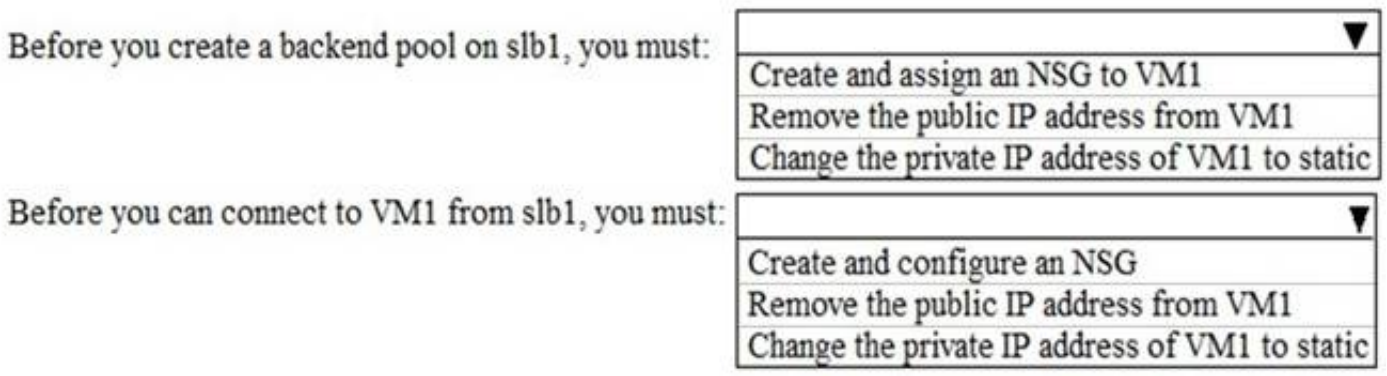
Microsoft

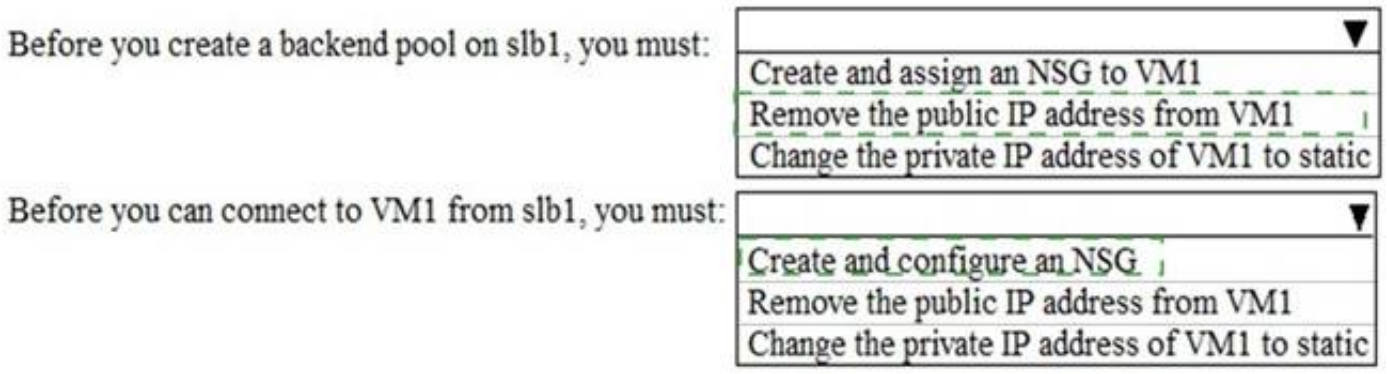
Exam Questions AZ-104

Microsoft Azure Administrator

NEW QUESTION 1
HOTSPOT - (Topic 5)
You have an Azure virtual machine named VM1 that connects to a virtual network named VNet1. VM1 has the following configurations:
? Subnet: 10.0.0.0/24
? Availability set: AVSet
? Network security group (NSG): None
? Private IP address: 10.0.0.4 (dynamic)
? Public IP address: 40.90.219.6 (dynamic)
You deploy a standard, Internet-facing load balancer named slb1. You need to configure slb1 to allow connectivity to VM1.
Which changes should you apply to VM1 as you configure slb1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Remove the public IP address from VM1
If the Public IP on VM1 is set to Dynamic, that means it is a Public IP with Basic SKU because Public IPs with Standard SKU have Static assignments by default, that cannot be changed. We cannot associate Basic SKUs IPs with Standard SKUs LBs. One cannot create a backend SLB pool if the VM to be associated has a Public IP. For Private IP it doesn't matter weather it is dynamic or static, still we can add the such VM into the SLB backend pool.
Box 2: Create and configure an NSG
Standard Load Balancer is built on the zero trust network security model at its core. Standard Load Balancer secure by default and is part of your virtual network. The virtual network is a private and isolated network. This means Standard Load Balancers and Standard Public IP addresses are closed to inbound flows unless opened by Network Security Groups. NSGs are used to explicitly permit allowed traffic. If you do not have an NSG on a subnet or NIC of your virtual machine resource, traffic is not allowed to reach this resource. To learn more about NSGs and how to apply them for your scenario, see Network Security Groups. Basic Load Balancer is open to the internet by default.

NEW QUESTION 2
- (Topic 5)
You have an Azure subscription. The subscription contains virtual machines that connect to a virtual network named VNet1.
You plan to configure Azure Monitor for VM Insights.
You need to ensure that all the virtual machines only communicate with Azure Monitor through VNet1.
What should you create first?

A. an Azure Monitor Private Link Scope (AMPIS)
B. a private endpoint
C. a Log Analytics workspace
D. a data collection rule (DCR)

Answer: A

Explanation:
Azure Monitor for VM Insights is a feature of Azure Monitor that provides comprehensive monitoring and diagnostics for your Azure virtual machines and virtual machine scale sets. It collects performance data, process information, and network dependencies from your virtual machines and displays them in interactive charts and maps. You can use Azure Monitor for VM Insights to troubleshoot performance issues, optimize resource utilization, and identify network bottlenecks1.
To enable Azure Monitor for VM Insights, you need to install two agents on your virtual machines: the Azure Monitor agent (preview) and the Dependency agent. The Azure Monitor agent collects performance metrics and sends them to a Log Analytics workspace. The Dependency agent collects process information and network dependencies and sends them to the InsightsMetrics table in the same workspace2.
By default, the agents communicate with Azure Monitor over the public internet. However, if you want to ensure that all the virtual machines only communicate with Azure Monitor through a virtual network named VNet1, you need to configure private network access for the agents.
Private network access allows the agents to communicate with Azure Monitor using a private endpoint, which is a special network interface that connects your virtual network to an Azure service without exposing it to the public internet. A private endpoint uses a private IP address from your virtual network address space, so you can

secure and control the network traffic between your virtual machines and Azure Monitor3.
To configure private network access for the agents, you need to create an Azure Monitor Private Link Scope (AMPIS) first. An AMPIS is a resource that groups one or more Log Analytics workspaces together and associates them with a private endpoint. An AMPIS allows you to manage the private connectivity settings for multiple workspaces in one place4.
After creating an AMPIS, you need to create a private endpoint in VNet1 and link it to the AMPIS. This will enable the agents on your virtual machines to send data to the Log Analytics workspaces in the AMPIS using the private IP address of the private endpoint5.

NEW QUESTION 3
HOTSPOT - (Topic 5)

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

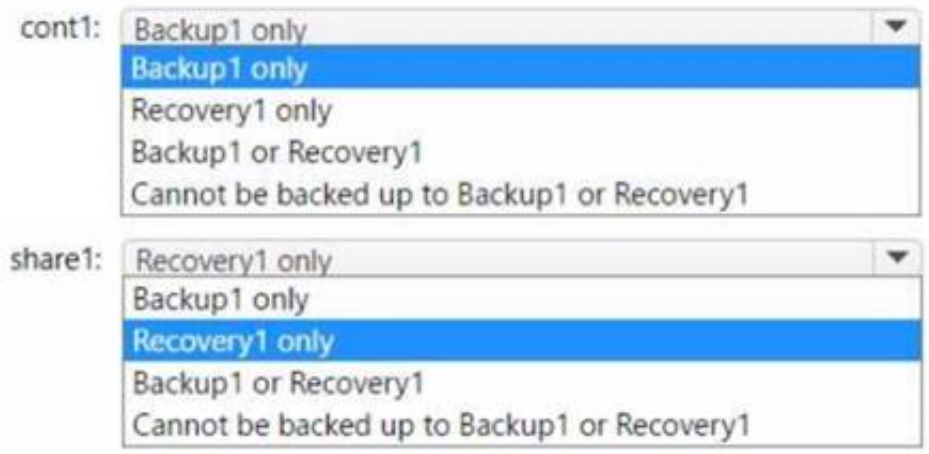
Name	Type
Backup1	Backup vault
Recovery1	Recovery Services vault

You create a storage account that contains the resources shown in the following table.

Name	Type
cont1	Blob container
share1	File share

To which vault can you back up cont1 and share1? To answer, select the appropriate options in the answer area. NOTE: Each correct answer is worth one point.

Answer Area

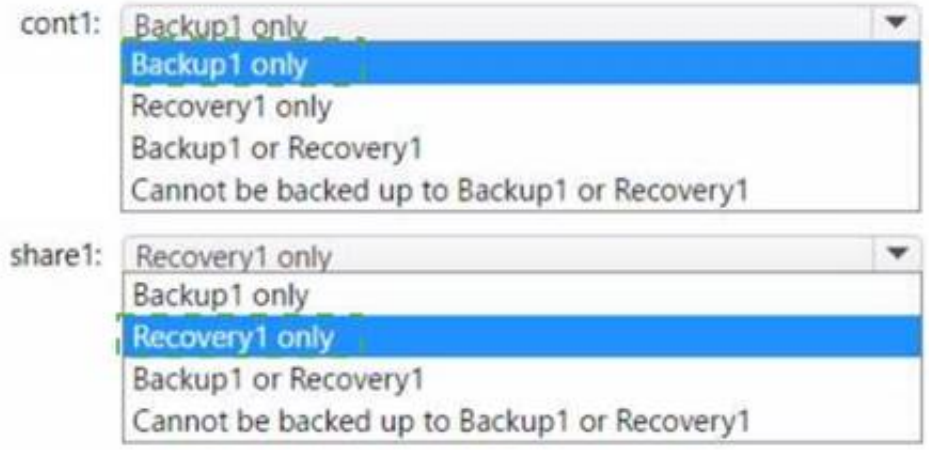


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



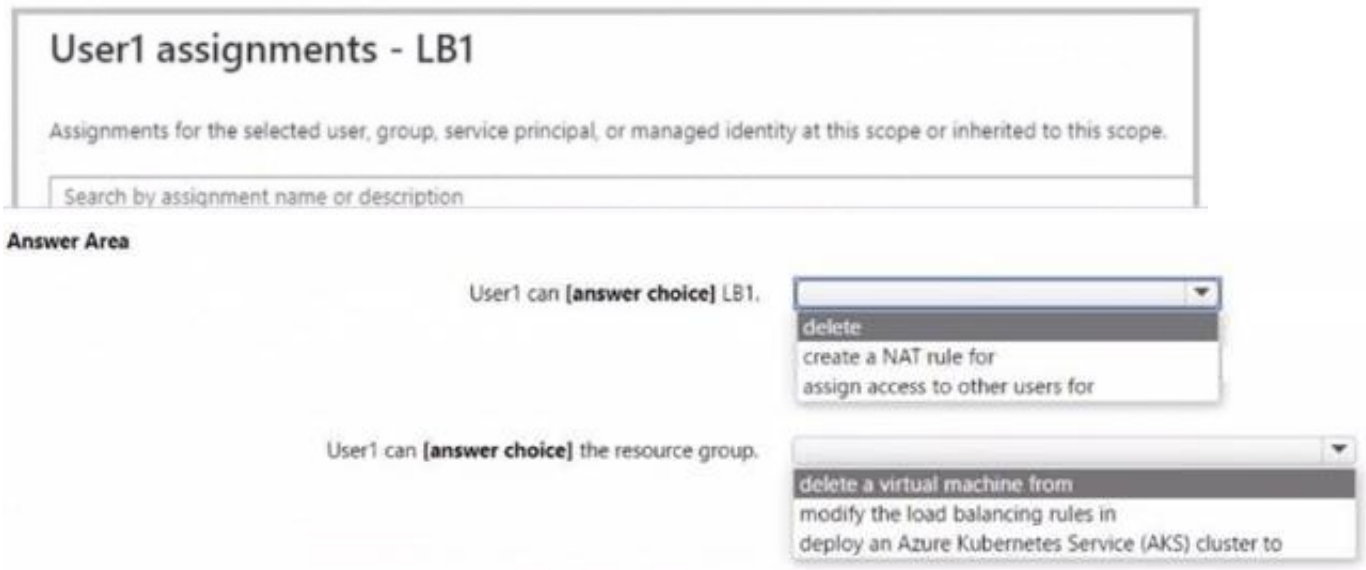
NEW QUESTION 4
- (Topic 5)
You have an Azure subscription that contains two Log Analytics workspaces named Workspace 1 and Workspace? and 100 virtual machines that run Windows Server.
You need to collect performance data and events from the virtual machines. The solution must meet the following requirements:
• Logs must be sent to Workspace! and Workspace?
• All Windows events must be captured
• All security events must be captured.
What should you install and configure on each virtual machine?

A. the Azure Monitor agent
B. the Windows Azure diagnostics extension (WAD)
C. the Windows VM agent

Answer: A

Explanation:
https://learn.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview Azure Monitor Agent (AMA) collects monitoring data from the guest operating system of Azure and hybrid virtual machines and delivers it to Azure Monitor for use by features, insights, and other services, such as Microsoft Sentinel and Microsoft Defender for Cloud. Azure Monitor Agent replaces all of Azure Monitor's legacy monitoring agents.

NEW QUESTION 5
HOTSPOT - (Topic 5)
You have an Azure Load Balancer named LB1.
You assign a user named User1 the roles shown in the following exhibit.



A. Mastered
B. Not Mastered

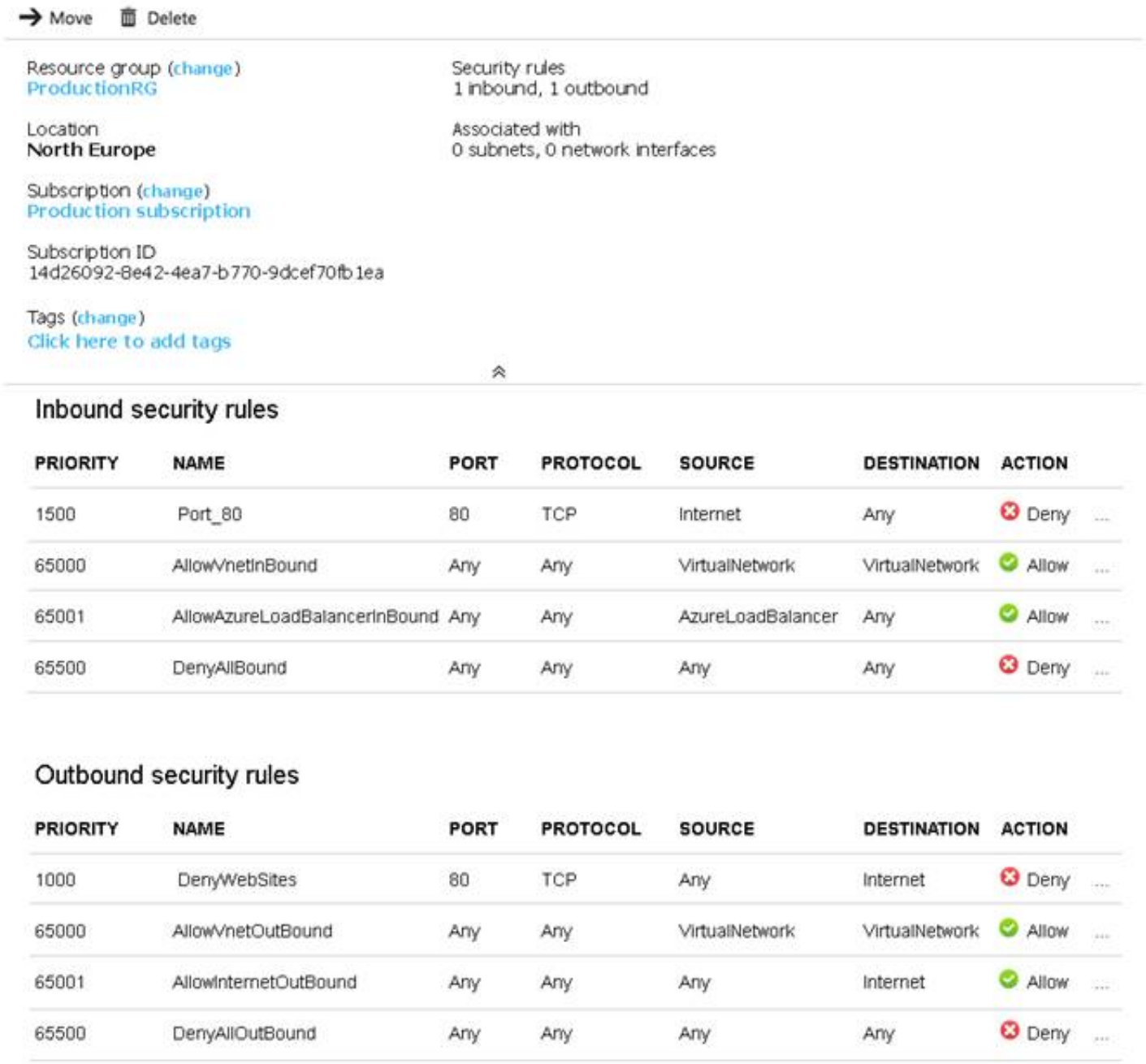
Answer: A

Explanation:
User Access Administrator can only assign access to other users
https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory- admin-roles
Virtual Machine Contributor can Manage VMs, which includes deleting VMs too. https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor
https://docs.microsoft.com/en-us/answers/questions/350635/can-virtual-machine-contributor-create-vm.html

NEW QUESTION 6
- (Topic 5)
You have an Azure subscription that contains the resources in the following table.

Name	Type	Details
VNet1	Virtual network	*Not applicable*
Subnet1	Subnet	Hosted on VNet1
VM1	Virtual machine	On Subnet1
VM2	Virtual machine	On Subnet1

VM1 and VM2 are deployed from the same template and host line-of-business applications accessed by using Remote Desktop. You configure the network security group (NSG) shown in the exhibit. (Click the Exhibit button.)



You need to prevent users of VM1 and VM2 from accessing websites on the Internet. What should you do?

A. Associate the NSG to Subnet1.
B. Disassociate the NSG from a network interface.
C. Change the DenyWebSites outbound security rule.
D. Change the Port_80 inbound security rule

Answer: A

Explanation:
Outbound rule “DenyWebSites” is setup correctly to block outbound internet traffic over port 80. In the screenshot it states, "Associated with: 0 subnets, 0 NIC's", so you need to associate the NSG to Subnet1.You can associate or dissociate a network security group from a NIC or Subnet. Reference: https://docs.microsoft.com/en-us/azure/virtual- network/manage-network-security-group

NEW QUESTION 7
- (Topic 5)
You deploy an Azure Kubernetes Service (AKS) cluster named Cluster1 that uses the IP addresses shown in the following table.

IP address	Assigned to
131.107.2.1	Load balancer front end
192.168.10.2	Kubernetes DNS service
172.17.7.1	Docker bridge address
10.0.10.11	Kubernetes cluster node

You need to provide internet users with access to the applications that run in Cluster1. Which IP address should you include in the DNS record for Ousted?

