Question 1: **Incorrect**

*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.*

You have an Azure subscription that contains the following users in an Azure Active Directory tenant named `az104exam.onmicrosoft.com`:

Larger image

Andy creates a new Azure Active Directory tenant named `external.az104exam.onmicrosoft.com`. You need to create new user accounts in `external.az104exam.onmicrosoft.com`.

Solution: You instruct Maria to create the user accounts.

Does that meet the goal?

- ● Yes **(Incorrect)**
- ○ No **(Correct)**

**Explanation**

To add or delete users from your Azure Active Directory (Azure AD) organization, you must be a User administrator or Global Administrator.

But only the user who creates a new tenant is added to it, and assigned the Global Administrator role.

User Administrators or Global Administrators in other tenants linked to the subscription do no inherit any administrative privileges on the new tenant.

So Maria has the Global Administrator role assigned in `az104exam.onmicrosoft.com`, and she will be able to create user accounts for this tenant, but she has no access on `external.az104exam.onmicrosoft.com` unless Andy grants specifically the User Administrator or the Global Administrator role in this new tenant.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-directory-independence

**Quick Preview:**

Question 2: Correct

*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.*

You have an Azure subscription that contains the following users in an Azure Active Directory tenant named `az104exam.onmicrosoft.com`:

Larger image

Andy creates a new Azure Active Directory tenant named `external.az104exam.onmicrosoft.com`. You need to create new user accounts in `external.az104exam.onmicrosoft.com`.

Solution: You instruct Beatrice to create the user accounts.

Does that meet the goal?

- ○ Yes
- ● No **(Correct)**

**Explanation**

To add or delete users from your Azure Active Directory (Azure AD) organization, you must be a User administrator or Global Administrator.

But only the user who creates a new tenant is added to it, and assigned the Global Administrator role.

User Administrators or Global Administrators in other tenants linked to the subscription do no inherit any administrative privileges on the new tenant.

So Beatrice doesn’t have a role allowing to manage user accounts in `az104exam.onmicrosoft.com`, like User Administrator or Global Administrator and she will not be able to create user accounts for this tenant.

Additionally, she doesn't have access to `external.az104exam.onmicrosoft.com` unless Andy grants specifically the User Administrator or the Global Administrator role in this new tenant.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory?view=azure-devops

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-directory-independence

**Quick Preview:**

Question 3: Correct

*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.*

You have an Azure subscription that contains the following users in an Azure Active Directory tenant named `az104exam.onmicrosoft.com`:

Larger image

Andy creates a new Azure Active Directory tenant named `external.az104exam.onmicrosoft.com`. You need to create new user accounts in `external.az104exam.onmicrosoft.com`.

Solution: You instruct John to create the user accounts.

Does that meet the goal?

- ○ Yes
- ● No (Correct)

**Explanation**

To add or delete users from your Azure Active Directory (Azure AD) organization, you must be a User administrator or Global Administrator.

But only the user who creates a new tenant is added to it, and assigned the global administrator role.

User Administrators or Global Administrators in other tenants linked to the subscription do no inherit any administrative privileges on the new tenant.

So John has the User Administrator role assigned in `az104exam.onmicrosoft.com`, and he will be able to create user accounts for this tenant, but he doesn't have access to `external.az104exam.onmicrosoft.com` unless Andy grants specifically the User Administrator or the Global Administrator role in this new tenant.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-directory-independence

**Quick Preview:**

Question 4: Correct
You have an Azure subscription named Subscription-Prod that contains a resource group named RG-01.

In RG-01, you create an internal load balancer named LB-01. You need to ensure that an administrator named Admin-01 can manage LB-01 and is allowed to add a backend pool to LB-01. The solution must follow the principle of least privilege.

Which role should you assign to Admin-01 ?

- ○ Contributor on LB-01
- ○ Network Contributor on LB-01
- ● Network Contributor on RG-01 **(Correct)**
- ○ Owner on LB-01

**Explanation**
The ***Network Contributor*** role lets you manage networks, but not access them. The Network Contributor role includes the Microsoft.Network/* action, so any action included in ***Microsoft.Network*** provider. When you assign the Network Contributor role to Admin-01, the exact permission (action) that will allow Admin-01 to create a backend pool is the following:

**Microsoft.Network/loadBalancers/backendAddressPools/write**

Action description as presented in the official documentation: This action will allow Admin-01 to create a load balancer backend address pool or update an existing load balancer backend address pool.

But in order to create the backend pool, is not enough to have Network Contributor access to the load balancer itself.

You also need read access over the Virtual Network, and the Virtual Machines you have to attach to the backend pool. And additionally you need some write permissions like **Microsoft.Network/virtualNetworks/subnets/join/action** to join the Vms to the backend pool.

So the least privilege role you can assign to Admin-01 is **Network Contributor on RG-01.**

**Reference:**

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork

**Quick Preview:**

Question 5: Correct

You have an Azure subscription named Subscription-Prod that contains a resource group named RG-01.

In RG-01, you create a public load balancer named LB-02. You need to ensure that an administrator named Admin-01 can manage LB-02 and is allowed to add a health probe to LB-02. The solution must follow the principle of least privilege.

