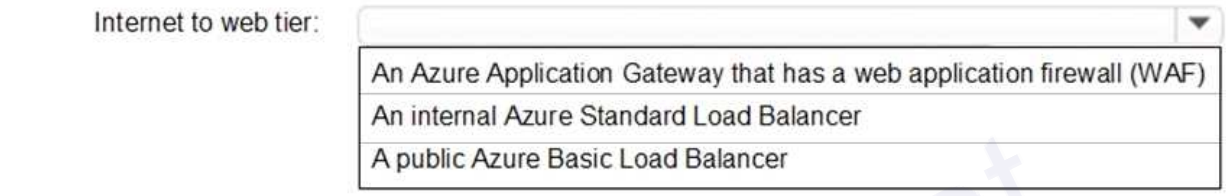
Answer: D

Explanation:
The Backup and Restore feature requires the App Service plan to be in the Standard, Premium or Isolated tier.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/manage-backup#requirements-and-restrictions

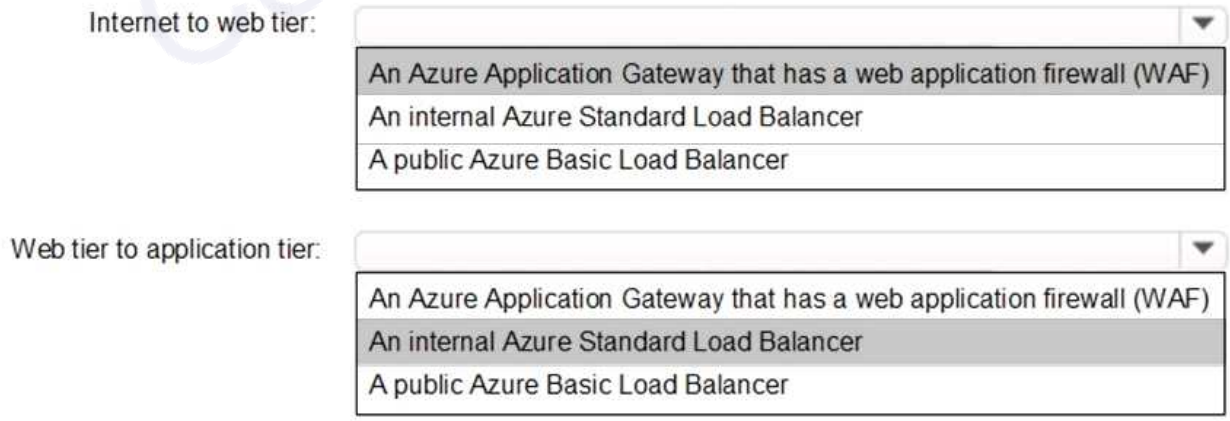
Question: 92

HOTSPOT
You have an Azure subscription.

You plan to deploy an app that has a web front end and an application tier.
You need to recommend a load balancing solution that meets the following requirements:
• Internet to web tier:
- Provides URL-based routing
- Supports connection draining
- Prevents SQL injection attacks
• Web tier to application tier:
- Provides port forwarding
- Supports HTTPS health probes
- Supports an availability set as a backend pool
Which load balancing solution should you recommend for each tier? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
Box 1: An Azure Application Gateway that has a web application firewall (WAF)
Azure Application Gateway offers a web application firewall (WAF) that provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

Application Gateway operates as an application delivery controller (ADC). It offers Secure Sockets Layer (SSL) termination, cookie-based session affinity, round-robin load distribution, content-based routing, ability to host multiple websites, and security enhancements.
Box 2: An internal Azure Standard Load Balancer
The internet to web tier is the public interface, while the web tier to application tier should be internal.
Note: When using load-balancing rules with Azure Load Balancer, you need to specify a health probes to allow Load Balancer to detect the backend endpoint status.
Health probes support the TCP, HTTP, HTTPS protocols.
References:
https://docs.microsoft.com/en-us/azure/application-gateway/waf-overview
https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview

Question: 93

You have 10 Azure virtual machines on a subnet named Subnet1. Subnet1 is on a virtual network named VNet1.
You plan to deploy a public Azure Standard Load Balancer named LB1 to the same Azure region as the 10 virtual machines.
You need to ensure that traffic from all the virtual machines to the internet flows through LB1. The solution must prevent the virtual machines from being accessible on the internet.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Add health probes to LB1.
B. Add the network interfaces of the virtual machines to the backend pool of LB1.
C. Add an inbound rule to LB1.
D. Add an outbound rule to LB1.
E. Associate a network security group (NSG) to Subnet1.
F. Associate a user-defined route to Subnet1.

Answer: ABD

Reference:
https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-standard-manage-portal2

Question: 94

You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.

Name	Connected to
VM1	VNET1/Subnet1
VM2	VNET1/Subnet2

KeyVault1 has an access policy that provides several users with Create Key permissions.

You need to ensure that the users can only register secrets in KeyVault1 from VM1.
What should you do?

A. Create a network security group (NSG) that is linked to Subnet1.
B. Configure the Firewall and virtual networks settings for KeyVault1.
C. Modify the access policy for KeyVault1.
D. Configure KeyVault1 to use a hardware security module (HSM).

Answer: C

Explanation:
You grant data plane access by setting Key Vault access policies for a key vault.
Note 1: Grant our VM's system-assigned managed identity access to the Key Vault.
• Select Access policies and click Add new.
• In Configure from template, select Secret Management.
• Choose Select Principal, and in the search field enter the name of the VM you created earlier. Select the VM in the result list and click Select.
• Click OK to finishing adding the new access policy, and OK to finish access policy selection.
Note 2: Access to a key vault is controlled through two interfaces: the management plane and the data plane. The management plane is where you manage Key Vault itself. Operations in this plane include creating and deleting key vaults, retrieving Key Vault properties, and updating access policies. The data plane is where you work with the data stored in a key vault. You can add, delete, and modify keys, secrets, and certificates.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad
https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault2

Question: 95

HOTSPOT
You have an Azure subscription named Subscription1 that contains a virtual network named VNet1.
You add the users in the following table.

User	Role
User1	Owner
User2	Security Admin
User3	Network Contributor

Which user can perform each configuration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Add a subnet to VNet1:	
	User1 only
	User2 only
	User3 only
	User1 and User2 only
	User1 and User3 only
	User2 and User3 only
	User1, User2, and User3

Assign a user the Reader role to VNet1:	
	User1 only
	User2 only
	User3 only
	User1 and User2 only
	User1 and User3 only
	User2 and User3 only
	User1, User2, and User3

Answer:

Box 1: User1 and User3 only.
Box 2: User1

Explanation:
Box 1: User1 and User3 only.
The Owner Role lets you manage everything, including access to resources.
The Network Contributor role lets you manage networks, but not access to them.
Box 2: User1
The Security Admin role: In Security Center only: Can view security policies, view security states, edit security policies, view alerts and recommendations, dismiss alerts and recommendations.
References:
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

Question: 96

You have resources in three Azure regions. Each region contains two virtual machines. Each virtual machine has a public IP address assigned to its network interface and a locally installed application named App1.
You plan to implement Azure Front Door-based load balancing across all the virtual machines.
You need to ensure that App1 on the virtual machines will only accept traffic routed from Azure Front Door.
What should you implement?

A. Azure Private Link
B. service endpoints
C. network security groups (NSGs) with service tags

D. network security groups (NSGs) with application security groups

Answer: C

Explanation:
Configure IP ACLing for your backends to accept traffic from Azure Front Door's backend IP address space and Azure's infrastructure services only. Refer the IP details below for ACLing your backend:
• Refer AzureFrontDoor.Backend section in Azure IP Ranges and Service Tags for Front Door's IPv4 backend IP address range or you can also use the service tag AzureFrontDoor.Backend in your network security groups.
Reference:
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq

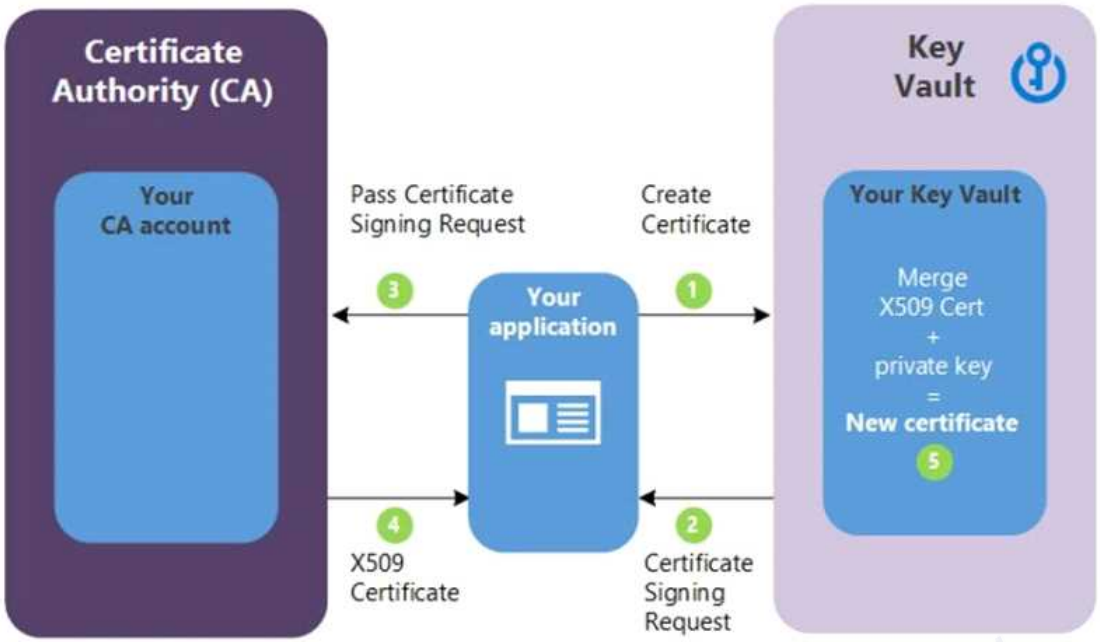
Question: 97

You have an Azure key vault named KV1.
You need to ensure that applications can use KV1 to provision certificates automatically from an external certification authority (CA).
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From KV1, create a certificate issuer resource.
B. Obtain the CA account credentials.
C. Obtain the root CA certificate.
D. From KV1, create a certificate signing request (CSR).
E. From KV1, create a private key,

Answer: CD

Explanation:
C: Obtain the root CA certificate (step 4 in the picture below)
D: From KV1, create a certificate signing request (CSR) (step 2 in the picture below)
Note:
Creating a certificate with a CA not partnered with Key Vault
This method allows working with other CAs than Key Vault's partnered providers, meaning your organization can work with a CA of its choice.



The following step descriptions correspond to the green lettered steps in the preceding diagram.

- In the diagram above, your application is creating a certificate, which internally begins by creating a key in your key vault.
- Key Vault returns to your application a Certificate Signing Request (CSR).
- Your application passes the CSR to your chosen CA.
- Your chosen CA responds with an X509 Certificate.
- Your application completes the new certificate creation with a merger of the X509 Certificate from your CA.

Reference:
https://docs.microsoft.com/en-us/azure/key-vault/certificates/certificate-scenarios

Question: 98

You create the following Azure role definition.

```
{
   "Name":  "Role1",
   "Id":  "80808080-8080-8080-8080-808080808080",
   "IsCustom":  false,
   "Description":  "",
   "Actions":  [
                  "Microsoft.Storage/*/read",
                  "Microsoft.Network/*/read",
                  "Microsoft.Compute/virtualMachines/start/action",
                  "Microsoft.Compute/virtualMachines/restart/action",
                  "Microsoft.Authorization/*/read"],
   "NotActions":  [  ],
   "DataActions":  [ ],
   "NotDataActions":  [   ],
   "AssignableScopes":  [  ]
}
```