A. 172.17.7.1
B. 131.107.2.1
C. 192.168.10.2
D. 10.0.10.11

Answer: B

Explanation:
When any internet user will try to access the cluster which is behind a load balancer, traffic will first hit to load balancer front end IP. So in the DNS configuration you have to provide the IP address of the load balancer.
Reference:
https://stackoverflow.com/questions/43660490/giving-a-dns-name-to-azure-load-balancer

NEW QUESTION 8

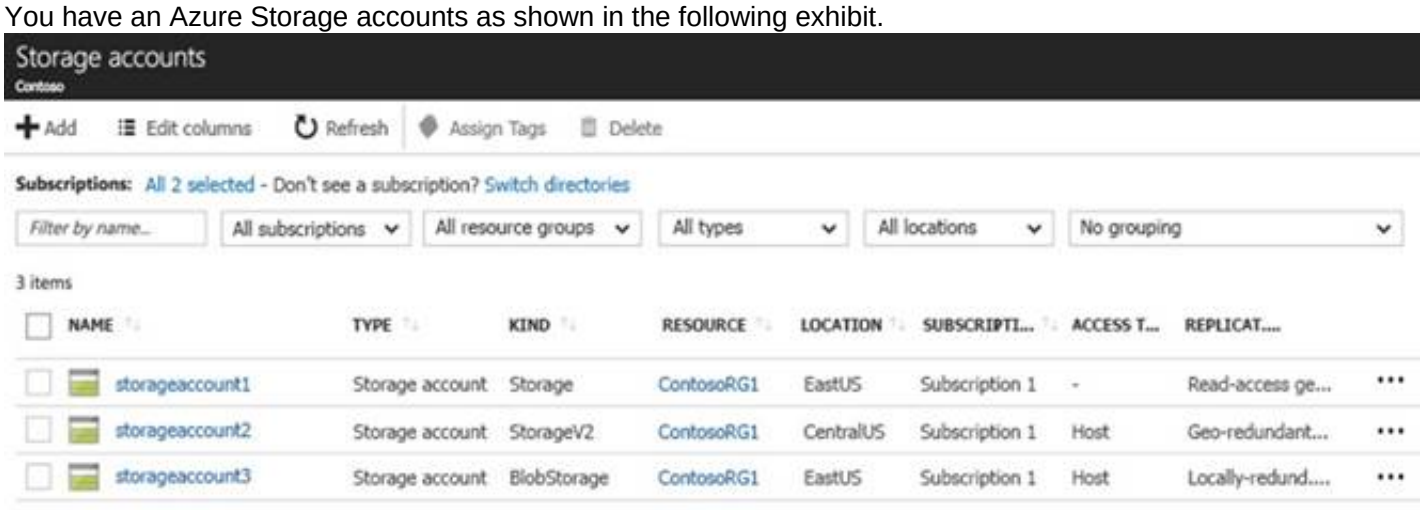
- (Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After 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 Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev.
You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.
Solution: On Subscription1, you assign the Logic App Operator role to the Developers group.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The Logic App Operator role only grants the ability to read, enable, disable, and run logic apps. It does not grant the ability to create logic apps. To create logic apps, you need to assign the Logic App Contributor role or a higher-level role such as Owner or Contributor. Then, References: [Built-in roles for Azure resources] [Azure Logic Apps permissions and access control]

NEW QUESTION 9
HOTSPOT - (Topic 5)
You have an 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.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: storageaccount1 and storageaccount2 only Box 2: All the storage accounts
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

NEW QUESTION 10
- (Topic 5)
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Resource group
VNET1	Virtual network	RG1
VM1	Virtual machine	RG1

The Not allowed resource types Azure policy that has policy enforcement enabled is assigned to RG1 and uses the following parameters:
Microsoft.Network/virtualNetworks Microsoft.Compute/virtualMachines
In RG1, you need to create a new virtual machine named VM2 which is connected toVNET1. What should you do first?

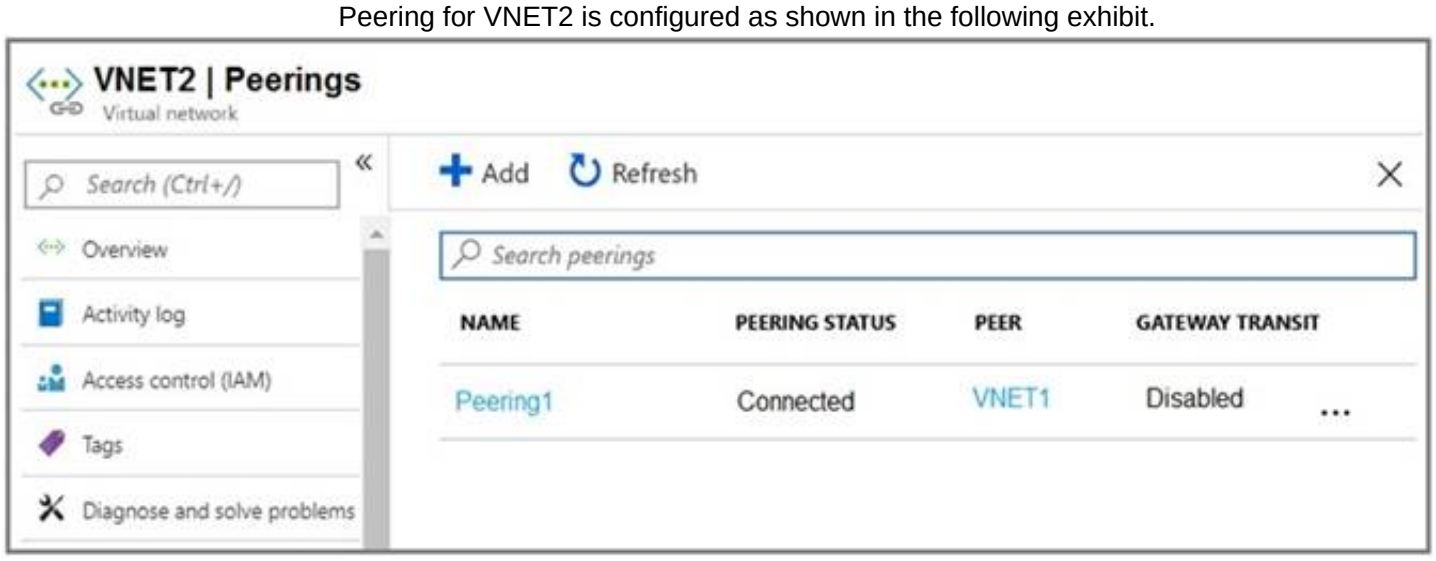
Create an Azure Resource Manager template.

A
B: AddasubnettoVNET1.
C. Remove Microsof
D. Network/virtualNetworks from the policy.
E. Remove Microsoft.Compute/virtualMachines from the policy.

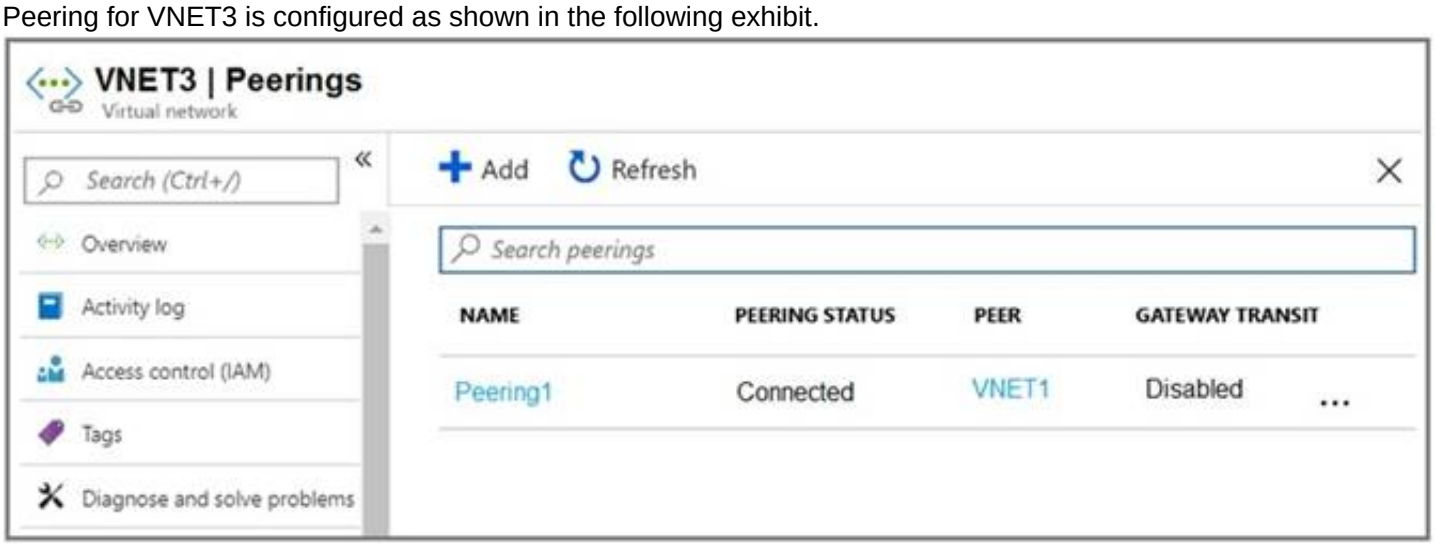
Answer: C

Explanation:
To create a new virtual machine named VM2 which is connected to VNET1 in RG1, you need to remove Microsoft.Network/virtualNetworks from the policy. This is because the Not allowed resource types Azure policy denies the deployment of the specified resource types in the scope of the assignment. In this case, the policy is assigned to RG1 and uses the parameters Microsoft.Network/virtualNetworks and Microsoft.Compute/virtualMachines. This means that you cannot create or update any virtual networks or virtual machines in RG1. Therefore, to create VM2 and connect it to VNET1, you need to remove Microsoft.Network/virtualNetworks from the policy parameters. This will allow you to create or update virtual networks in RG1, but still prevent you from creating or updating virtual machines. Alternatively, you can also exclude VNET1 from the policy assignment scope, but this will affect the compliance of the policy for the entire virtual network.
References:
? Not allowed resource types (Deny)
? Create and manage policies to enforce compliance

NEW QUESTION 10
HOTSPOT - (Topic 5)
Peering for VNET2 is configured as shown in the following exhibit.



Peering for VNET3 is configured as shown in the following exhibit.

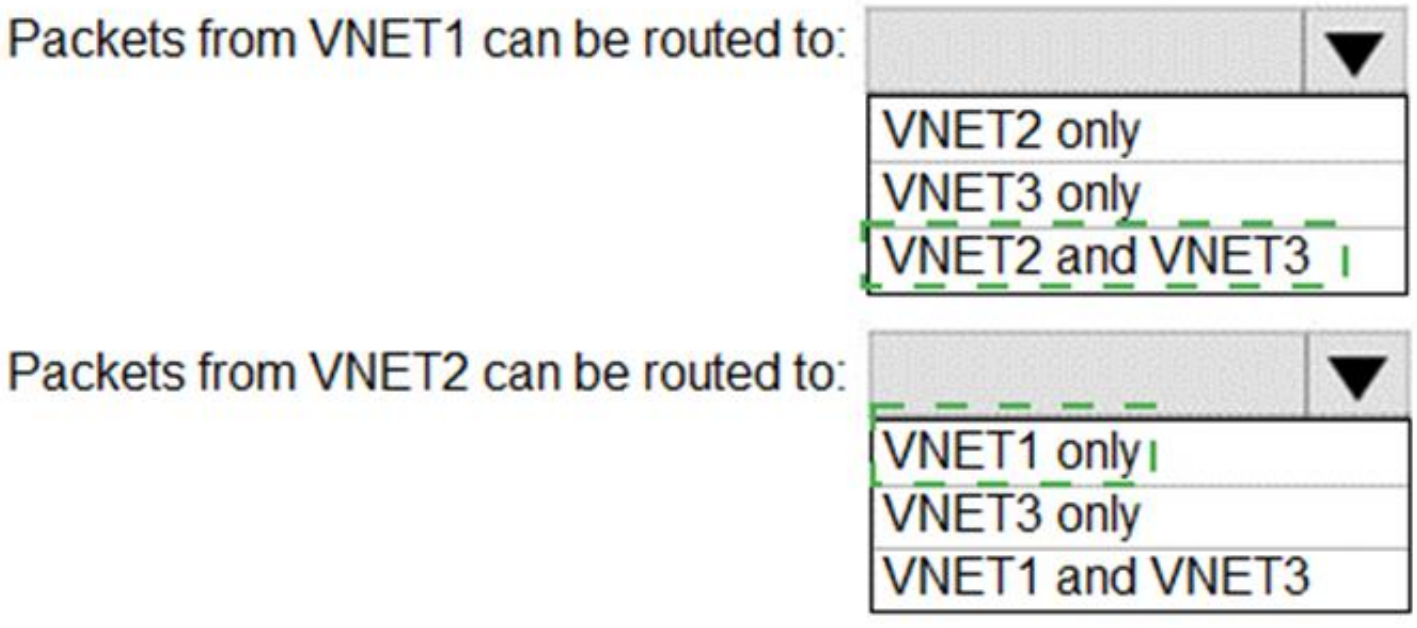


How can packets be routed between the virtual networks? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Packets from VNET1 can be routed to:
- VNET2 only
- VNET3 only
- VNET2 and VNET3

Packets from VNET2 can be routed to:
- VNET1 only
- VNET3 only
- VNET1 and VNET3

Answer:



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1. VNET2 and VNET3 Box 2: VNET1
Gateway transit is disabled.

NEW QUESTION 11
- (Topic 5)
You have an Azure virtual machine named VM1.
You use Azure Backup to create a backup of VM1 named Backup1. After creating Backup1, you perform the following changes to VM1:
? Modify the size of VM1.
? Copy a file named Budget.xls to a folder named Data.
? Reset the password for the built-in administrator account.
? Add a data disk to VM1.
An administrator uses the Replace existing option to restore VM1 from Backup1. You need to ensure that all the changes to VM1 are restored.
Which change should you perform again?

A. Modify the size of VM1.
B. Add a data disk.
C. Reset the password for the built-in administrator account.
D. Copy Budget.xls to Data.

Answer: D

Explanation:
The scenario mentioned in the question, we are using the replace option. So in this case we would lose the existing data written to the disk after the backup was taken. The file was copied to the disk after the backup was taken. Hence, we would need to copy the file once again.
References:
https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms#replace- existing-disks

NEW QUESTION 15
HOTSPOT - (Topic 5)
You have an Azure subscription named Sub1.
You plan to deploy a multi-tiered application that will contain the tiers shown in the following table.

Tier	Accessible from the Internet	Number of virtual machines
Front-end web server	Yes	10
Business logic	No	100
Microsoft SQL Server database	No	5

You need to recommend a networking solution to meet the following requirements:
• Ensure that communication between the web servers and the business logic tier spreads equally across the virtual machines.
• Protect the web servers from SQL injection attacks.
Which Azure resource should you recommend for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: an internal load balancer
Azure Internal Load Balancer (ILB) provides network load balancing between virtual machines that reside inside a cloud service or a virtual network with a regional scope.
Box 2: an application gateway that uses the WAF tier
Azure Web Application Firewall (WAF) on Azure Application Gateway 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. Application gateway which uses WAF tier.

NEW QUESTION 16
- (Topic 5)
You have an Azure App Services web app named App1. You plan to deploy App1 by using Web Deploy.
You need to ensure that the developers of App1 can use their Azure Active Directory (Azure AD) credentials to deploy content to App1. The solution must use the principle of least privilege.
What should you do?

A. Configure app-level credentials for FTPS.
B. Assign The Website Contributor role to the developers.
C. Assign the Owner role to the developers.
D. Configure user-level credentials for FTPS.

Answer: B

Explanation:
"To secure app deployment from a local computer, Azure App Service supports two types of credentials for local Git deployment and FTP/S deployment. These credentials are not the same as your Azure subscription credentials." https://learn.microsoft.com/en- us/azure/app-service/deploy-configure-credentials?tabs=cli

NEW QUESTION 17
- (Topic 5)
You have the Azure virtual networks shown in the following table.

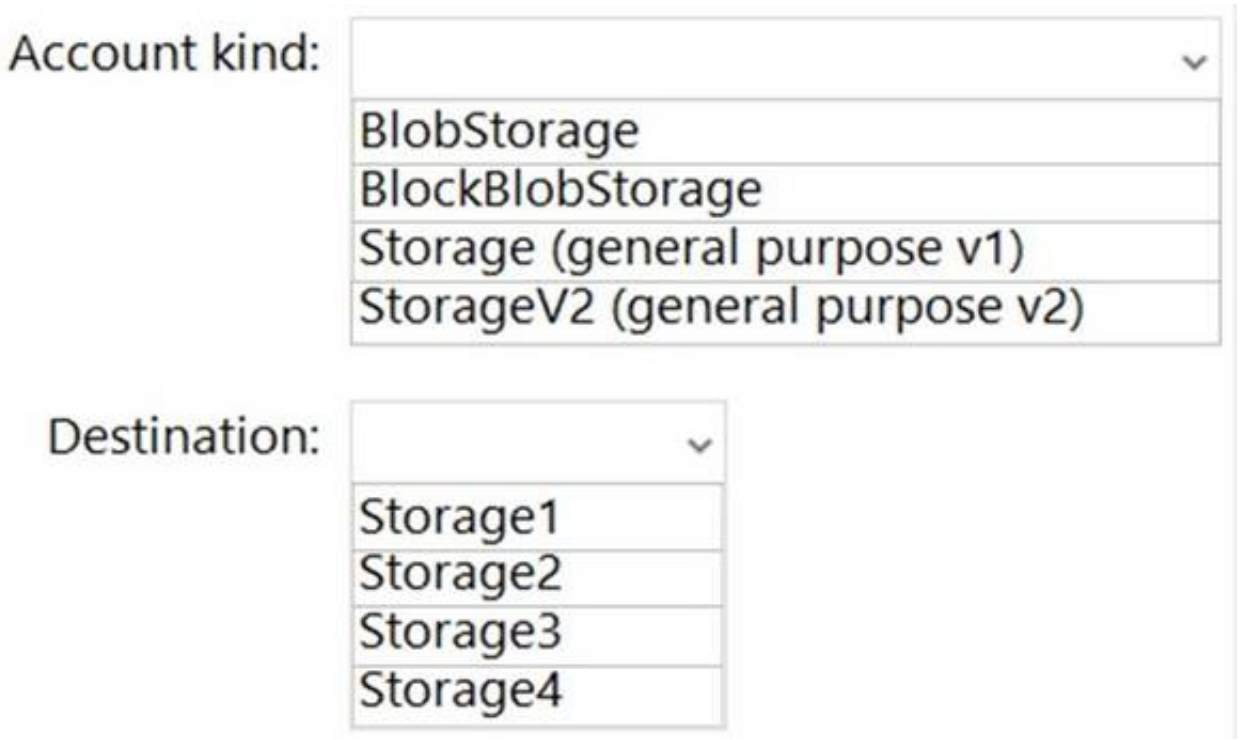
Name	Address space	Subnet	Resource group Azure region
VNet1	10.11.0.0/16	10.11.0.0/17	West US
VNet2	10.11.0.0/17	10.11.0.0/25	West US
VNet3	10.10.0.0/22	10.10.1.0/24	East US
VNet4	192.168.16.0/22	192.168.16.0/24	North Europe

To which virtual networks can you establish a peering connection from VNet1?

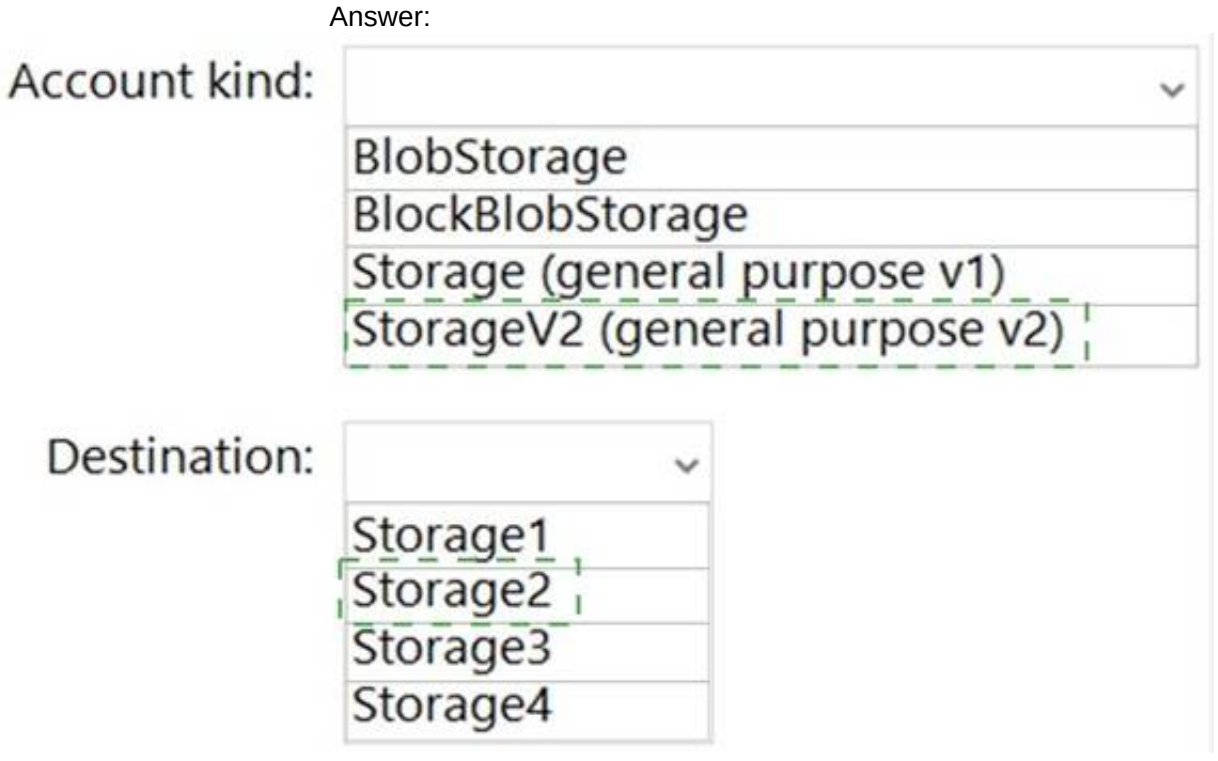
A. VNet2, VNet3, and VNet4
B. VNet2only
C. VNet3 and VNet4 only
D. VNet2 and VNet3 only

Answer: C

NEW QUESTION 18
HOTSPOT - (Topic 4)
You need to create storage5. The solution must support the planned changes.
Which type of storage account should you use, and which account should you configure as the destination storage account? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 21
- (Topic 5)
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 need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.
Solution: You assign the Traffic Manager Contributor role at the subscription level to Admin1

A. Yes
B. NO

Answer: B

Explanation:
The Traffic Manager Contributor role is not related to Traffic Analytics. Traffic Manager is a service that provides DNS-based load balancing and traffic routing across different regions and endpoints. Traffic Manager Contributor is a role that allows you to create and manage Traffic Manager profiles, endpoints, and geographies1.
Traffic Analytics is a service that provides visibility into user and application activity in your cloud networks. Traffic Analytics analyzes Azure Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud. With Traffic Analytics, you can visualize network activity, identify hot spots, secure your network, optimize your network deployment, and pinpoint network misconfigurations2.
To enable Traffic Analytics for an Azure subscription, you need to have a role that grants you the following permissions at the subscription level:
? Microsoft.Network/applicationGateways/read
? Microsoft.Network/connections/read
? Microsoft.Network/loadBalancers/read
? Microsoft.Network/localNetworkGateways/read
? Microsoft.Network/networkInterfaces/read
? Microsoft.Network/networkSecurityGroups/read
? Microsoft.Network/publicIPAddresses/read
? Microsoft.Network/routeTables/read
? Microsoft.Network/virtualNetworkGateways/read

? Microsoft.Network/virtualNetworks/read
? Microsoft.OperationalInsights/workspaces/*
Some of the built-in roles that have these permissions are Owner, Contributor, or Network Contributor3. However, these roles also grant other permissions that may not be necessary or desirable for enabling Traffic Analytics. Therefore, the best practice is to use the principle of least privilege and create a custom role that only has the required permissions for enabling Traffic Analytics4.
Therefore, to meet the goal of ensuring that an Azure AD user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription, you should create a custom role with the required permissions and assign it to Admin1 at the subscription level.

NEW QUESTION 24
- (Topic 4)
You need to add VM1 and VM2 to the backend poo! of LB1. What should you do first?

A. Create a new NSG and associate the NSG to VNET1/Subnet1.
B. Connect VM2 to VNET1/Subnet1.
C. Redeploy VM1 and VM2 to the same availability zone.
D. Redeploy VM1 and VM2 to the same availability set.

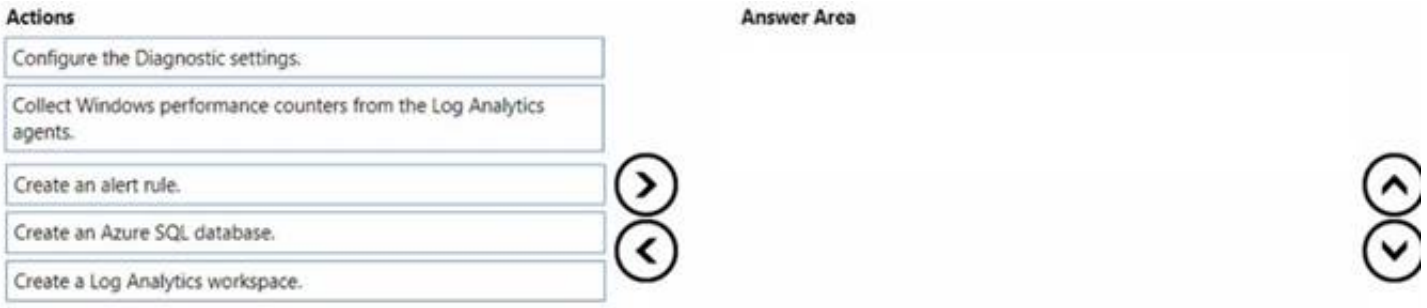
Answer: B

NEW QUESTION 28
- (Topic 4)
You need to ensure that you can grant Group4 Azure RBAC read-only permissions to all the A2ure file shares. What should you do?

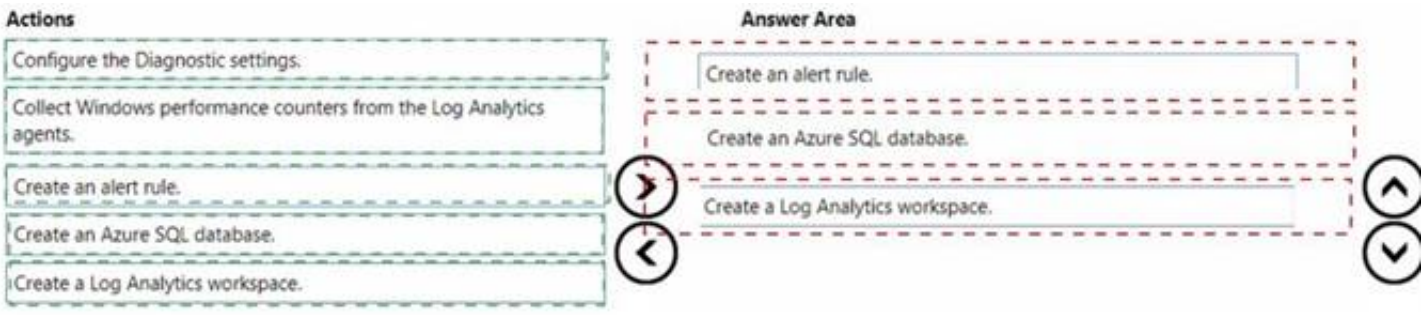
A. On storagel and storage4, change the Account kind type to StorageV2 (general purpose v2).
B. Recreate storage2 and set Hierarchical namespace to Enabled.
C. On storage2, enable identity-based access for the file shares.
D. Create a shared access signature (SAS) for storagel, storage2, and storage4.

Answer: A

NEW QUESTION 29
DRAG DROP - (Topic 4)
You need to configure the alerts for VM1 and VM2 to meet the technical requirements.
Which three actions should you perform in sequence? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 30
- (Topic 3)
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 Interne
B. Associate the NSG to all the subnets.
C. Create an incoming security rule for port 443 from the Interne
D. Associate the NSG to all the subnets.
E. Create an incoming security rule for port 443 from the Interne
F. Associate the NSG to the subnet that contains the web servers.
G. Create an outgoing security rule for port 443 from the Interne
H. 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.

NEW QUESTION 32
- (Topic 2)
You need to resolve the Active Directory issue. What should you do?

A. From Active Directory Users and Computers, select the user accounts, and then modify the User Principal Name value.
B. Run idfix.exe, and then use the Edit action.
C. From Active Directory Domains and Trusts, modify the list of UPN suffixes.
D. From Azure AD Connect, modify the outbound synchronization rule.

Answer: B

Explanation:
IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.
Scenario: Active Directory Issue

Several users in humongousinsurance.com have UPNs that contain special characters. You suspect that some of the characters are unsupported in Azure AD.
References: https://www.microsoft.com/en-us/download/details.aspx?id=36832

NEW QUESTION 33
- (Topic 2)
Which blade should you instruct the finance department auditors to use?

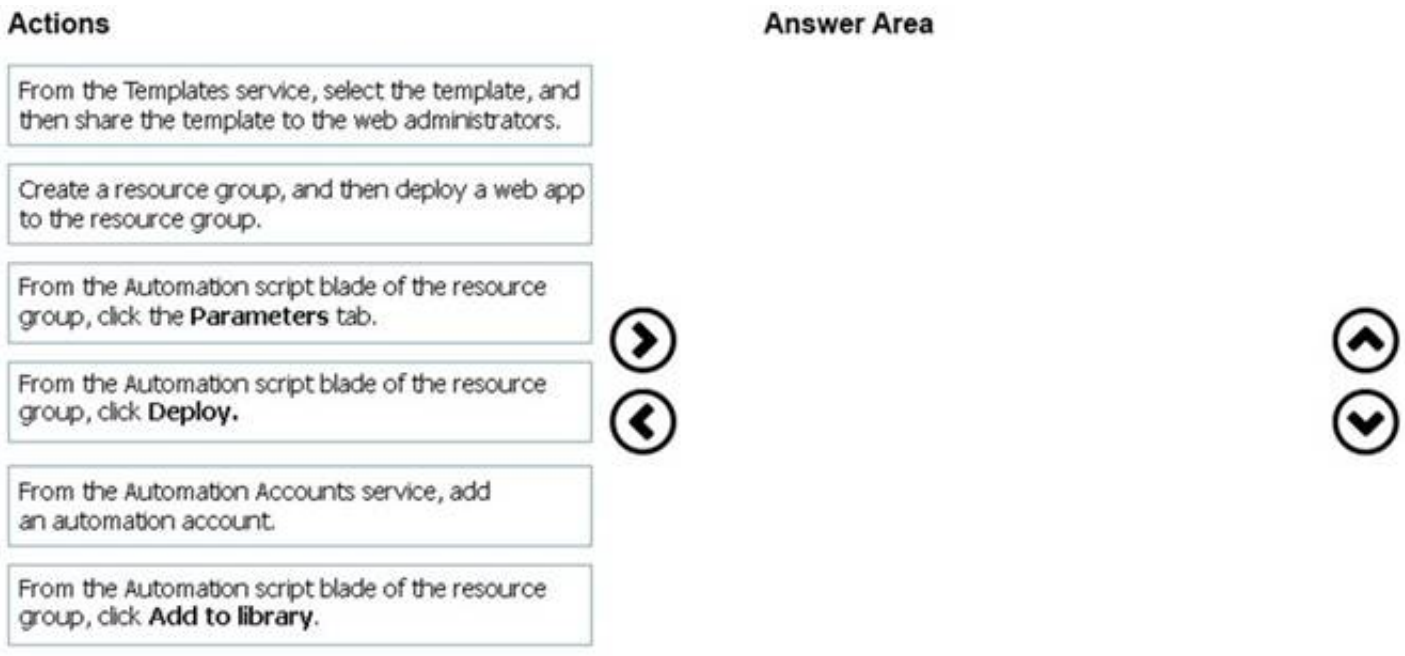
A. Partner information
B. Overview
C. Payment methods
D. Invoices

Answer: D

Explanation:
You can opt in and configure additional recipients to receive your Azure invoice in an email. This feature may not be available for certain subscriptions such as support offers, Enterprise Agreements, or Azure in Open.
? Select your subscription from the Subscriptions page. Opt-in for each subscription you own. Click Invoices then Email my invoice.A screenshot of a computer

Description automatically generated
? Click Opt in and accept the terms.
Scenario: During the testing phase, auditors in the finance department must be able to review all Azure costs from the past week.
References: https://docs.microsoft.com/en-us/azure/billing/billing-download-azure-invoice-daily-usage-date

NEW QUESTION 35
DRAG DROP - (Topic 2)
You need to prepare the environment to ensure that the web administrators can deploy the web apps as quickly as possible.
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 1. Web administrators will deploy Azure web apps for the marketing department.
* 2. Each web app will be added to a separate resource group.

* 3. The initial configuration of the web apps will be identical.
* 4. The web administrators have permission to deploy web apps to resource groups.
Steps:
1 --> Create a resource group, and then deploy a web app to the resource group.
2 --> From the Automation script blade of the resource group , click Add to Library.
3 --> From the Templates service, select the template, and then share the template to the web administrators .
References:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/quickstart-create-templates-use-the-portal

NEW QUESTION 36
- (Topic 2)
You need to prepare the environment to meet the authentication requirements.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Allow inbound TCP port 8080 to the domain controllers in the Miami office.
B. Add http://autogon.microsoftazuread-sso.com to the intranet zone of each client computer in the Miami office.
C. Join the client computers in the Miami office to Azure AD.
D. Install the Active Directory Federation Services (AD FS) role on a domain controller in the Miami office.
E. Install Azure AD Connect on a server in the Miami office and enable Pass-through Authentication.

Answer: BE

Explanation:
B: You can gradually roll out Seamless SSO to your users. You start by adding the following Azure AD URL to all or selected users' Intranet zone settings by using Group Policy in Active Directory: https://autologon.microsoftazuread-sso.com
E: Seamless SSO works with any method of cloud authentication - Password Hash Synchronization or Pass-through Authentication, and can be enabled via Azure AD Connect.
References:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick- start

NEW QUESTION 38
- (Topic 1)
You discover that VM3 does NOT meet the technical requirements. You need to verify whether the issue relates to the NSGs.
What should you use?

A. Diagram in VNet1
B. the security recommendations in Azure Advisor
C. Diagnostic settings in Azure Monitor
D. Diagnose and solve problems in Traffic Manager Profiles
E. IP flow verify in Azure Network Watcher

Answer: E

Explanation:
Scenario: Litware must meet technical requirements including:
Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.
IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps

administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.
References:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify- overview

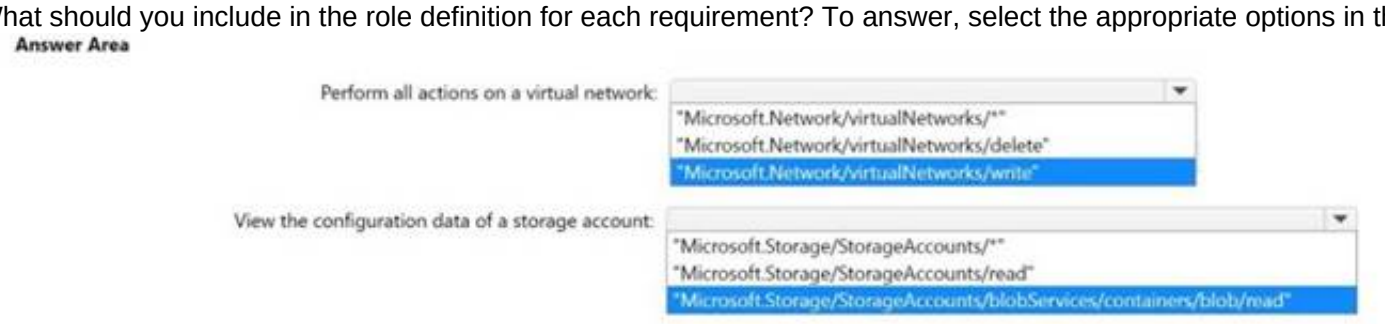
NEW QUESTION 41
- (Topic 1)
You need to meet the technical requirement for VM4. What should you create and configure?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Scenario: Create a workflow to send an email message when the settings of VM4 are modified.
You can start an automated logic app workflow when specific events happen in Azure resources or third-party resources. These resources can publish those events to an Azure event grid. In turn, the event grid pushes those events to subscribers that have queues, webhooks, or event hubs as endpoints. As a subscriber, your logic app can wait for those events from the event grid before running automated workflows to perform tasks - without you writing any code.
References:
https://docs.microsoft.com/en-us/azure/event-grid/monitor-virtual-machine-changes-event- grid-logic-app

NEW QUESTION 42
HOTSPOT - (Topic 5)
You have an Azure subscription.
You plan to create a role definition to meet the following requirements:
• Users must be able to view the configuration data of a storage account.
• Users must be able to perform all actions on a virtual network.
• The solution must use the principle of least privilege.
What should you include in the role definition for each requirement? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Perform all actions on a virtual network: “Microsoft.Network/virtualNetworks/*”
View the configuration data of a storage account: “Microsoft.Storage/StorageAccounts/read”
To perform all actions on a virtual network, you need to use the wildcard () character in the action string, which grants access to all actions that match the string. The action string for virtual networks is "Microsoft.Network/virtualNetworks/". To view the configuration data of a storage account, you need to use the read action substring in the action string, which enables read actions (GET). The action string for storage accounts is “Microsoft.Storage/StorageAccounts/read”. References:
? https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions
? https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

NEW QUESTION 45

HOTSPOT - (Topic 5)
You have an Azure Active Directory tenant named Contoso.com that includes following users:

Name	Role
User1	Cloud device administrator
User2	User administrator

Contoso.com includes following Windows 10 devices:

Name	Join type
Device1	Azure AD registered
Device2	Azure AD joined

You create following security groups in Contoso.com:

Name	Join type	Owner
Group1	Assigned	User1
Group2	Dynamic Device	User2

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

Statements	Yes	No
User1 can add Device2 to Group1	○	○
User2 can add Device1 to Group1	○	○
User2 can add Device2 to Group2	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
User1 is a Cloud Device Administrator. Device2 is Azure AD joined.