You need to create Role1 by using the role definition.
Which two values should you modify before you create Role1? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. AssignableScopes
B. Description
C. DataActions
D. IsCustom
E. Id

Answer: AD

Explanation:
Part of example:
"IsCustom": true,
"AssignableScopes": [
"/subscriptions/{subscriptionId1}",
"/subscriptions/{subscriptionId2}",
"/subscriptions/{subscriptionId3}"
The following shows what a custom role looks like as displayed in JSON format. This custom role can be used for monitoring and restarting virtual machines.

```
{
 "Name": "Virtual Machine Operator",
 "Id": "88888888-8888-8888-8888-888888888888",
 "IsCustom": true,
 "Description": "Can monitor and restart virtual machines.",
 "Actions": [
  "Microsoft.Storage/*/read",
  "Microsoft.Network/*/read",
  "Microsoft.Compute/*/read",
  "Microsoft.Compute/virtualMachines/start/action",
  "Microsoft.Compute/virtualMachines/restart/action",
  "Microsoft.Authorization/*/read",
  "Microsoft.ResourceHealth/availabilityStatuses/read",
  "Microsoft.Resources/subscriptions/resourceGroups/read",
  "Microsoft.Insights/alertRules/*",
  "Microsoft.Insights/diagnosticSettings/*",
  "Microsoft.Support/*"
 ],
 "NotActions": [],
 "DataActions": [],
 "NotDataActions": [],
 "AssignableScopes": [
  "/subscriptions/{subscriptionId1}",
  "/subscriptions/{subscriptionId2}",
  "/subscriptions/{subscriptionId3}"
 ]
```

}
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

Question: 99

Note: This question is part of 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 a server named Server1 that runs Windows Server 2019. Server1 is a container host.
You are creating a Dockerfile to build a container image.
You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.
Solution: You add the following line to the Dockerfile.
Copy-Item File1.txt C:\Folder1\File1.txt
You then build the container image.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Copy-Item is not supported. Copy is the correct command to copy a file to the container image.
References:
https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy
https://docs.docker.com/engine/reference/builder/

Question: 100

Note: This question is part of 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 a server named Server1 that runs Windows Server 2019. Server1 is a container host.
You are creating a Dockerfile to build a container image.
You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.
Solution: You add the following line to the Dockerfile.
COPY File1.txt /Folder1/
You then build the container image.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Copy is the correct command to copy a file to the container image.
References:
https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy
https://docs.docker.com/engine/reference/builder/

Question: 101

Note: This question is part of 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 a server named Server1 that runs Windows Server 2019. Server1 is a container host.
You are creating a Dockerfile to build a container image.
You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.
Solution: You add the following line to the Dockerfile.
COPY File1.txt C:/Folder1/
You then build the container image.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Copy is the correct command to copy a file to the container image but the root directory is specified as '/' and not as 'C:/'.
References:
https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy
https://docs.docker.com/engine/reference/builder/

Question: 102

Note: This question is part of 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 a server named Server1 that runs Windows Server 2019. Server1 is a container host.

You are creating a Dockerfile to build a container image.
You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.
Solution: You add the following line to the Dockerfile.
ADD File1.txt C:/Folder1/
You then build the container image.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Copy is the correct command to copy a file to the container image. The ADD command can also be used. However, the root directory is specified as '/' and not as 'C:/'.
Reference:
https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy
https://docs.docker.com/engine/reference/builder/

Question: 103

Note: This question is part of 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 a server named Server1 that runs Windows Server 2019. Server1 is a container host.
You are creating a Dockerfile to build a container image.
You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.
Solution: You add the following line to the Dockerfile.
XCOPY File1.txt C:\Folder1\
You then build the container image.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Copy is the correct command to copy a file to the container image. Furthermore, the root directory is specified as '/' and not as 'C:/'.
References:
https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy
https://docs.docker.com/engine/reference/builder/

Question: 104

Your network contains an on-premises Active Directory domain named contoso.com that contains a member server named Server1.
You have the accounts shown in the following table.
You are installing Azure AD Connect on Server1.
You need to specify the account for Azure AD Connect synchronization. The solution must use the principle of
least privilege.
Which account should you specify?