Group1 has the assigned to join type. User1 is the owner of Group1.
Note: Assigned groups - Manually add users or devices into a static group.
Azure AD joined or hybrid Azure AD joined devices utilize an organizational account in Azure AD
Box 2: No
User2 is a User Administrator. Device1 is Azure AD registered.
Group1 has the assigned join type, and the owner is User1.
Note: Azure AD registered devices utilize an account managed by the end user, this account is either a Microsoft account or another locally managed credential.
Box 3: Yes
User2 is a User Administrator. Device2 is Azure AD joined.
Group2 has the Dynamic Device join type, and the owner is User2.
References:
https://docs.microsoft.com/en-us/azure/active-directory/devices/overview

NEW QUESTION 47
- (Topic 5)
You have an Azure Kubernetes Service (AKS) cluster named AKS1. You need to configure cluster autoscaler for AKS1.
Which two tools should you use? Each correct answer presents a complete solution, NOTE: Each correct selection is worth one point

A. the set-AzAKs cmdlet
B. the Azure portal
C. The az aks command
D. the kubect1 command
E. the set Azure cmdlet

Answer: BC

Explanation:
AKS clusters can scale in one of two ways: - The cluster autoscaler watches for pods that can't be scheduled on nodes because of resource constraints. The cluster then automatically increases the number of nodes. - The horizontal pod autoscaler uses the Metrics Server in a Kubernetes cluster to monitor the resource demand of pods. If an application needs more resources, the number of pods is automatically increased to meet the demand. Reference:
https://docs.microsoft.com/en-us/azure/aks/cluster-autoscaler

NEW QUESTION 50
HOTSPOT - (Topic 5)
You have an Azure App Service plan named ASP1. CPU usage for ASP1 is 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.
Answer Area

The average CPU percentage is calculated **[answer choice]** per day.
- once
- four times
- six times
- 24 times

ASP1 must be **[answer choice]** to optimize CPU usage.
- scaled up
- scaled down
- scaled out

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? The average CPU percentage is calculated 24 times per day. This is because the exhibit shows the CPU percentage for ASP1 in a 24-hour period, with one data point for each hour. Therefore, the average CPU percentage is calculated once per hour, or 24 times per day1.
? ASP1 must be scaled out to optimize CPU usage. This is because the exhibit shows that the CPU percentage for ASP1 is consistently above 80%, which indicates that the app service plan is under high load and needs more instances to handle the traffic. Scaling out means adding more instances to an app service plan, which can improve the performance and availability of the apps hosted on it2. Scaling up means changing the pricing tier of an app service plan, which can increase the resources available for each instance, but not necessarily reduce the CPU usage3.

NEW QUESTION 52
- (Topic 5)
You have an Azure AD tenant that contains the groups shown In the following table.

Name	Type	Security
Group1	Security	Enabled
Group2	Mail-enabled security	Enabled
Group3	Microsoft 365	Enabled
Group4	Microsoft 365	Disabled

You purchase Azure Active Directory Premium P2 licenses. To which groups can you assign a license?

A. Group 1 only
B. Group1 and Group3 only
C. Group3 and Group4 only
D. Group1, Group2, and Group3 only
E. Group1, Group2, Group3, and Group4

Answer: B

Explanation:
To assign a license to a group, the group must be a security group, not an Office 365 group or a mail-enabled security group1. According to the image, Group1 and Group3 are security groups, while Group2 and Group4 are Office 365 groups. Therefore, only Group1 and Group3 can be assigned a license.
To assign a license to a group, you need to follow these steps2:
? Sign in to the Azure portal with a license administrator account.
? Go to Azure Active Directory > Licenses and select the product license that you want to assign to groups.
? Select Assign at the top of the page and then select Users and groups.
? Search for and select the group that you want to assign the license to and then select OK.
? Select Assignment options to enable or disable specific services within the product license and then select OK.
? Select Assign at the bottom of the page to complete the assignment.

NEW QUESTION 54
- (Topic 5)
You have an Azure subscription that contains multiple virtual machines in the West US Azure region.
You need to use Traffic Analytics in Azure Network Watcher to monitor virtual machine traffic.
Which two resources should you create? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. a Data Collection Rule (OCR) in Azure Monitor
B. a Log Analytics workspace
C. an Azure Monitor workbook
D. a storage account
E. a Microsoft Sentinel workspace

Answer: BD

Explanation:
To use Traffic Analytics in Azure Network Watcher, you need to create a Log Analytics workspace and a storage account. A Log Analytics workspace is a cloud-based repository that collects and stores data from various sources, such as NSG flow logs. A storage account is a container that provides a unique namespace to store and access your data objects in Azure Storage. You need to enable NSG flow logs and configure them to send data to both the Log Analytics workspace and the storage account. Traffic Analytics analyzes the NSG flow logs and provides insights into traffic flow in your Azure cloud. References:
? Traffic analytics - Azure Network Watcher | Microsoft Learn
? Traffic analytics FAQ - Azure Network Watcher | Microsoft Learn

NEW QUESTION 57
- (Topic 5)
You have an Azure subscription that contains a storage account. The account stores website data.
You need to ensure that inbound user traffic uses the Microsoft point-of-presence (POP) closest to the user's location.
What should you configure?

A. load balancing
B. private endpoints
C. Azure Firewall rules
D. Routing preference

Answer: D

Explanation:
Routing preference is a feature that allows you to configure how network traffic is routed to your storage account from clients over the internet. By default, traffic from the internet is routed to the public endpoint of your storage account over the Microsoft global network, which is optimized for low-latency path selection and high reliability. Both inbound and outbound traffic are routed through the point of presence (POP) that is closest to the client. This ensures that traffic to and from your storage account traverses over the Microsoft global network for the bulk of its path, maximizing network performance. You can also change the routing preference to use internet routing, which minimizes the traversal of your traffic over the Microsoft global network, handing it off to the transit ISP at the earliest opportunity. This lowers networking costs, but may compromise network performance. Therefore, to ensure that inbound user traffic uses the Microsoft POP closest to the user's location, you should configure routing preference to use the Microsoft global network as the default routing option for your storage account.
References:
? Network routing preference for Azure Storage
? Configure network routing preference for Azure Storage

NEW QUESTION 62
- (Topic 5)
You have an Azure subscription named Subscription1 that is used be 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

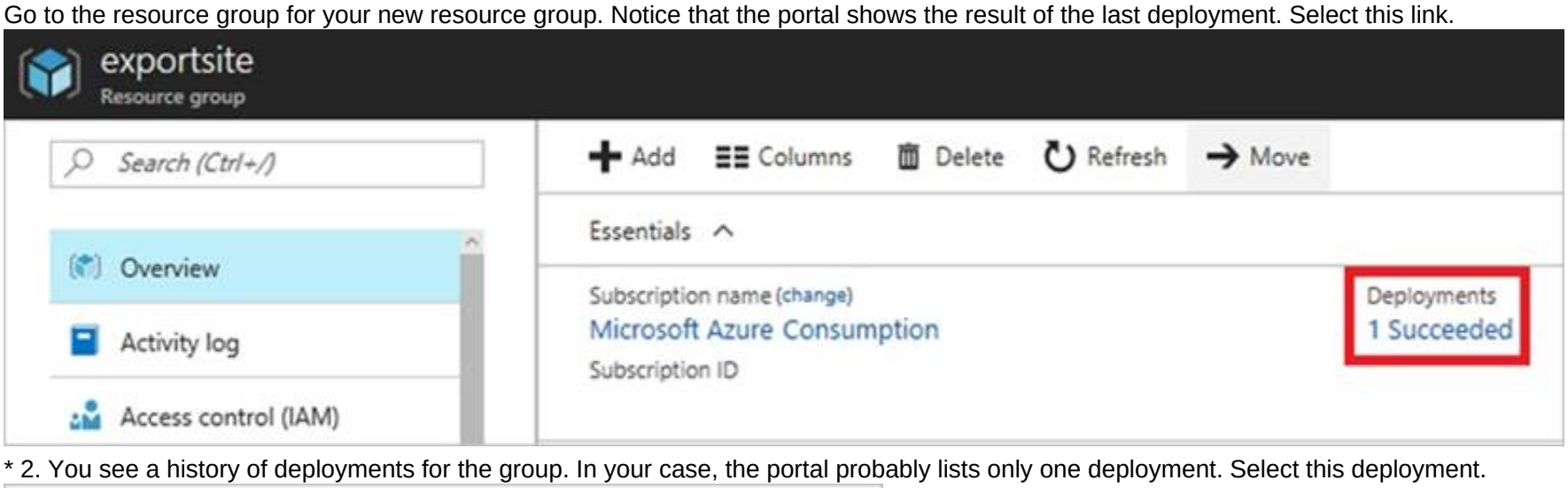
Another administrator deploys a virtual machine named VM1 and an Azure Storage account named Storage2 by using a single Azure Resource Manager template.
You need to view the template used for the deployment.

From which blade can you view the template that was used for the deployment?

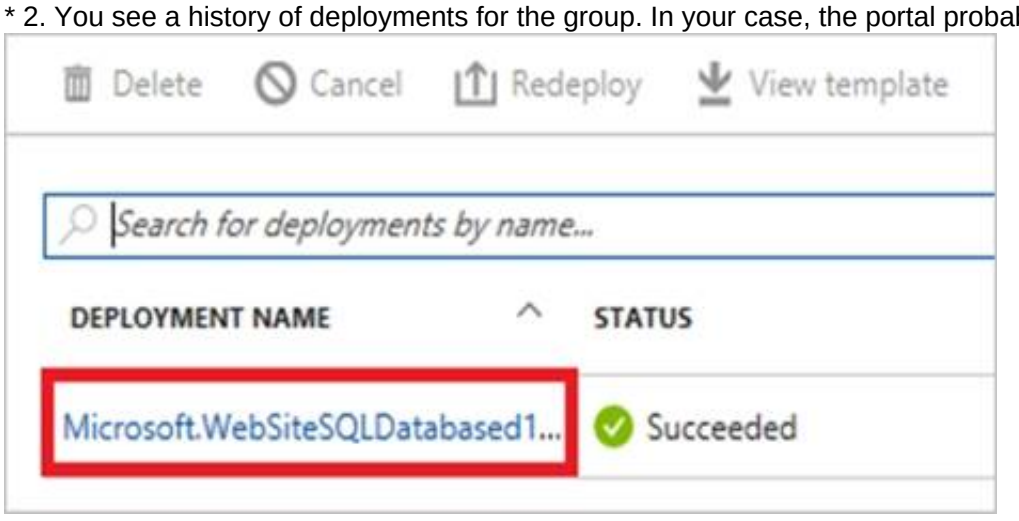
A. RG1
B. VM1
C. Storage1
D. Container1

Answer: A

Explanation:
* 1. View template from deployment history
Go to the resource group for your new resource group. Notice that the portal shows the result of the last deployment. Select this link.



* 2. You see a history of deployments for the group. In your case, the portal probably lists only one deployment. Select this deployment.



The portal displays a summary of the deployment. The summary includes the status of the deployment and its operations and the values that you provided for parameters. To see the template that you used for the deployment, select View template.

References: https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-export-template

NEW QUESTION 66
- (Topic 5)
You have an Azure subscription that contains a storage account named storageacct1234 and two users named User1 and User2.
You assign User1 the roles shown in the following exhibit.

Which two actions can User1 perform? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. View file shares in storageacct1234.
B. Upload blob data to storageacct1234.
C. Assign roles to User2 for storageacctl234.
D. View blob data in storageacctl234.
E. Modify the firewall of storageacct1234.

Answer: AC

NEW QUESTION 70

- (Topic 5)

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 virtual machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.
You receive a notification that VM1 will be affected by maintenance. You need to move VM1 to a different host immediately.
Solution: From the Overview blade, you move the virtual machine to a different subscription.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Moving the virtual machine to a different subscription does not change the host that the virtual machine runs on. It only changes the billing and management of the resources. To move the virtual machine to a different host, you need to redeploy it or use Azure Site Recovery. Then, References: [Move resources to new resource group or subscription] [Redeploy Windows VM to new Azure node] [Use Azure Site Recovery to migrate Azure VMs between Azure regions]

NEW QUESTION 73
- (Topic 5)
You have an Azure subscription that contains a web app named webapp1. You need to add a custom domain named www.contoso.com to webapp1. What should you do first?

A. Upload a certificate.
B. Add a connection string.
C. Stop webapp1.
D. Create a DNS record.

Answer: D

Explanation:
You can use either a CNAME record or an A record to map a custom DNS name to App Service. You should use CNAME records for all custom DNS names except root domains (for example, contoso.com). For root domains, use A records. Reference: https://docs.microsoft.com/en-us/Azure/app-service/app-service-web-tutorial-custom- domain

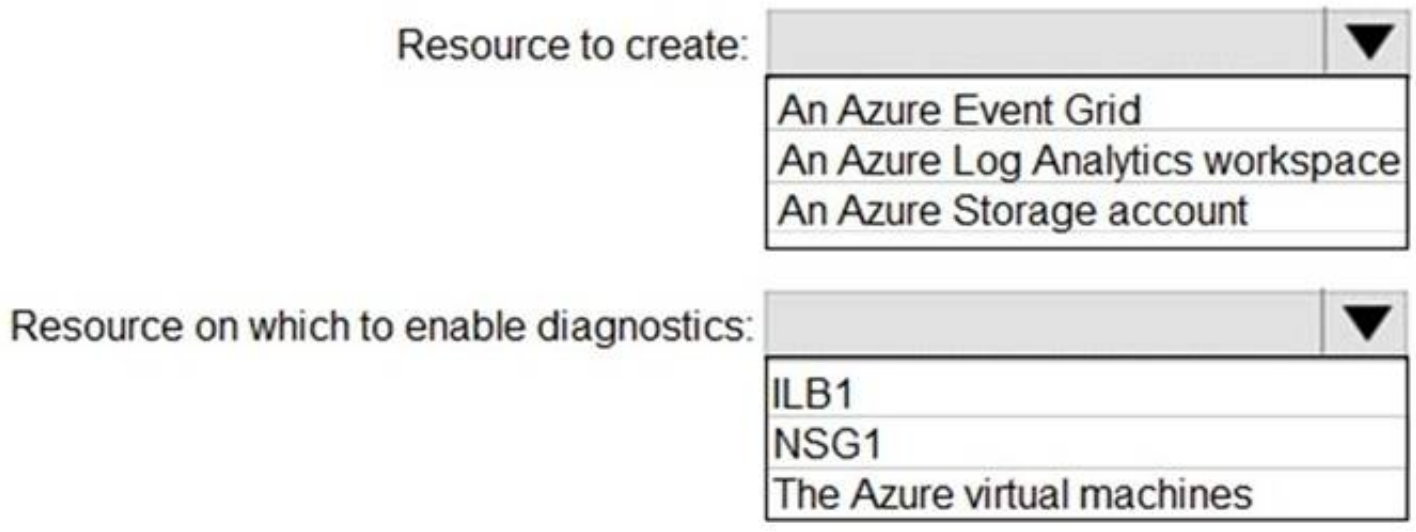
NEW QUESTION 77
- (Topic 5)
You have an Azure subscription that contains a storage account named storage1.
You plan to use conditions when assigning role-based access control (RABC) roles to storage1
Which storage1 services support conditions when assigning roles?

A. containers only
B. file shares only
C. tables only
D. queues only
E. containers and queues only
F. files shares and tables only

Answer: A

Explanation:
"Currently, conditions can be added to built-in or custom role assignments that have blob storage or queue storage data actions. " https://learn.microsoft.com/en-us/azure/role- based-access-control/conditions-overview#where-can-conditions-be-added

NEW QUESTION 81
HOTSPOT - (Topic 5)
You have an Azure virtual network named VNet1 that connects to your on-premises network by using a site-to-site VPN. VMet1 contains one subnet named Subnet1.
Subnet1 is associated to a network security group (NSG) named NSG1. Subnet1 contains a basic internal load balancer named ILB1. ILB1 has three Azure virtual machines in the backend pool.
You need to collect data about the IP addresses that connects to ILB1. You must be able to run interactive queries from the Azure portal against the collected data.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: An Azure Log Analytics workspace
In the Azure portal you can set up a Log Analytics workspace, which is a unique Log Analytics environment with its own data repository, data sources, and solutions.
Box 2: NSG1
NSG flow logs allow viewing information about ingress and egress IP traffic through a Network security group. Through this, the IP addresses that connect to the ILB can be monitored when the diagnostics are enabled on a Network Security Group.
We cannot enable diagnostics on an internal load balancer to check for the IP addresses. As for Internal LB, it is basic one. Basic can only connect to storage account. Also, Basic LB has only activity logs, which doesn't include the connectivity workflow. So, we need to use NSG to meet the mentioned requirements.

NEW QUESTION 86
- (Topic 5)
You have two subscriptions named Subscription1 and Subscription2. Each subscription is associated to a different Azure AD tenant.
Subscription1 contains a virtual network named VNet1. VNet1 contains an Azure virtual machine named VM1 and has an IP address space of 10.0.0.0/16.
Subscription2 contains a virtual network named VNet2. VNet2 contains an Azure virtual machine named VM2 and has an IP address space of 10.10.0.0/24.
You need to connect VNet1 to VNet2. What should you do first?

A. Move VM1 to Subscription2.
B. Modify the IP address space of VNet2.
C. Provision virtual network gateways.
D. Move VNet1 to Subscription2.

Answer: C

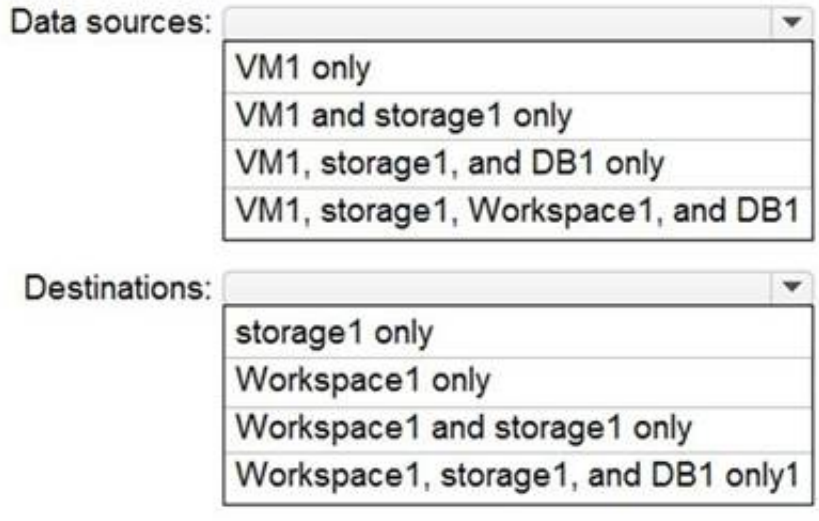
Explanation:
https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal

NEW QUESTION 89
HOTSPOT - (Topic 5)
You have an Azure subscription that contains the resources shown in the following table.

Name	Type
VM1	Virtual machine
storage1	Storage account
Workspace1	Log Analytics workspace
DB1	Azure SQL database

You plan to create a data collection rule named DCRI in Azure Monitor.
Which resources can you set as data sources in DCRI, and which resources can you set as destinations in DCRI? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Data Sources: VM1 only Destination: Workspace1 Only

NEW QUESTION 93
HOTSPOT - (Topic 5)

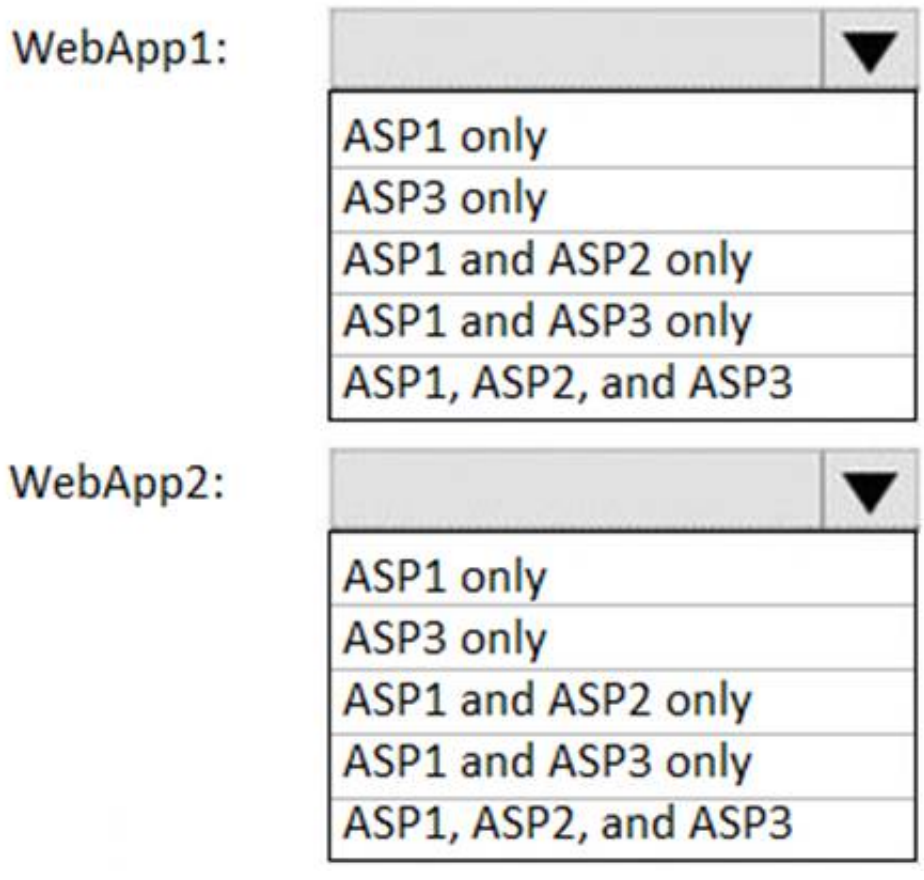
You have the App Service plans shown in the following table.

Name	Operating system	Location
ASP1	Windows	West US
ASP2	Windows	Central US
ASP3	Linux	West US

You plan to create the Azure web apps shown in the following table.

Name	Runtime stack	Location
WebApp1	.NET Core 3.0	West US
WebApp2	ASP.NET 4.7	West US

You need to identify which App Service plans can be used for the web apps.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: ASP1 ASP3
Asp1, ASP3: ASP.NET Core apps can be hosted both on Windows or Linux.
Not ASP2: The region in which your app runs is the region of the App Service plan it's in.
Box 2: ASP1
ASP.NET apps can be hosted on Windows only.

NEW QUESTION 96
HOTSPOT - (Topic 5)
You have an Azure subscription that contains an Azure Directory (Azure AD) tenant named contoso.com. The tenant is synced to the on-premises Active Directory domain. The domain contains the users shown in the following table.

Name	Role
SecAdmin1	Security administrator
BillAdmin1	Billing administrator
User1	Reports reader

You enable self-service password reset (SSPR) for all users and configure SSPR to have the following authentication methods:
? Number of methods required to reset: 2
? Methods available to users: Mobile phone, Security questions
? Number of questions required to register: 3
? Number of questions required to reset: 3
You select the following security questions:
? What is your favorite food?
? In what city was your first job?
? What was the name of your first pet?
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
SecAdmin1 must answer the following question if he wants to reset his password: In what city was your first job?	○	○
BillAdmin1 must answer the following question if he wants to reset his password: What is your favorite food?	○	○
User1 must answer the following question if he wants to reset his password: What was the name of your first pet?	○	○

Answer:

Answer Area

Statements	Yes	No
SecAdmin1 must answer the following question if he wants to reset his password: In what city was your first job?	○	○
BillAdmin1 must answer the following question if he wants to reset his password: What is your favorite food?	○	○
User1 must answer the following question if he wants to reset his password: What was the name of your first pet?	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
No, No, Yes
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept- authentication-security-questions

NEW QUESTION 100
- (Topic 5)
You have an Azure Active Directory (Azure AD) tenant named contoso.com.
You have a CSV file that contains the names and email addresses of 500 external users. You need to create a guest user account in contoso.com for each of the 500 external users.
Solution: You create a Power Shell script that runs the New-MgUser cmdlet for each user.
Does this meet the goal?

A. Yes

B. NO

Answer: B

Explanation:
The New-MgUser cmdlet is part of the Microsoft Graph PowerShell SDK, which is a module that allows you to interact with the Microsoft Graph API. The Microsoft Graph API is a service that provides access to data and insights across Microsoft 365, such as users, groups, mail, calendar, contacts, files, and more1.
The New-MgUser cmdlet can be used to create new users in your Azure AD tenant, but it has some limitations and requirements. For example, you need to have the Global Administrator or User Administrator role in your tenant, you need to authenticate with the Microsoft Graph API using a certificate or a client secret, and you need to specify the required parameters for the new user, such as userPrincipalName, accountEnabled, displayName, mailNickname, and passwordProfile2.
However, the New-MgUser cmdlet does not support creating guest user accounts in your Azure AD tenant. Guest user accounts are accounts that belong to external users from other organizations or domains. Guest user accounts have limited access and permissions in your tenant, and they are typically used for collaboration or sharing purposes3.
To create guest user accounts in your Azure AD tenant, you need to use a different cmdlet: New-AzureADMSInvitation. This cmdlet is part of the Azure AD PowerShell module, which is a module that allows you to manage your Azure AD resources and objects. The New- AzureADMSInvitation cmdlet can be used to create and send an invitation email to an external user, which contains a link to join your Azure AD tenant as a guest user. You can also specify some optional parameters for the invitation, such as the invited user display name, message info, redirect URL, or send invitation message.
Therefore, to meet the goal of creating guest user accounts for 500 external users from a CSV file, you need to use a PowerShell script that runs the New-AzureADMSInvitation cmdlet for each user, not the New-MgUser cmdlet.

NEW QUESTION 101
- (Topic 5)
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 manage a virtual network named VNet1 that is hosted in the West US Azure region. VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.
You need to inspect all the network traffic from VM1 to VM2 for a period of three hours. Solution: From Performance Monitor, you create a Data Collector Set (DCS).
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Correct answer is packet capture in Azure Network Watcher. https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-overview

NEW QUESTION 103
- (Topic 5)
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 virtual machine named VM1. VM1 was deployed by using a custom
Azure Resource Manager template named ARM1.json.
You receive a notification that VM1 will be affected by maintenance. You need to move VM1 to a different host immediately.
Solution: From the Update management blade, you click Enable. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 107
HOTSPOT - (Topic 5)
You have an Azure subscription that contains the public load balancers shown in the following table.

Name	SKU
LB1	Basic
LB2	Standard

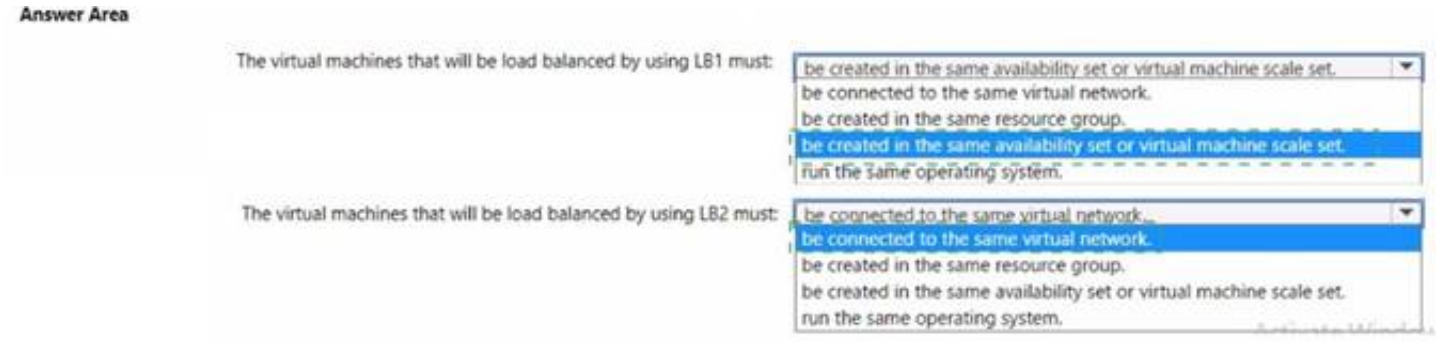
You plan to create six virtual machines and to load balance requests to the virtual machines. Each load balancer will load balance three virtual machines.
You need to create the virtual machines for the planned solution.
How should you create the virtual machines? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

The virtual machines that will be load balanced by using LB1 must: be created in the same availability set or virtual machine scale set.
- be connected to the same virtual network.
- be created in the same resource group.
- be created in the same availability set or virtual machine scale set.
- run the same operating system.

The virtual machines that will be load balanced by using LB2 must: be connected to the same virtual network.
- be connected to the same virtual network.
- be created in the same resource group.
- be created in the same availability set or virtual machine scale set.
- run the same operating system.

Answer:



A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/load-balancer/skus>

NEW QUESTION 112
DRAG DROP - (Topic 5)
You have an Azure subscription named Sub1 that contains two users named User1 and User2.
You need to assign role-based access control (RBAC) roles to User1 and User2. The users must be able to perform the following tasks in Sub1:
• User1 must view the data in any storage account.
• User2 must assign users the Contributor role for storage accounts. The solution must use the principle of least privilege.
Which RBAC role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? User1: You should assign the Reader and Data Access role to User1. This role grants read access to Azure resources and data, including the data in any storage account1. This role is suitable for User1's task of viewing the data in any storage account, and it follows the principle of least privilege by not granting any write or delete permissions.
? User2: You should assign the Storage Account Contributor role to User2. This role
grants full access to manage storage accounts and their data, including the ability to assign roles in Azure RBAC2. This role is suitable for User2's task of assigning users the Contributor role for storage accounts, and it follows the principle of least privilege by not granting access to other types of resources.

NEW QUESTION 117
HOTSPOT - (Topic 5)
You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Subnet	Subnet-associated network security group (NSG)	Peered with
VNet1	Subnet1	NSG1	VNet2
VNet2	Subnet2	NSG2	VNet1

The subscription contains the virtual machines shown in the following table.

Name	Connected to
VM1	Subnet1
VM2	Subnet2

The subscription contains the Azure App Service web apps shown in the following table.

Name	Description
WebApp1	Uses the Premium pricing tier and has virtual network integration with VNet1
WebApp2	Uses the Isolated pricing tier and is deployed to Subnet2

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
WebApp1 can communicate with VM2.	○	○
NSG1 controls inbound traffic to WebApp1.	○	○
WebApp2 can communicate with VM1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? WebApp1 can communicate with VM2. No, this is not correct. According to the tables, WebApp1 is integrated with VNet1, which has a peering connection with VNet2. However, VM2 is in VNet3, which is not peered with VNet1 or VNet2. Therefore, WebApp1 cannot communicate with VM2 across different virtual networks1.
? NSG1 controls inbound traffic to WebApp1. No, this is not correct. According to the tables, NSG1 is associated with Subnet1 in VNet1, which is integrated with WebApp1. However, network security groups only control outbound traffic from App Service apps to virtual networks, not inbound traffic to App Service apps from virtual networks2. Therefore, NSG1 does not control inbound traffic to WebApp1.
? WebApp2 can communicate with VM1. Yes, this is correct. According to the tables, WebApp2 is integrated with VNet3, which has a peering connection with VNet2. VM1 is in Subnet2 in VNet2, which has a network security group named NSG2 that allows inbound traffic from any source on port 803. Therefore, WebApp2 can communicate with VM1 on port 80 across peered virtual networks.

NEW QUESTION 119
- (Topic 5)
You have an Azure virtual machine named VM1 and an Azure key vault named Vault1. On VM1, you plan to configure Azure Disk Encryption to use a key encryption key (KEK) You need to prepare Vault! for Azure Disk Encryption.
Which two actions should you perform on Vault1? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Create a new key.
B. Select Azure Virtual machines for deployment
C. Configure a key rotation policy.
D. Create a new secret.
E. Select Azure Disk Encryption for volume encryption

Answer: AC

Explanation:
To prepare Vault1 for Azure Disk Encryption, you need to perform the following actions on Vault1:
? Create a new key. A key encryption key (KEK) is an encryption key that is used to encrypt the encryption secrets before they are stored in the key vault. You can create a new KEK by using the Azure CLI, the Azure PowerShell, or the Azure portal1. You can also import an existing KEK from another source, such as a hardware security module (HSM)2. The KEK must be a 2048-bit RSA key or a 256-bit AES key3.
? Select Azure Disk Encryption for volume encryption. This is an advanced access policy setting that enables Azure Disk Encryption to access the keys and secrets in the key vault. You can select this setting by using the Azure CLI, the Azure PowerShell, or the Azure portal4. You must also enable access to Microsoft Trusted Services if you have enabled the firewall on the key vault.

NEW QUESTION 124
- (Topic 5)
You have an Azure subscription that contains 20 virtual machines, a network security group (NSG) named NSG1, and two virtual networks named VNET1 and VNET2 that are peered.
You plan to deploy an Azure Bastion Basic SKU host named Bastion1 to VNET1. You need to configure NSG1 to allow inbound access from the internet to Bastion1.
Which port should you configure for the inbound security rule?

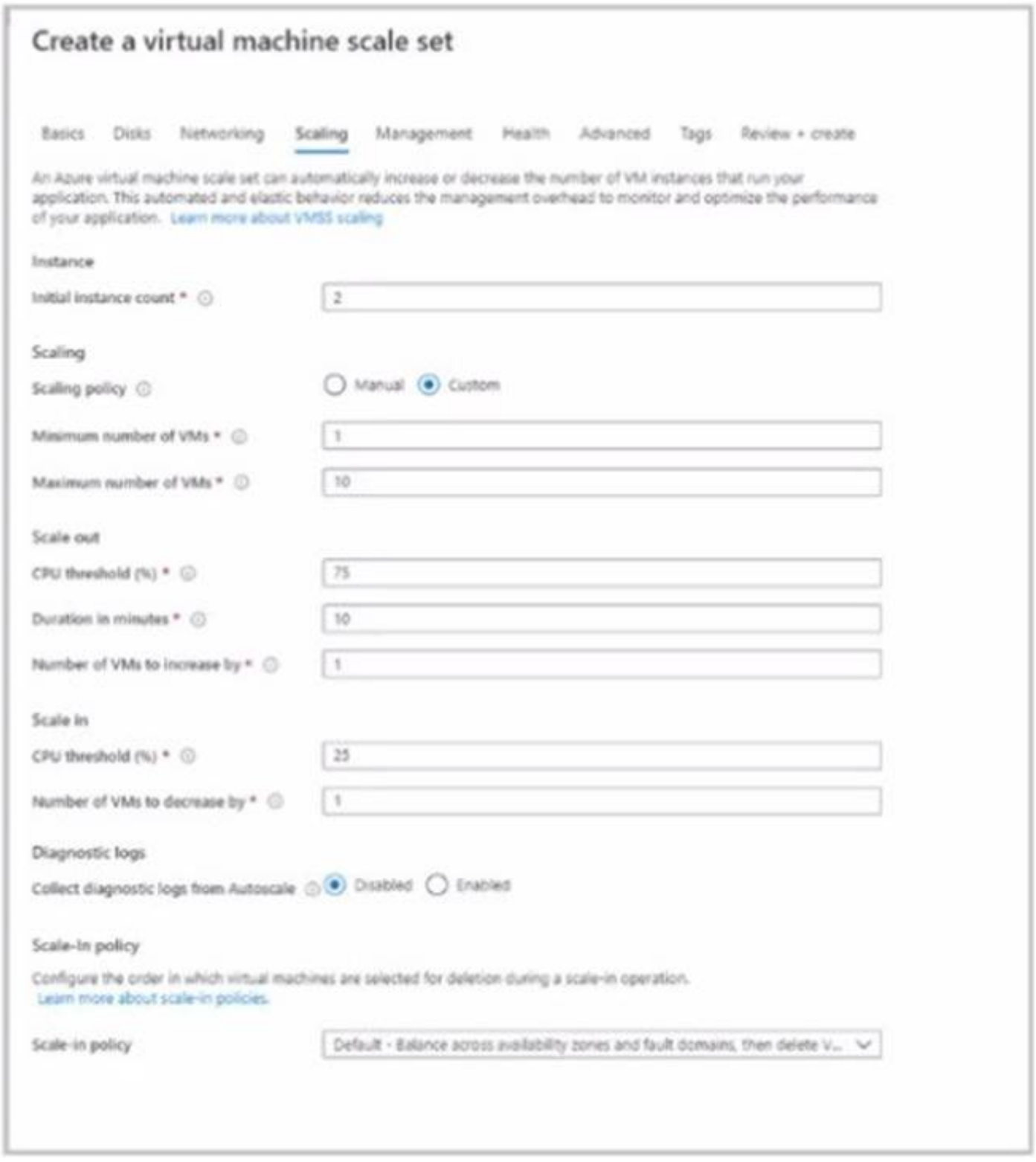
A. 22
B. 443
C. 3389
D. 8080

Answer: B

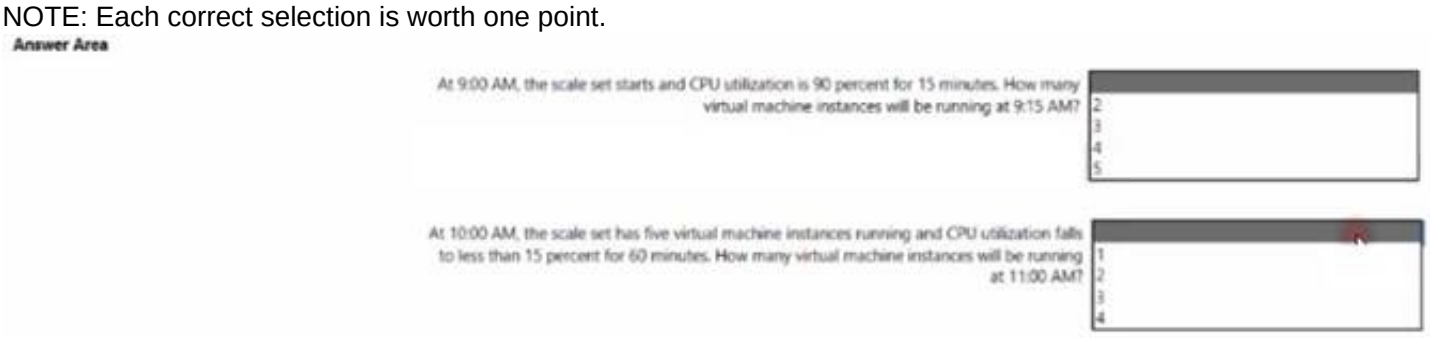
Explanation:
Azure Bastion is a service that provides secure and seamless RDP/SSH connectivity to virtual machines directly over TLS from the Azure portal or via native client. Azure Bastion uses an HTML5 based web client that is automatically streamed to your local device. Your RDP/SSH session is over TLS on port 443. This enables the traffic to traverse firewalls more securely. To allow inbound access from the internet to Bastion1, you need to configure NSG1 to allow port 443 for the inbound security rule. References:
? What is Azure Bastion?
? About Azure Bastion configuration settings

NEW QUESTION 129
HOTSPOT - (Topic 5)

You have an Azure subscription.
You deploy a virtual machine scale set that is configure as shown in the following exhibit.