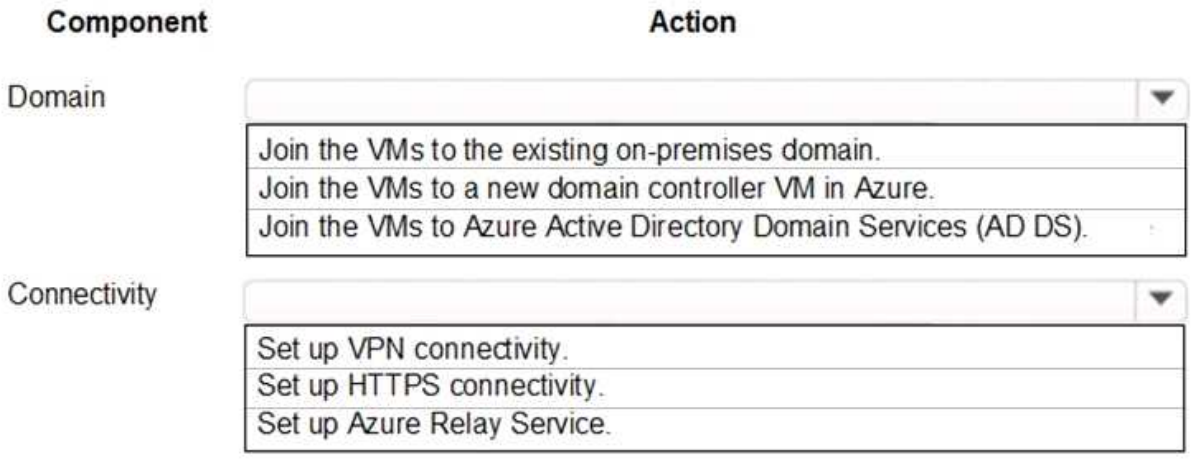
A. CONTOSO\User2
B. SERVER1\User4
C. CONTOSO\User1
D. CONTOSO\User3

Answer: A

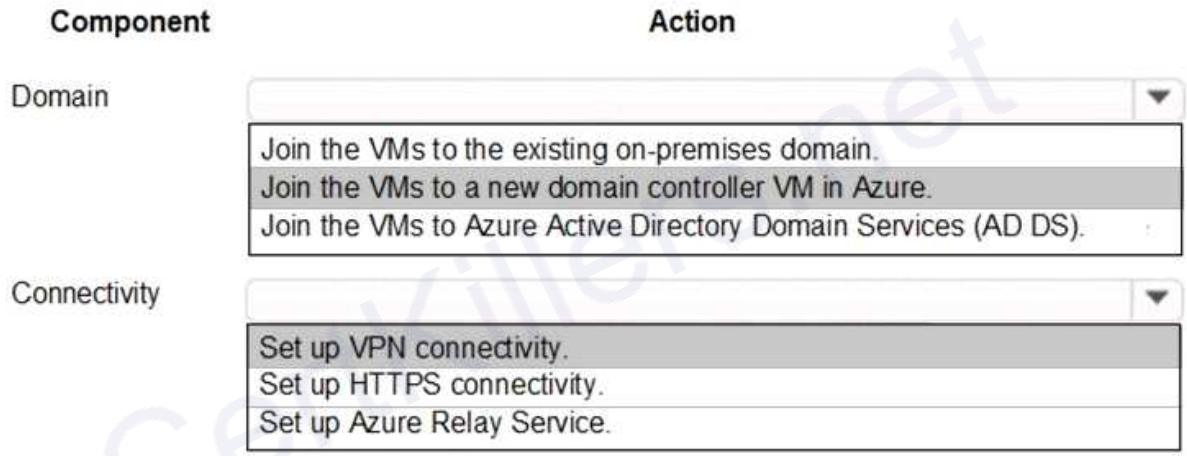
Explanation:
The default Domain User permissions are sufficient
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