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



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box-1 : 3
Initial starts 2 VM's 15 minutes have passed. at 10 minutes 1 VM was added we now have 3 VM's. Cool down is 5 Minutes before another 10 minute wait cycle starts so the answer is 3.
Box-2: 1
Initial 5 VM's 60 minutes Pass. 1 VM removed every 15 minute cycle. 10 minutes wait timer plus 5 minute cool down equals 15 minutes cycle. Four 15 minute cycles pass equaling 60 minutes removing 4 VM's. We have 1 VM left.
Default Scale in and Out Default Durations are 10 minutes with 5 minute cool down. The default scale set settings in Azure are:
-Minimum number of instances 1
-Maximum number of instances 10
-Scale out CPU threshold (%) 75
-Duration in minutes10
-Number of instances to increase by 1
-Scale in CPU threshold (%) 25
-Number of instances to decrease by -1
https://learn.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale- sets-autoscale-portal#create-a-rule-to-automatically-scale-in

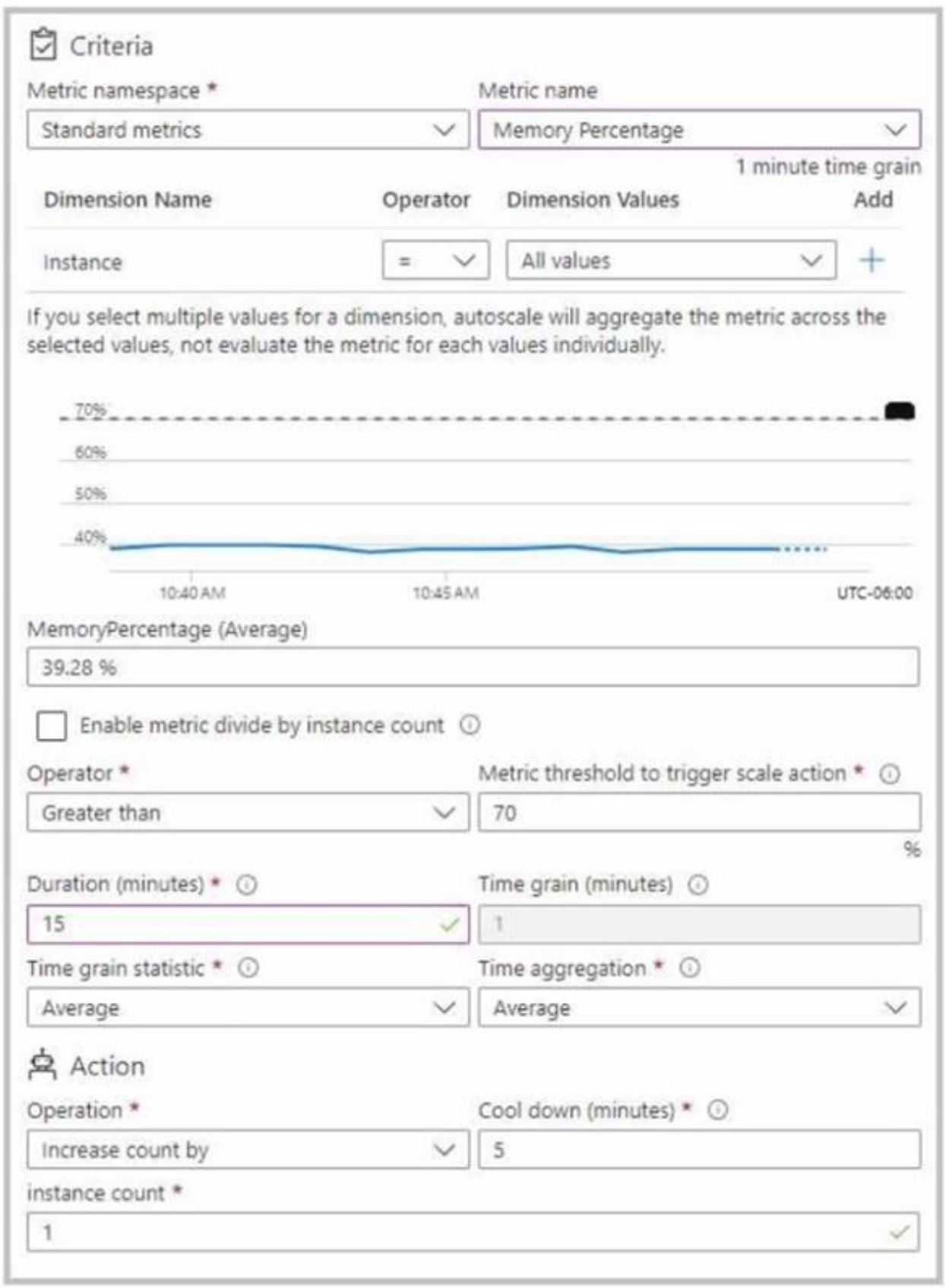
NEW QUESTION 130
- (Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.
Another administrator plans to create several network security groups (NSGs) in the subscription.
You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.
Solution: You configure a custom policy definition, and then you assign the policy to the subscription.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
A custom policy definition is a way to define your own rules for using Azure resources. You can use custom policies to enforce compliance, security, cost management, or organization-specific requirements. However, a custom policy definition alone is not enough to meet the goal of automatically blocking TCP port 8080 between the virtual networks. You also need to create a policy assignment that applies the custom policy definition to the scope of the subscription. A policy assignment is the link between a policy definition and an Azure resource. Without a policy assignment, the custom policy definition will not take effect. Therefore, the solution does not meet the goal.
References:
? Tutorial: Create a custom policy definition
? Create and manage policies to enforce compliance

NEW QUESTION 134
- (Topic 5)
You have an Azure App Service app named App1 that contains two running instances. You have an autoscale rule configured as shown in the following exhibit.



For the Instance limits scale condition setting, you set Maximum to 5. During a 30-minute period, App1 uses 80 percent of the available memory.
What is the maximum number of instances for App1 during the 30-minute period?

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 139
- (Topic 5)
You have an app named App1 that runs on an Azure web app named webapp1.
The developers at your company upload an update of App1 to a Git repository named GUI. Webapp1 has the deployment slots shown in the following table.

Name	Function
webapp1-prod	Production
webapp1-test	Staging

You need to ensure that the App1 update is tested before the update is made available to users.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Swap the slots
B. Deploy the App1 update to webapp1-prod, and then test the update
Stop webapp1-prod
6
D: Deploy the App1 update to webapp1-test, and then test the update
E. Stop webapp1-test

Answer: AD

Explanation:
https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots

NEW QUESTION 141
HOTSPOT - (Topic 5)
You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Operating system	Connects to
VM1	Windows Server 2019	Subnet1
VM2	Windows Server 2019	Subnet2

VM1 and VM2 use public IP addresses. From Windows Server 2019 on VM1 and VM2, you allow inbound Remote Desktop connections.
Subnet1 and Subnet2 are in a virtual network named VNET1.
The subscription contains two network security groups (NSGs) named NSG1 and NSG2. NSG1 uses only the default rules.
NSG2 uses the default rules and the following custom incoming rule;
• Priority: 100
• Name: Rule1
• Port: 3389
• Protocol: TCP
• Source: Any
• Destination: Any
• Action: Allow
NSG1 is associated to Subnet! NSG2 is associated to the network interface of VM2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
From the internet, you can connect to VM1 by using Remote Desktop.	○	○
From the internet, you can connect to VM2 by using Remote Desktop.	○	○
From VM1, you can connect to VM2 by using Remote Desktop.	○	○

Answer:

Answer Area

Statements	Yes	No
From the internet, you can connect to VM1 by using Remote Desktop.	○	○
From the internet, you can connect to VM2 by using Remote Desktop.	○	○
From VM1, you can connect to VM2 by using Remote Desktop.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
No: VM1 has default rules which denies any port open for inbound rules Yes: VM2 has custom rule allowing RDP port
Yes: VM1 and VM2 are in the same Vnet. by default, communication are allowed

NEW QUESTION 143
- (Topic 5)
You have a Microsoft 365 tenant and an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to grant three users named User1, User2, and User3 access to a temporary Microsoft SharePoint document library named Library1.
You need to create groups for the users. The solution must ensure that the groups are deleted automatically after 180 days.
Which two groups should you create? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. a Security group that uses the Assigned membership type
B. an Office 365 group that uses the Assigned membership type
C. an Office 365 group that uses the Dynamic User membership type
D. a Security group that uses the Dynamic User membership type
E. a Security group that uses the Dynamic Device membership type

Answer: BC

Explanation:
You can set expiration policy only for Office 365 groups in Azure Active Directory (Azure AD).
Note: With the increase in usage of Office 365 Groups, administrators and users need a way to clean up unused groups. Expiration policies can help remove inactive groups from the system and make things cleaner.
When a group expires, all of its associated services (the mailbox, Planner, SharePoint site, etc.) are also deleted.
You can set up a rule for dynamic membership on security groups or Office 365 groups.

NEW QUESTION 147
HOTSPOT - (Topic 5)
You have an Azure subscription that contains a storage account named storage1. The subscription is linked to an Azure Active Directory (Azure AD) tenant named contoso.com that syncs to an on-premises Active Directory domain.
The domain contains the security principals shown in the following table.

Name	Type
User1	User
Computer1	Computer

In Azure AD, you create a user named User2.
The storage1 account contains a file share named share1 and has the following configurations.

```
"kind": "StorageV2",
"properties": {
                "azureFilesIdentityBasedAuthentication": {
                    "directoryServiceOptions": "AD",
                    "activeDirectoryProperties": {
                        "domainName": "Contoso.com",
                        "netBiosDomainName": "Contoso.com",
                        "forestName": "Contoso.com",
-
                    }
}
```

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 assign the Storage File Data SMB Share Contributor role to User1 for share1.	○	○
You can assign the Storage File Data SMB Share Reader role to Computer1 for share1.	○	○
You can assign the Storage File Data SMB Share Elevated Contributor role to User2 for share1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
You can assign the Storage File Data SMB Share Contributor role to User1 for share1.	○	○
You can assign the Storage File Data SMB Share Reader role to Computer1 for share1.	○	○
You can assign the Storage File Data SMB Share Elevated Contributor role to User2 for share1.	○	○

NEW QUESTION 152
- (Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.
Another administrator plans to create several network security groups (NSGs) in the subscription.
You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.
Solution: From the Resource providers blade, you unregister the Microsoft.ClassicNetwork provider.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
No, this does not meet the goal. Unregistering the Microsoft.ClassicNetwork provider does not affect the creation of network security groups (NSGs) in the subscription. The Microsoft.ClassicNetwork provider is used for managing classic deployment model resources, such as virtual networks, network interfaces, and public IP addresses1. However, NSGs are only supported for Resource Manager deployment model resources2. Therefore, unregistering the Microsoft.ClassicNetwork provider will not automatically block TCP port 8080 between the virtual networks.
To meet the goal, you need to create a custom policy definition that enforces a default security rule for NSGs. A policy definition is a set of rules and actions that Azure performs when evaluating your resources3. You can use a policy definition to specify the required properties and values for NSGs, such as the direction, protocol, source, destination, and port of the security rule. You can then assign the policy definition to the subscription scope, so that it applies to all the resource groups and virtual networks in the subscription.

NEW QUESTION 154
- (Topic 5)
You have an Azure subscription named Subscription1.
You have 5 TB of data that you need to transfer to Subscription1. You plan to use an Azure Import/Export job.
What can you use as the destination of the imported data?

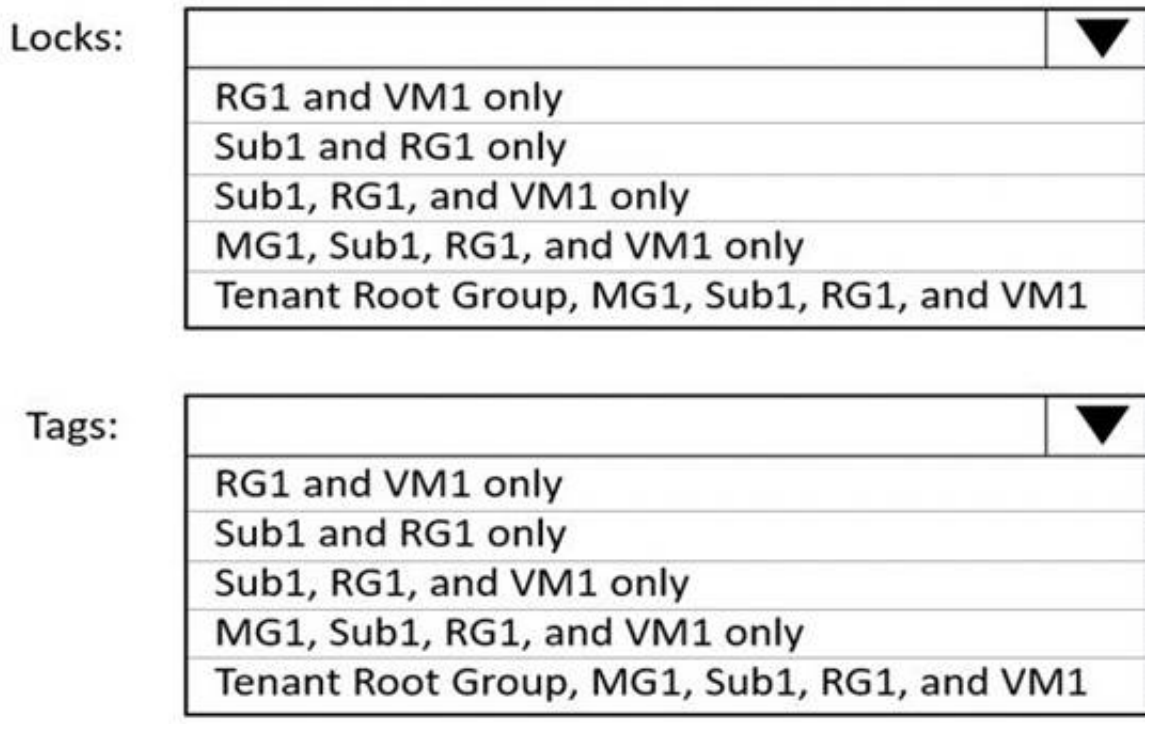
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter.
The maximum size of an Azure Files Resource of a file share is 5 TB. Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service

NEW QUESTION 159
HOTSPOT - (Topic 5)
You have the Azure resources shown on the following exhibit.

You plan to track resource usage and prevent the deletion of resources.
To which resources can you apply locks and tags? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Sub1, RG1, and VM1 only
You can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources.
Box 2: Sub1, RG1, and VM1 only
You apply tags to your Azure resources, resource groups, and subscriptions.

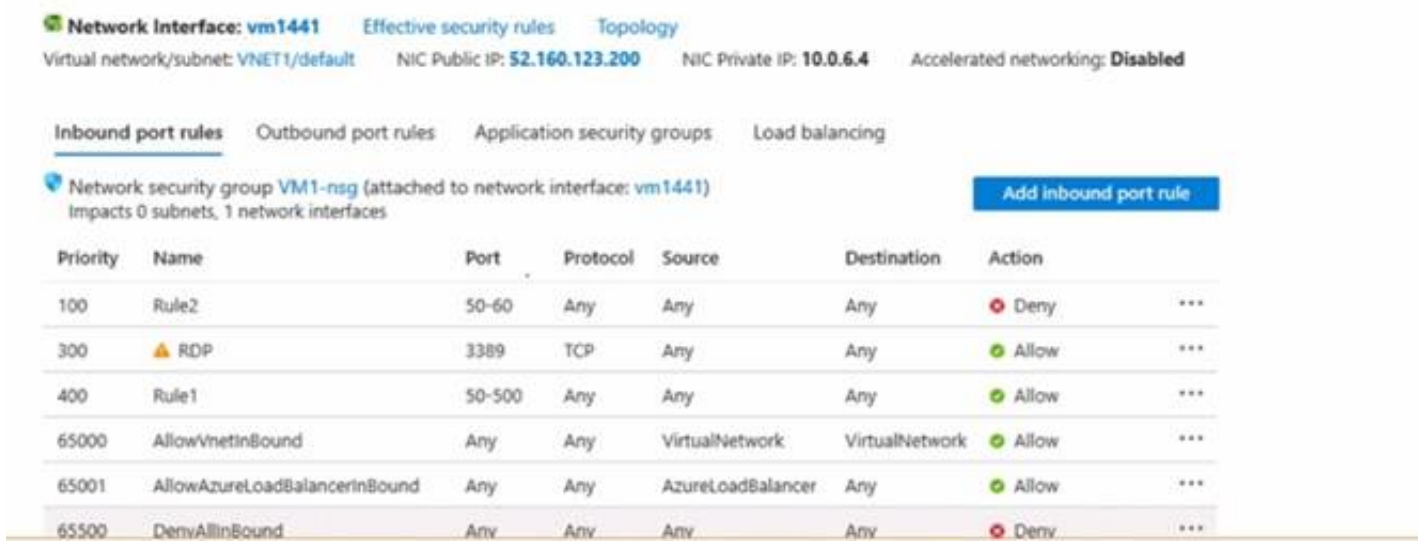
NEW QUESTION 163
- (Topic 5)
You are configuring Azure AD authentication for an Azure Storage account named storage1.
You need to ensure that the members of a group named Group1 can upload files by using the Azure portal. The solution must use the principle of least privilege.
Which two roles should you assign to Group1? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Storage Blob Data Contributor
B. Reader
C. Storage Blob Data Reader
D. Contributor
E. Storage Account Contributor

Answer: AB

Explanation:
To ensure that the members of Group1 can upload files by using the Azure portal, they need to have both data access and management access to the storage account. Data access refers to the ability to read, write, or delete blob data in the storage account. Management access refers to the ability to view the storage account resources in the Azure portal, but not modify them. The Azure role-based access control (Azure RBAC) system provides built-in roles that encompass common sets of permissions for data access and management access. The Storage Blob Data Contributor role grants read, write, and delete access to blob data in the storage account. The Reader role grants view access to the storage account resources in the Azure portal. Therefore, by assigning both roles to Group1, the members of the group can upload files by using the Azure portal. This solution also follows the principle of least privilege, as the group members are only granted the minimum permissions required to perform the task. References:
? Assign an Azure role for access to blob data
? Data access from the Azure portal

NEW QUESTION 166
HOTSPOT - (Topic 5)
You have an Azure subscription named Subscription1. Subscription1 contains a virtual machine named VM1.
You install and configure a web server and a DNS server on VM1.
VM1 has the effective network security rules 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.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed. https://docs.microsoft.com/en-us/azure/virtual-network/network-security- groups-overview

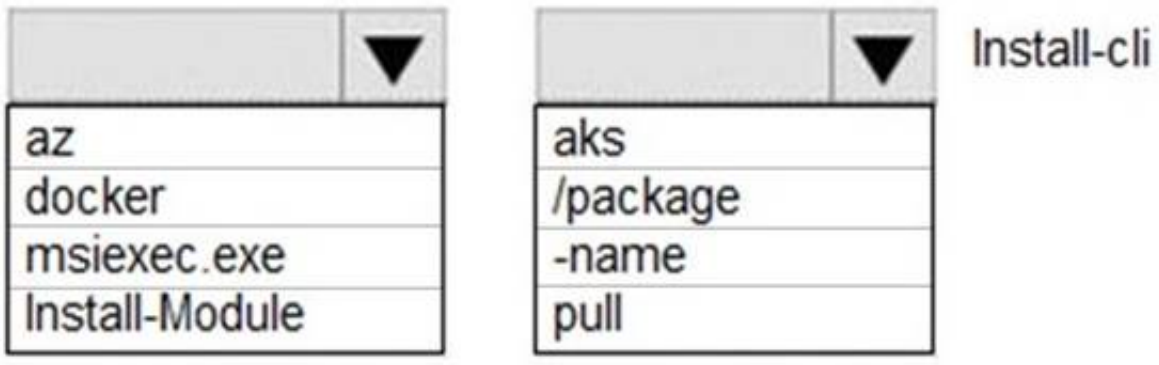
NEW QUESTION 167
- (Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups.
Another administrator plans to create several network security groups (NSGs) in the subscription.
You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks.
Solution: You create a resource lock, and then you assign the lock to the subscription.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
No, this does not meet the goal. Creating a resource lock and assigning it to the subscription is not enough to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks. This is because a resource lock does not affect the configuration or functionality of a resource, but only prevents it from being deleted or modified1. A resource lock does not apply any security rules to an NSG or a virtual network.
To meet the goal, you need to create a custom policy definition that enforces a default security rule for NSGs. A policy definition is a set of rules and actions that Azure performs when evaluating your resources2. You can use a policy definition to specify the required properties and values for NSGs, such as the direction, protocol, source, destination, and port of the security rule. You can then assign the policy definition to the subscription scope, so that it applies to all the resource groups and virtual networks in the subscription.