Question: 105

HOTSPOT
A company runs multiple Windows virtual machines (VMs) in Azure.
The IT operations department wants to apply the same policies as they have for on-premises VMs to the VMs running in Azure, including domain administrator permissions and schema extensions.
You need to recommend a solution for the hybrid scenario that minimizes the amount of maintenance required.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
Box 1: Join the VMs to a new domain controller VM in Azure
Azure provides two solutions for implementing directory and identity services in Azure:
• (Used in this scenario) Extend your existing on-premises Active Directory infrastructure to Azure, by deploying a VM in Azure that runs AD DS as a Domain Controller. This architecture is more common when the on-premises network and the Azure virtual network (VNet) are connected by a VPN or ExpressRoute connection.
• Use Azure AD to create an Active Directory domain in the cloud and connect it to your on-premises Active Directory domain. Azure AD Connect integrates your on-premises directories with Azure AD.
Box 2: Set up VPN connectivity.
This architecture is more common when the on-premises network and the Azure virtual network (VNet) are connected by a VPN or ExpressRoute connection.
References:
https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/identity/

Question: 106

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

Name	Runtime stack
WebApp1	Java SE
WebApp2	Ruby 2.6
WebApp3	Python 3.7
WebApp4	ASP.NET V4.7

For which web app can you configure a WebJob?

A. WebApp4
B. WebApp3
C. WebApp1
D. WebApp2

Answer: A

Explanation:
Publishing a .NET Core WebJob to App Service from Visual Studio uses the same tooling as publishing an
ASP.NET Core app.
References:
https://docs.microsoft.com/en-us/azure/app-service/webjobs-dotnet-deploy-vs

Question: 107

The developers at your company request that you create databases in Azure Cosmos DB as shown in the following table.

Name	Requirement
CosmosDB1	• Provides a throughput of 1,200 RU/s • Has multiple write regions • Uses the Core (SQL) API
CosmosDB2	• Provides a throughput of 800 RU/s • Uses the MongoDB API
CosmosDB3	• Provides a throughput of 1,200 RU/s • Has only one write region • Uses the Core (SQL) API
CosmosDB4	• Provides a throughput of 2,000 RU/s • Uses the MongoDB API

You need to create the Azure Cosmos DB databases to meet the developer request. The solution

must minimize costs.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Create three Azure Cosmos DB accounts, one for the databases that use the Core (SQL) API, one for CosmosDB2, and one for CosmosDB4.
B. Create two Azure Cosmos DB accounts, one for CosmosDB2 and CosmosDB4 and one for CosmosDB1 and CosmosDB3.
C. Create one Azure Cosmos DB account for each database.
D. Create three Azure Cosmos DB accounts, one for the databases that use the MongoDB API, one for CosmosDB1, and one for CosmosDB3.

Answer: BD

Explanation:
Note:
Microsoft recommends using the same API for all access to the data in a given account.
One throughput provisioned container per subscription for SQL, Gremlin API, and Table accounts.
Up to three throughput provisioned collections per subscription for MongoDB accounts.
The throughput provisioned on an Azure Cosmos container is exclusively reserved for that container.
The container receives the provisioned throughput all the time.
Reference:
https://docs.microsoft.com/en-us/azure/cosmos-db/set-throughput#set-throughput-on-a-container

Question: 108

You have three Azure SQL Database servers shown in the following table.

Name	Resource group	Location
sqlserver1	RG1	West US
sqlserver2	RG1	West US
sqlserver3	RG2	West US
sqlserver4	RG1	West Europe
sqlserver5	RG2	West Europe

You plan to specify sqlserver1 as the primary server in a failover group.
Which servers can be used as a secondary server?