NEW QUESTION 170
HOTSPOT - (Topic 5)
You have an Azure Kubernetes Service (AKS) cluster named AKS1 and a computer named Computer1 that runs Windows 10. Computer1 that has the Azure CLI installed.
You need to install the kubectl client on Computer1.
Which command should you run? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
To install kubectl locally, use the az aks install-cli command: az aks install-cli

NEW QUESTION 172
- (Topic 5)

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 need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.
Solution: You assign the Owner role at the subscription level to Admin1. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The Owner role is a very high-level role that grants full access to manage all resources in the scope, including the ability to assign roles to other users. This role does not follow the principle of least privilege, which means that you should only grant the minimum level of access required to accomplish the goal.
To enable Traffic Analytics for an Azure subscription, you need to have a role that grants you the following permissions at the subscription level:
? Microsoft.Network/applicationGateways/read
? Microsoft.Network/connections/read
? Microsoft.Network/loadBalancers/read
? Microsoft.Network/localNetworkGateways/read
? Microsoft.Network/networkInterfaces/read
? Microsoft.Network/networkSecurityGroups/read
? Microsoft.Network/publicIPAddresses/read
? Microsoft.Network/routeTables/read
? Microsoft.Network/virtualNetworkGateways/read
? Microsoft.Network/virtualNetworks/read
? Microsoft.OperationalInsights/workspaces/*
Some of the built-in roles that have these permissions are Owner, Contributor, or Network Contributor1. However, these roles also grant other permissions that may not be necessary or desirable for enabling Traffic Analytics. Therefore, the best practice is to use the principle of least privilege and create a custom role that only has the required permissions for enabling Traffic Analytics2.
Therefore, to meet the goal of ensuring that an Azure AD user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription, you should create a custom role with the required permissions and assign it to Admin1 at the subscription level.

NEW QUESTION 173
HOTSPOT - (Topic 5)
You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Location	IP address space	Subnet
VNet1	East US	10.1.128.0/23	Subnet1
VNet2	East US	192.168.0.0/16	Subnet21, Subnet22
VNet3	East US	172.16.0.0/16	Subnet3

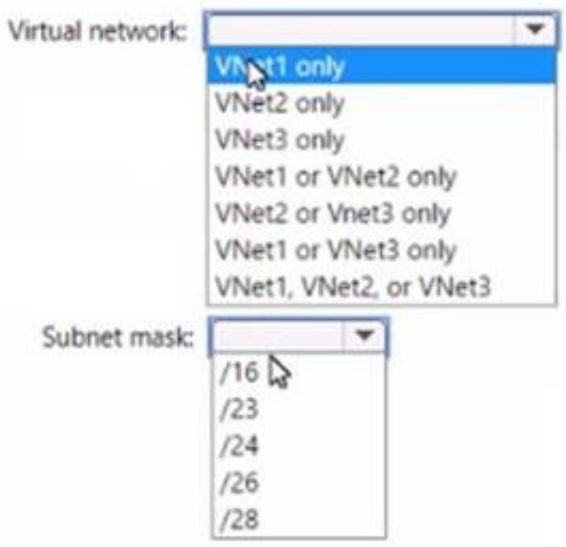
The subnets have the IP address spaces shown in the following table.

Name	IP address space
Subnet1	10.1.128.0/24
Subnet21	192.168.0.0/17
Subnet22	192.168.128.0/17
Subnet3	172.16.1.0/24

You plan to create a container app named contapp1 in the East US Azure region.

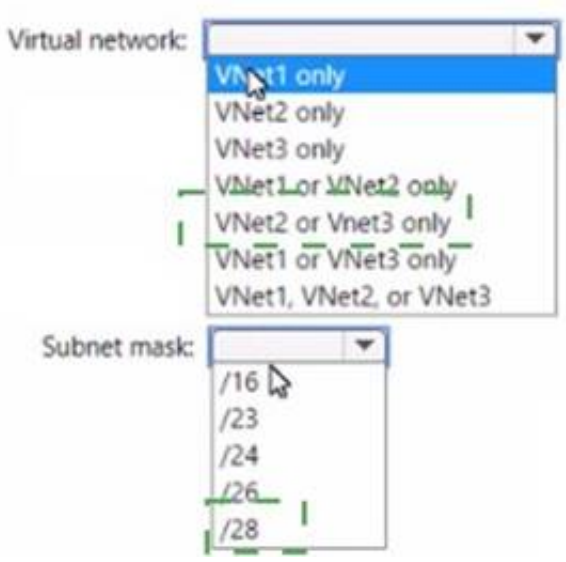
You need to create a container app environment named con-env1 that meets the following requirements:
• Uses its own virtual network.
• Uses its own subnet.
• Is connected to the smallest possible subnet.
To which virtual networks can you connect con-env1, and which subnet mask should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Virtual Network: You can connect con-env1 to VNet2 and VNet3 only. This is because VNet1 is in a different region than the container app, which is East US. According to the web search results, you can only connect a container app environment to a virtual network that is in the same region as the container app1. Therefore, VNet1 is not a valid option. VNet2 and VNet3 are both in the same region as the container app, and they have enough available IP addresses to support a container app environment.
? Subnet mask: You should use /28 as the subnet mask for con-env1. This is
because /28 is the smallest possible subnet mask that can accommodate a container app environment. According to the web search results, a container app environment requires a minimum of 16 IP addresses in a subnet2. A /28 subnet mask provides 16 IP addresses, while a /26 subnet mask provides 64 IP addresses, a /24 subnet mask provides 256 IP addresses, a /23 subnet mask provides 512 IP addresses, and a /16 subnet mask provides 65,536 IP addresses. Therefore, /28 is the most efficient choice for minimizing the subnet size.

NEW QUESTION 177
- (Topic 5)
You have an Azure subscription that contains the virtual machines shown in the following table.
javascript:void(0)

Name	Public IP SKU	Connected to	Status
VM1	*None*	VNET1/Subnet1	Stopped (deallocated)
VM2	Basic	VNET1/Subnet2	Running

You deploy a load balancer that has the following configurations:
• Name: LB1
• Type internal
• SKU: Standard
• Virtual network VNET1
You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.
Solution: You create a Basic SKU public IP address, associate the address to the network interface of VM1, and then start VM1.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
You can only attach virtual machines that are in the same location and on the same virtual network as the LB. Virtual machines must have a standard SKU public IP or no public IP.
The LB needs to be a standard SKU to accept individual VMs outside an availability set or vmss. VMs do not need to have public IPs but if they do have them they have to be standard SKU. Vms can only be from a single network. When they don't have a public IP they are assigned an ephemeral IP.
Also, when adding them to a backend pool, it doesn't matter in which status are the VMs. Note: Load balancer and the public IP address SKU must match when you use them with public IP addresses.

NEW QUESTION 180
- (Topic 5)
You have an app named App1 that runs on two Azure virtual machines named VM1 and VM2.
You plan to implement an Azure Availability Set for Appl. The solution must ensure that App1 is available during planned maintenance of the hardware hosting VM1 and VM2.
What should you include in the Availability Set?

A. one update domain
B. two update domains
C. one fault domain
D. two fault domains

Answer: B

NEW QUESTION 181
- (Topic 5)
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 app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.
The effective network security configurations for VM2 are shown in the following exhibit.

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail. You verify that the Load Balancer rules are configured correctly.
You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.
Solution: You create an inbound security rule that denies all traffic from the 131.107.100.50 source and has a cost of 64999.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 183
DRAG DROP - (Topic 5)
You have an Azure subscription that contains virtual machine named VM1.
You need to back up VM. The solution must ensure that backups are stored across three availability zones in the primary region.
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
According to 1, Availability Zones are unique physical locations within an Azure region that provide high availability and disaster recovery for your virtual machines.
To back up your VM across three availability zones in the primary region, you need to perform the following actions in sequence:
? Create a Recovery Services vault2 that will store your backups and enable geo-
redundancy for cross-region protection.
? For VM1, create a backup policy and configure the backup2 to use the Recovery Services vault as the backup destination.
? Configure a replication policy1 that will replicate your VM1 to another availability zone in the same region.

NEW QUESTION 184
- (Topic 5)
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.
You have a CSV file that contains the names and email addresses of 500 external users. You need to create a guest user account in contoso.com for each of the 500 external users.
Solution: From Azure AD in the Azure portal, you use the Bulk create user operation. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite?source=recommendations

NEW QUESTION 187
- (Topic 5)
You have an Azure subscription. The subscription contains a storage account named storage1 that has the lifecycle management rules shown in the following table.

Name	If base blobs were last modified more than (days)	Then
Rule1	5 days	Move to cool storage
Rule2	5 days	Delete the blob
Rule3	5 days	Move to archive storage

On June 1, you store a blob named File1 in the Hot access tier of storage1. What is the state of File1 on June 7?

A. stored in the Archive access tier
B. stored in the Hot access tier
C. stored in the Cool access tier
D. deleted

Answer: D

Explanation:
If you define more than one action on the same blob, lifecycle management applies the least expensive action to the blob. For example, action delete is cheaper than action tierToArchive. Action tierToArchive is cheaper than action tierToCool. https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview

NEW QUESTION 190
- (Topic 5)
You have two Azure virtual networks named VNet1 and VNet2. VNet1 contains an Azure virtual machine named VM1. VNet2 contains an Azure virtual machine named VM2.
VM1 hosts a frontend application that connects to VM2 to retrieve data.
Users report that the frontend application is slower than usual.
You need to view the average round-trip time (RTT) of the packets from VM1 to VM2. Which Azure Network Watcher feature should you use?

A. NSG flow logs
B. Connection troubleshoot
C. IP flow verify
D. Connection monitor

Answer: D

Explanation:
https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview#monitoring
The connection monitor capability monitors communication at a regular interval and informs you of reachability, latency, and network topology changes between the VM and the endpoint.
Connection monitor also provides the minimum, average, and maximum latency observed over time. After learning the latency for a connection, you may find that you can decrease the latency by moving your Azure resources to different Azure regions.

NEW QUESTION 192
- (Topic 5)
You have an Azure subscription that contains a storage account named account1.
You plan to upload the disk files of a virtual machine to account! from your on-premises network. The on-premises network uses a public IP address space of

131.107.1.0/24.
You plan to use the disk files to provision an Azure virtual machine named VM1. VM1 will be attached to a virtual network named VNet1. VNet1 uses an IP address space of 192.168.0.0/24.
You need to configure account1 to meet the following requirements:
• Ensure that you can upload the disk files to account1.
• Ensure that you can attach the disks to VM1.
• Prevent all other access to account1.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. From the Networking blade of account1, select Selected networks
B. From the Service endpoints blade of VNet1, add a service endpoint.
C. From the Networking blade of account11, add the 131.107.1.0/24 IP address range.
D. From the Networking blade of account1. select Allow trusted Microsoft services to access this storage account
E. From the Networking blade of account1, add VNet1.

Answer: AE

Explanation:
To restrict access to account1, you need to enable the firewall and virtual network settings on the storage account. This allows you to specify which networks can access the storage account. By selecting Selected networks, you can block all access from the public internet and only allow access from the specified networks. By adding VNet1, you can allow access from the virtual network that contains VM1. You do not need to add the on-premises IP address range or enable the service endpoint option, as these are not required for uploading the disk files to the storage account. You do not need to allow trusted Microsoft services, as this is not relevant for the scenario. Then, References: [Configure Azure Storage firewalls and virtual networks] [Upload a generalized VHD to Azure]

NEW QUESTION 194
HOTSPOT - (Topic 5)
You plan to deploy the following Azure Resource Manager (ARM) template.

```
{
  "$schema":"https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion":"1.0.0.0",
  "parameters":{},
  "variables":{
    "vnetId":"[resourceId('Microsoft.Network/virtualNetworks/', 'VNET1')]",
    "lbId":"[resourceId('Microsoft.Network/loadBalancers/', 'LB1')]",
    "sku":"Standard",
    "netname":"APP1"
  },
  "resources":[
    {
      "apiVersion":"2017-08-01",
      "type":"Microsoft.Network/loadBalancers",
      "name":"LB1",
      "location":"EastUS",
      "sku":{
        "name":"[variables('sku')]"
      },
      "properties":{
        "frontendIPConfigurations":[
          {
            "name":"[variables('netname')]",
  }
],
"loadBalancingRules":[
    properties :{
      "frontendIPConfiguration":{
  "id":"[concat(variables('lbId'),'/frontendIPConfigurations/', variables('netname'))]"
},
"backendAddressPool":{
  "id":"[concat(variables('lbId'), '/backendAddressPools/',variables('netname'),'-Servers')]"
},
"probe":{
  "id":"[concat(variables('lbId'), '/probes/probe')]"

          },
          "backendPort":8080,
          "protocol":"Tcp",
          "frontendPort":80,
          "enableFloatingIP":false,
          "idleTimeoutInMinutes":4,
          "loadDistribution":"SourceIPProtocol"
        }
      }
    ],
    "probes":[
      {
        "name":"probe",
        "properties":{
          "protocol":"Tcp",
          "port":8080,
          "intervalInSeconds":15,
          "numberOfProbes":2
        }
      }
```

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

Statements	Yes	No
LB1 will be connected to a subnet named VNET1/netname.	○	○
LB1 can be deployed only to the resource group that contains VNET1.	○	○
The value of the sku variable can be provided as a parameter when the template is deployed	○	○

Answer:

Statements	Yes	No
LB1 will be connected to a subnet named VNET1/netname.	○	○
LB1 can be deployed only to the resource group that contains VNET1.	○	○
The value of the sku variable can be provided as a parameter when the template is deployed	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? LB1 will be connected to a subnet named LB1 in VNET1. Yes, this is correct. The template specifies that the load balancer resource named LB1 has a property called frontendIPConfigurations, which defines the subnet where the load balancer is located. The value of this property is a reference to the resource ID of the subnet named LB1 in VNET1. You can see this reference in line 38 of the template1.
? LB1 can be deployed only to the resource group that contains VNET1. No, this is not correct. The template does not specify a resource group for the load balancer resource, which means it can be deployed to any resource group in the same subscription as VNET1. However, if you want to deploy the load balancer to a specific resource group, you can add a property called resourceGroup to the reference of the subnet in line 382.
? The value of the sku variable can be provided as a parameter when the template is deployed. No, this is not correct. The template defines the sku variable as a constant value of “Standard” in line 9. This means that the value cannot be changed or overridden by a parameter when the template is deployed. If you want to make the sku value configurable, you need to change the variable definition to a parameter definition, and use the parameter reference instead of the variable reference in line 363.

NEW QUESTION 198
HOTSPOT - (Topic 5)
You have an Azure subscription named Subscription1 that has a subscription ID of c276fc76-9cd4-44c9-99a7-4fd71546436e.
You need to create a custom RBAC role named CR1 that meets the following requirements:
? Can be assigned only to the resource groups in Subscription1
? Prevents the management of the access permissions for the resource groups
? Allows the viewing, creating, modifying, and deleting of resource within the resource groups
What should you specify in the assignable scopes and the permission elements of the definition of CR1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
"assignableScopes": [
    [ "/" | "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e" | "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e/resourceGroups" ]
],
"permissions": [
  {
    "actions": [
    "*"
    ],
    "additionalProperties" : {},
    "dataActions": [],
    "notActions" : [
      [ "Microsoft.Authorization/*" | "Microsft.Resources/*" | "Microsoft.Security/*" ]
    ],
    "notDataActions": []
  }
],
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: "/subscription/c276fc76-9cd4-44c9-99a7-4fd71546436e"
In the assignableScopes you need to mention the subscription ID where you want to implement the RBAC
Box 2: "Microsoft.Authorization/*" Microsoft.Authorization/* is used to Manage authorization
References:
https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftauthorization
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles
References:
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles
https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftresources

NEW QUESTION 203
- (Topic 5)
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 virtual machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.
You receive a notification that VM1 will be affected by maintenance. You need to move VM1 to a different host immediately.
Solution: From the Overview blade, you move the virtual machine to a different resource group.
Does this meet the goal?
A. Yes
B. No

Answer: B

Explanation:
Moving the virtual machine to a different resource group does not change the host that the virtual machine runs on. It only changes the logical grouping of the resources. To move the virtual machine to a different host, you need to redeploy it or use Azure Site Recovery. Then, References: [Move resources to new resource group or subscription] [Redeploy Windows VM to new Azure node] [Use Azure Site Recovery to migrate Azure VMs between Azure regions]

NEW QUESTION 206
- (Topic 5)
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Resource group	Location
RG1	Resource group	**Not applicable**	Central US
RG2	Resource group	**Not applicable**	West US
VMSS1	Virtual machine scale set	RG2	West US
Proximity1	Proximity placement group	RG1	West US
Proximity2	Proximity placement group	RG2	Central US
Proximity3	Proximity placement group	RG1	Central US

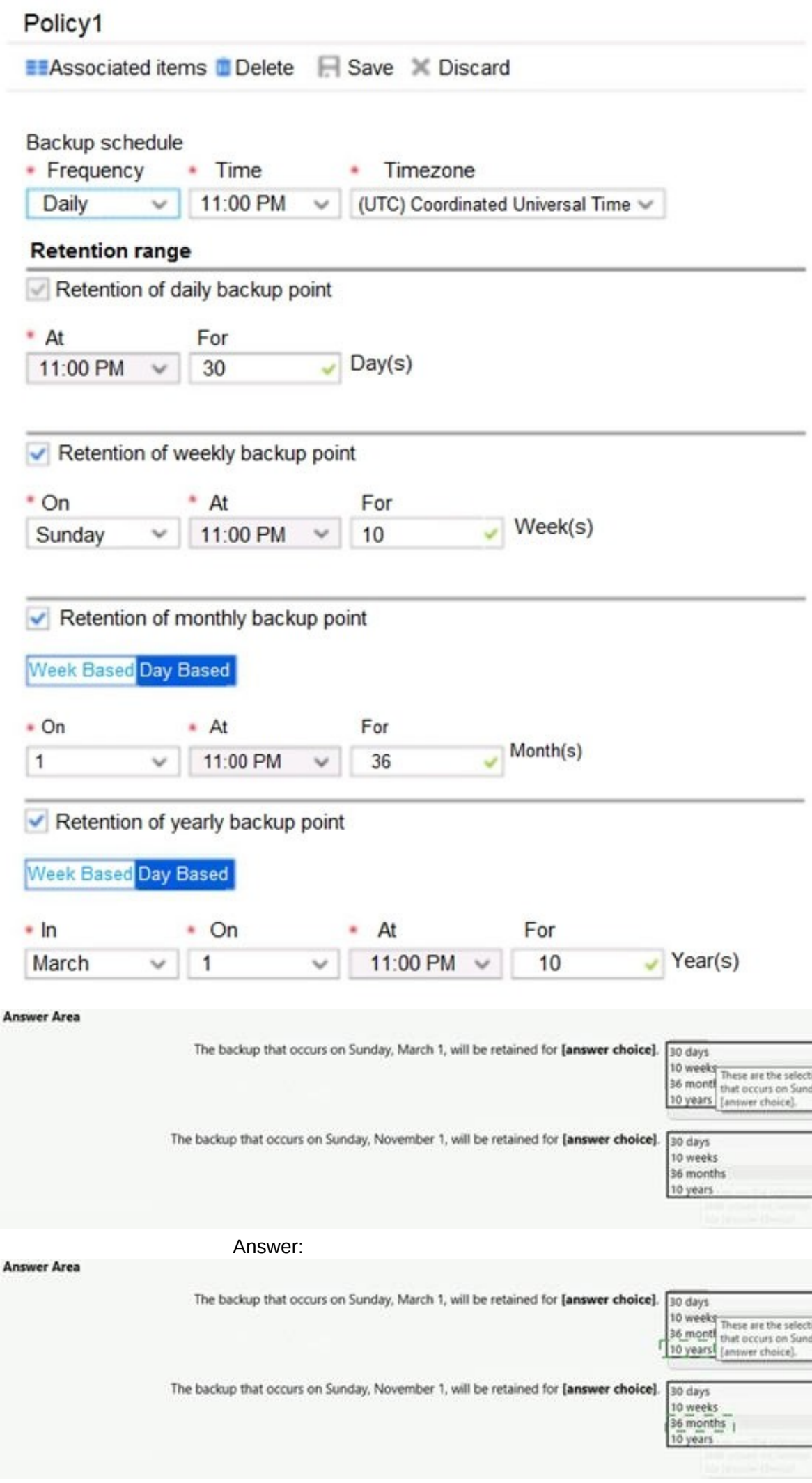
You need to configure a proximity placement group for VMSS1. Which proximity placement groups should you use?

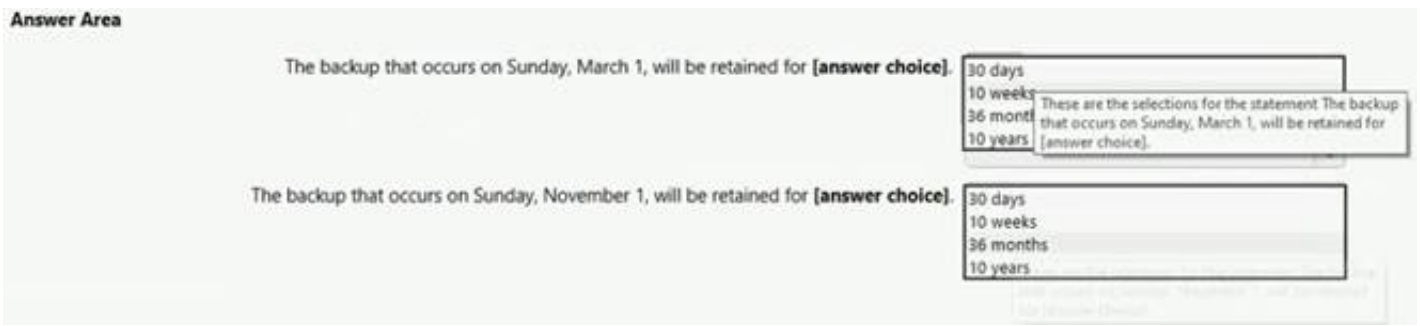
A. Proximity2 only
B. Proximity 1, Proximity2, and Proximity3
C. Proximity 1 and Proximity3 only
D. Proximity1 only

Answer: A

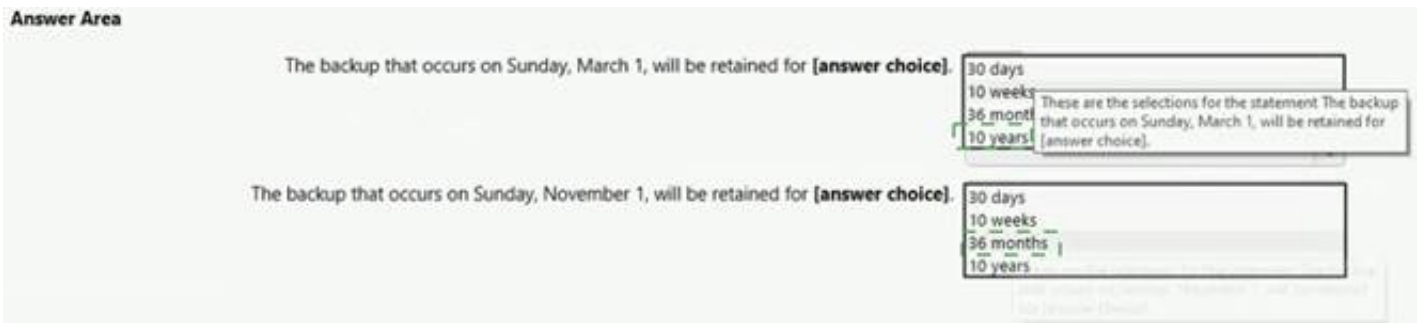
Explanation:
Placement Groups is a capability to achieve co-location of your Azure Infrastructure as a Service (IaaS) resources and low network latency among them, for improved application performance.
Azure proximity placement groups represent a new logical grouping capability for your Azure Virtual Machines, which in turn is used as a deployment constraint when selecting where to place your virtual machines. In fact, when you assign your virtual machines to a proximity placement group, the virtual machines are placed in the same data center, resulting in lower and deterministic latency for your applications.
The VMSS should share the same region, even it should be the same zone as proximity groups are located in the same data center. Accordingly, it should be proximity 2 only.
Reference:
https://azure.microsoft.com/en-us/blog/introducing-proximity-placement-groups

NEW QUESTION 211
HOTSPOT - (Topic 5)
You create a Recovery Services vault backup policy named Policy1 as shown in the following exhibit.





Answer:



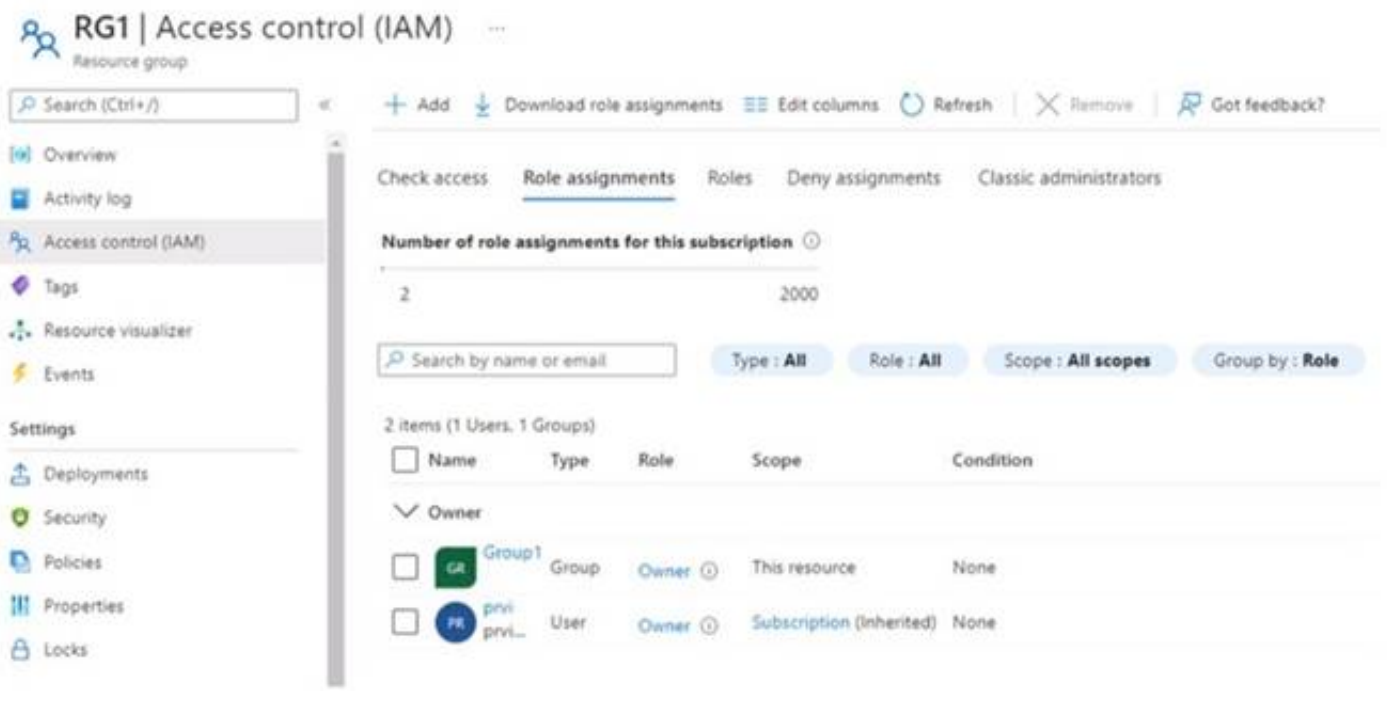
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: 10 years
The yearly backup point occurs to 1 March and its retention period is 10 years.
Box 2: 36 months
The monthly backup point occurs on the 1
of every month and its retention period is 36 months.
Note: Azure retention policy takes the longest period of retention for each backup. In case of conflict between 2 different policies.

NEW QUESTION 214
HOTSPOT - (Topic 5)

You have an Azure subscription that contains the users shown in the following table. The groups are configured as shown in the following table.



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
You can assign User2 the Owner role for RG1 by adding Group2 as a member of Group1.	○	○
You can assign User3 the Owner role for RG1 by adding Group3 as a member of Group1.	○	○
You can assign User3 the Owner role for RG1 by assigning the Owner role to Group3 for RG1.	○	○

Answer:

Answer Area

Statements	Yes	No
You can assign User2 the Owner role for RG1 by adding Group2 as a member of Group1.	○	○
You can assign User3 the Owner role for RG1 by adding Group3 as a member of Group1.	○	○
You can assign User3 the Owner role for RG1 by assigning the Owner role to Group3 for RG1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept#how-are- role-assignable-groups-protected
"Group nesting isn't supported. A group can't be added as a member of a role-assignable group."
For the second question:
https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/how-to-manage- groups#add-or-remove-a-group-from-another-group
"We currently don't support:
Adding Microsoft 365 groups to Security groups or other Microsoft 365 groups. "
For the third question, although it appears truncated in the screenshot (ending with "for...") there is a reference about Microsoft 365 groups support for roles assignment here: https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept#how-role- assignments-to-groups-work
"To assign a role to a group, you must create a new security or Microsoft 365 group with the is AssignableToRole property set to true. "

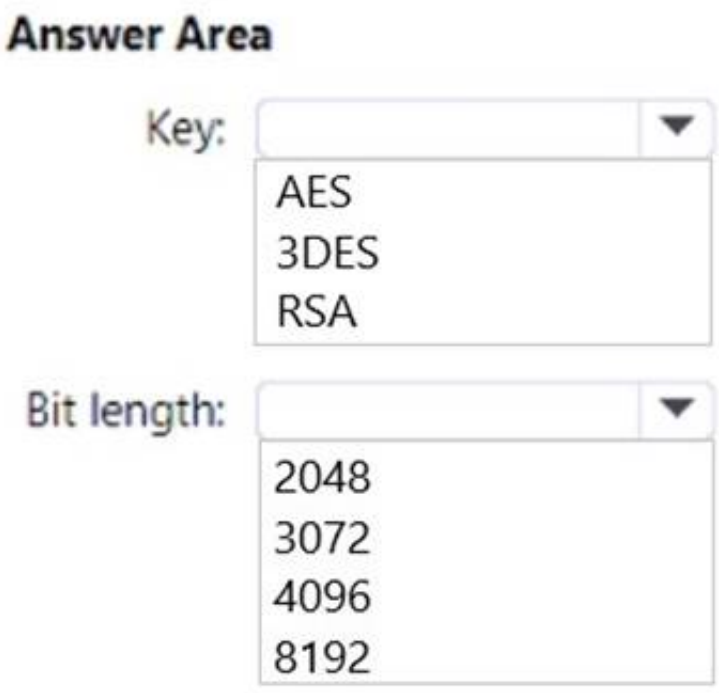
NEW QUESTION 216
- (Topic 5)
You have an Azure Storage account named storage1.
For storage 1. you create an encryption scope named Scope1. Which storage types can you encrypt by using Scope1?

A. file shares only
B. containers only
C. file shares and containers only
D. containers and tables only
E. file shares, containers, and tables only
F. file shares, containers, tables, and queues

Answer: B

Explanation:
"Encryption scopes enable you to manage encryption at the level of an individual blob or container." https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-scope- manage?tabs=portal

NEW QUESTION 221
HOTSPOT - (Topic 5)
You have an Azure subscription
You plan to deploy a new storage account
You need to configure encryption for the account The solution must meet the following requirements
• Use a customer-managed key stored in an key vault
• Use the maximum supported bit length.
Which type of key and which bit length should you use?



A. Mastered
B. Not Mastered

Answer: A

Explanation:
RSA 4096
Key: RSA
length: 4096 https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview#key-vault-requirements

NEW QUESTION 222
- (Topic 5)
You have an Azure virtual network named VNet1 that contains a subnet named Subnet1. Subnet1 contains three Azure virtual machines. Each virtual machine has a public IP address.
The virtual machines host several applications that are accessible over port 443 to user on the Internet.
Your on-premises network has a site-to-site VPN connection to VNet1.
You discover that the virtual machines can be accessed by using the Remote Desktop Protocol (RDP) from the Internet and from the on-premises network.
You need to prevent RDP access to the virtual machines from the Internet, unless the RDP connection is established from the on-premises network. The solution must ensure that all the applications can still be accesses by the Internet users.
What should you do?

A. Modify the address space of the local network gateway.
B. Remove the public IP addresses from the virtual machines.
C. Modify the address space of Subnet1.
D. Create a deny rule in a network security group (NSG) that is linked to Subnet1

Answer: D

Explanation:
You can use a site-to-site VPN to connect your on-premises network to an Azure virtual network. Users on your on-premises network connect by using the RDP or SSH protocol over the site-to-site VPN connection. You have to deny direct RDP or SSH access over the internet through an NSG.
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices

NEW QUESTION 227
- (Topic 5)
You have an Azure virtual network named VNet1 that contains a subnet named Subnet1. Subnet1 contains three Azure virtual machines. Each virtual machine has a public IP address.
The virtual machines host several applications that are accessible over port 443 to user on the Internet.
Your on-premises network has a site-to-site VPN connection to VNet1.
You discover that the virtual machines can be accessed by using the Remote Desktop Protocol (RDP) from the Internet and from the on-premises network.
You need to prevent RDP access to the virtual machines from the Internet, unless the RDP connection is established from the on-premises network. The solution must ensure that all the applications can still be accesses by the Internet users.
What should you do?

A. Modify the address space of the local network gateway.
B. Remove the public IP addresses from the virtual machines.
C. Modify the address space of Subnet1.
D. Create a deny rule in a network security group (NSG) that is linked to Subnet1.

Answer: D

Explanation:
You can filter network traffic to and from Azure resources in an Azure virtual network with a network security group. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.
You can use a site-to-site VPN to connect your on-premises network to an Azure virtual network. Users on your on-premises network connect by using the RDP or SSH protocol over the site-to-site VPN connection. You don't have to allow direct RDP or SSH access over the internet. And this can be achieved by configuring a deny rule in a network security group (NSG) that is linked to Subnet1 for RDP / SSH protocol coming from internet.
Modify the address space of Subnet1 : Incorrect choice
Modifying the address space of Subnet1 will have no impact on RDP traffic flow to the virtual network.
Modify the address space of the local network gateway : Incorrect choice
Modifying the address space of the local network gateway will have no impact on RDP traffic flow to the virtual network.
Remove the public IP addresses from the virtual machines : Incorrect choice
If you remove the public IP addresses from the virtual machines, none of the applications be accessible publicly by the Internet users.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/security-overview https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices

NEW QUESTION 231
- (Topic 5)
You have an Azure Storage account named storage1. You plan to use AzCopy to copy data to storage1.
You need to identify the storage services in storage1 to which you can copy the data.
What should you identify?

A. blob, file, table, and queue
B. blob and file only
C. file and table only
D. file only
E. blob, table, and queue only

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/import-export/storage-import-export-requirements

NEW QUESTION 232
- (Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some
question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that contains the virtual machines shown in the following table.
You deploy a load balancer that has the following configurations:
•Name: LB1
•Type: Internal
•SKU: Standard
•Virtual network: VNET1
You need to ensure that you can add VM1 and VM2 to the backend pool of LB1. Solution: You create two Standard public IP addresses and associate a Standard SKU
public IP address to the network interface of each virtual machine. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 236
- (Topic 5)
Your company has an Azure subscription named Subscription1.
The company also has two on-premises servers named Server1 and Server2 that run Windows Server 2016. Server1 is configured as a DNS server that has a primary DNS zone named adatum.com. Adatum.com contains 1,000 DNS records.
You manage Server1 and Subscription1 from Server2. Server2 has the following tools installed:
? The DNS Manager console
? Azure PowerShell
? Azure CLI 2.0
You need to move the adatum.com zone to Subscription1. The solution must minimize administrative effort.
What should you use?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Azure DNS supports importing and exporting zone files by using the Azure command-line interface (CLI). Zone file import is not currently supported via Azure PowerShell or the Azure portal.
References: https://docs.microsoft.com/en-us/azure/dns/dns-import-export

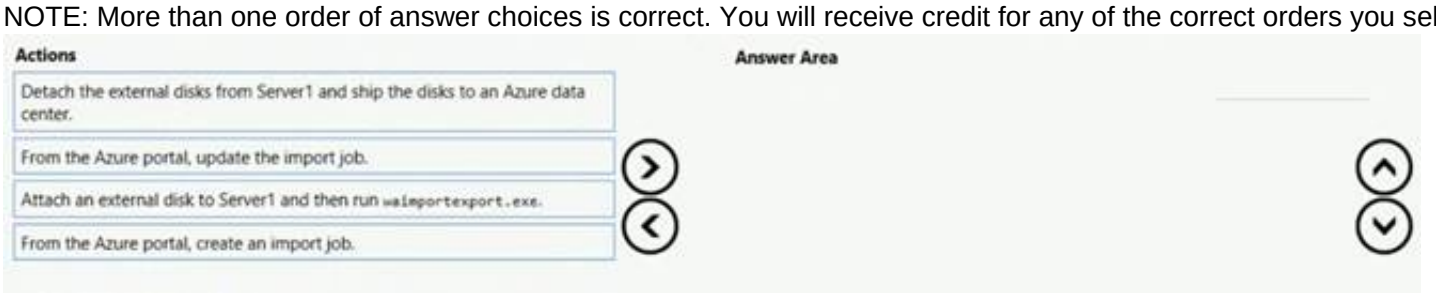
NEW QUESTION 238

- (Topic 5)
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 manage a virtual network named VNet1 that is hosted in the West US Azure region. VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.
You need to inspect all the network traffic from VM1 to VM2 for a period of three hours. Solution: From Azure Monitor, you create a metric on Network in and Network Out. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 243
DRAG DROP - (Topic 5)
You have an Azure subscription that contains a storage account.
You have an on-premises server named Server1 that runs Window Server 2016. Server1 has 2 TB of data.
You need to transfer the data to the storage account by using the Azure Import/Export service.
In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.
NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

At a high level, an import job involves the following steps:
Step 1: Attach an external disk to Server1 and then run waimportexport.exe
Determine data to be imported, number of drives you need, destination blob location for your data in Azure storage.
Use the WAImportExport tool to copy data to disk drives. Encrypt the disk drives with BitLocker.
Step 2: From the Azure portal, create an import job.
Create an import job in your target storage account in Azure portal. Upload the drive journal files.
Step 3: Detach the external disks from Server1 and ship the disks to an Azure data center. Provide the return address and carrier account number for shipping the drives back to you. Ship the disk drives to the shipping address provided during job creation.
Step 4: From the Azure portal, update the import job
Update the delivery tracking number in the import job details and submit the import job. The drives are received and processed at the Azure data center.
The drives are shipped using your carrier account to the return address provided in the import job.
References:
https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service

NEW QUESTION 245
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

AZ-104 Practice Exam Features:

* AZ-104 Questions and Answers Updated Frequently

* AZ-104 Practice Questions Verified by Expert Senior Certified Staff

* AZ-104 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* AZ-104 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year