A. sqlserver4 and sqlserver5 only
B. sqlserver2 and sqlserver3 only
C. sqlserver1 and sqlserver3 only
D. sqlserver2 and sqlserver4 only

Answer: D

Explanation:
The Resource Group must be the same.
The secondary server can have another location.
The secondary server cannot be the same as the primary server.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/auto-failover-group-configure

Question: 109

Note: This question is part of 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 Active Directory (Azure AD) tenant that contains a group named Group1.
You need to enable multi-factor authentication (MFA) for the users in Group1 only.
Solution: From the Azure portal, you configure an authentication method policy.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
We should use a Conditional Access policy.
Note: There are two ways to secure user sign-in events by requiring multi-factor authentication in Azure AD. The first, and preferred, option is to set up a Conditional Access policy that requires multi-factor authentication under certain conditions. The second option is to enable each user for Azure Multi-Factor Authentication. When users are enabled individually, they perform multi-factor authentication each time they sign in (with some exceptions, such as when they sign in from trusted IP addresses or when the remembered devices feature is turned on).
Enabling Azure Multi-Factor Authentication using Conditional Access policies is the recommended approach. Changing user states is no longer recommended unless your licenses don't include Conditional Access as it requires users to perform MFA every time they sign in.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

Question: 110

Note: This question is part of 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 Active Directory (Azure AD) tenant that contains a group named Group1.
You need to enable multi-factor authentication (MFA) for the users in Group1 only.
Solution: From Multi-Factor Authentication, you select Bulk update, and you provide a CSV file that contains the members of Group1.
Does this meet the goal?

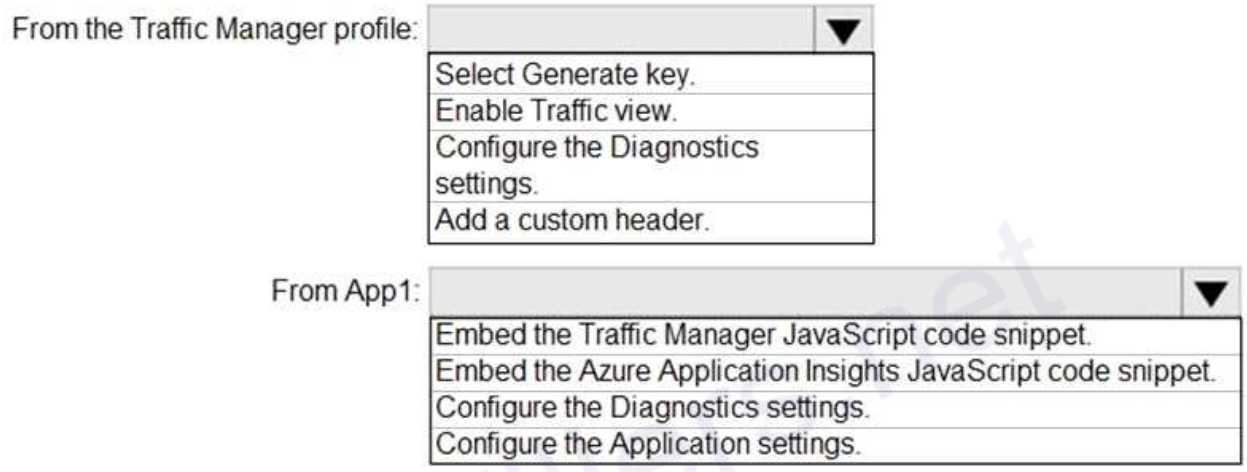
A. Yes
B. No

Answer: B

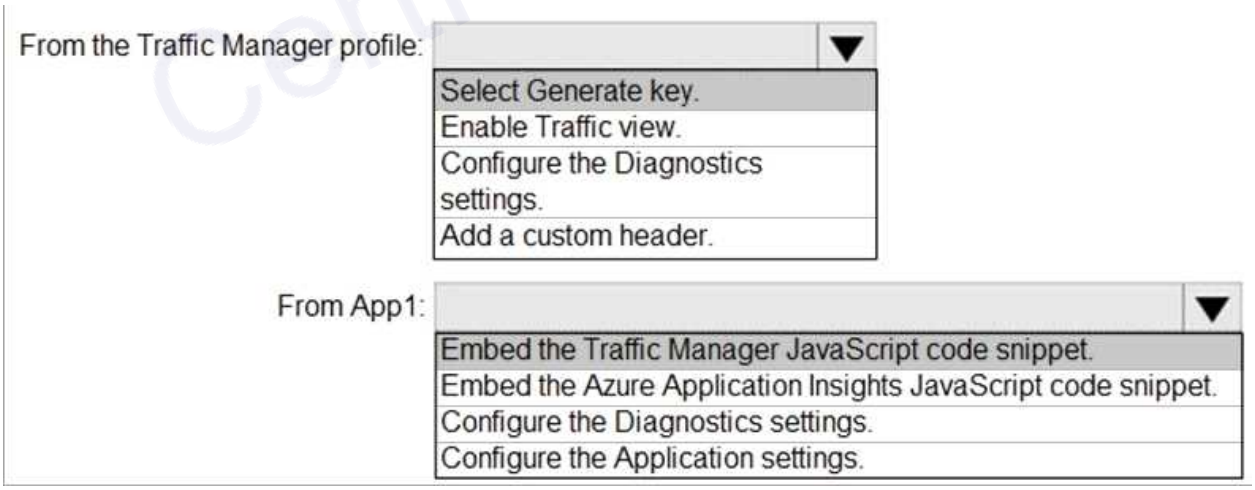
Explanation:
We should use a Conditional Access policy.
Note: There are two ways to secure user sign-in events by requiring multi-factor authentication in Azure AD. The first, and preferred, option is to set up a Conditional Access policy that requires multi-factor authentication under certain conditions. The second option is to enable each user for Azure Multi-Factor Authentication. When users are enabled individually, they perform multi-factor authentication each time they sign in (with some exceptions, such as when they sign in from trusted IP addresses or when the remembered devices feature is turned on).
Enabling Azure Multi-Factor Authentication using Conditional Access policies is the recommended approach. Changing user states is no longer recommended unless your licenses don't include Conditional Access as it requires users to perform MFA every time they sign in.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

Question: 111

HOTSPOT
You have a web server app named App1 that is hosted in three Azure regions.
You plan to use Azure Traffic Manager to distribute traffic optimally for App1.
You need to enable Real User Measurements to monitor the network latency data for App1.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer



Explanation:
Box 1: Select Generate key
You can configure your web pages to send Real User Measurements to Traffic Manager by obtaining a Real User Measurements (RUM) key and embedding the generated code to web page.
Obtain a Real User Measurements key
The measurements you take and send to Traffic Manager from your client application are identified by the service using a unique string, called the Real User Measurements (RUM) Key. You can get a

RUM key using the Azure portal, a REST API, or by using the PowerShell or Azure CLI.
To obtain the RUM Key using Azure portal:
• From a browser, sign in to the Azure portal. If you don't already have an account, you can sign up for a free one-month trial.
• In the portal's search bar, search for the Traffic Manager profile name that you want to modify, and then click the Traffic Manager profile in the results that the displayed.
• In the Traffic Manager profile blade, click Real User Measurements under Settings.
• Click Generate Key to create a new RUM Key.
Box 2: Embed the Traffic Manager JavaScript code snippet.
Embed the code to an HTML web page
After you have obtained the RUM key, the next step is to embed this copied JavaScript into an HTML page that your end users visit.
This example shows how to update an HTML page to add this script. You can use this guidance to adapt it to your HTML source management workflow.
• Open the HTML page in a text editor
• Paste the JavaScript code you had copied in the earlier step to the BODY section of the HTML (the copied code is on line 8 & 9, see figure 3).

```
1  <HTML>
2  <HEAD>
3  <TITLE>Webpage powered by Azure</TITLE>
4  </HEAD>
5  <BODY BGCOLOR="FFFFFF">
6  <H1>Welcome</H1>
7  <P> <B>Hello!</B>
8  <script src="//www.atmrum.net/rum.js"></script>
9  <script>rum.start("0123456789abcdef0123456789abcdff");</script>
10 </BODY>
11 </HTML>
```

Reference:
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-create-rum-web-pages