Which role should you assign to Admin-01 ?

- ○ Contributor on LB-02
- ○ Network Contributor on LB-02
- ● Network Contributor on RG-01 **(Correct)**
- ○ Owner on LB-02

**Explanation**

The ***Network Contributor*** role lets you manage networks, but not access them. The Network Contributor role includes the Microsoft.Network/* action, so any action included in ***Microsoft.Network*** provider. When you assign the Network Contributor role to Admin-01, the exact permissions (actions) that will allow Admin-01 to add a health probe to the public load balancer, is the following:

**Microsoft.Network/loadBalancers/probes/read**

**Microsoft.Network/loadBalancers/probes/join/action**

But in order to create the health probe, it is not enough to have Network Contributor access to the load balancer itself.

You also need read access over the Virtual Network, and the Virtual Machines you have to attach to the backend pool. And additionally you need some write permissions like **Microsoft.Network/virtualNetworks/subnets/join/action** to join the VMs to the backend pool.

So the least privilege role you can assign to Admin-01 is **Network Contributor on RG-01**

**Reference:**

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftnetwork

**Quick Preview:**

Question 6: Correct

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named exam.com and an Azure Kubernetes Service (AKS) cluster named AKS1.

An administrator reports that she is unable to grant access to AKS1 to the users in exam.com. You need to ensure that access to AKS1 can be granted to the exam.com users.

What should you do first?

- ○ From exam.com, modify the Organization relationships settings
- ● From exam.com, create an OAuth 2.0 authorization endpoint **(Correct)**
- ○ Recreate AKS1

- ○
  From AKS1, create a namespace

**Explanation**
There are different ways to authenticate, control access/authorize and secure Kubernetes clusters.

Azure AD authentication is provided to AKS clusters with OpenID Connect. OpenID Connect is an identity layer built on top of the ***OAuth 2.0 protocol.***

**Reference:**

https://docs.microsoft.com/en-us/azure/aks/concepts-identity

**Quick Preview:**

Question 7: Correct
You have a Microsoft 365 tenant and an Azure Active Directory (Azure AD) tenant named az104exam.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? (SELECT TWO) Each correct answer presents a complete solution.

- ☑
  an Office 365 group that uses the Assigned membership type
  **(Correct)**
- □
  a Security group that uses the Assigned membership type
- ☑
  an Office 365 group that uses the Dynamic User membership type
  **(Correct)**
- □
  a Security group that uses the Dynamic User membership type
- □
  a Security group that uses the Dynamic Device membership type

**Explanation**
With the increase in usage of Microsoft 365 groups and Microsoft Teams, administrators and users need a way to clean up unused groups and teams. A Microsoft 365 groups expiration policy can help remove inactive groups from the system and make things cleaner.

You can set expiration policy only for Office 365 groups in Azure Active Directory (Azure AD). When a group expires, all of its associated services (the mailbox, Planner, SharePoint site, etc.) are also deleted.

**Reference:**

https://docs.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-groups-expiration-policy?view=o365-worldwide

**Quick Preview:**

Question 8: Correct
You have an Azure Storage account named storage-01. You plan to use AzCopy to copy data to storage-01.

Which of the following are valid storage services in storage-01 that you can copy data to?

- ○ blob, file, table, and queue
- ● blob and file only **(Correct)**
- ○ file and table only
- ○ file only
- ○ blob, table, and queue only

**Explanation**
AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account. AzCopy does not support table and queue storage services.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10

**Quick Preview:**

Question 9: Correct
You have an Azure Storage account named storage-01 that uses Azure Blob storage. You need to use AzCopy to copy data to blob storage, in storage account storage-01.

Which authentication method should you use for blob storage?

- ○ Azure Active Directory (Azure AD) only
- ○ Shared Access Signatures (SAS) only
- ○ Access Keys and Shared Access Signatures (SAS) only
- ● Azure Active Directory (Azure AD) and Shared Access Signatures (SAS) only **(Correct)**
- ○ Azure Active Directory (Azure AD), access keys and Shared Access Signatures (SAS)

**Explanation**

You can provide authorization credentials by using Azure Active Directory (AD), or by using a Shared Access Signature (SAS) token. Both Azure Active Directory (AD) and Shared Access Signature (SAS) token are supported for Blob storage.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10

**Quick Preview:**

Question 10: Correct

You have an Azure Storage account named storage-01 that uses Azure File storage. You need to use AzCopy to copy data to the  file storage in storage-01.

Which authentication method should you use for file storage?

- ○ Azure Active Directory (Azure AD) only
- ● Shared Access Signatures (SAS) only **(Correct)**
- ○ Access keys and Shared Access Signatures (SAS) only
- ○ Azure Active Directory (Azure AD) and Shared Access Signatures (SAS) only
- ○ Azure Active Directory (Azure AD), access keys and Shared Access Signatures (SAS)

**Explanation**

When using AzCopy, **Shared Access Signature (SAS)** token is the only authentication method supported for File storage.

When you access from **AzCopy**, your access uses HTTPS protocol, this access type is known as REST.

REST, or REpresentational State Transfer, is an architectural style for providing standards between computer systems on the web, making it easier for systems to communicate with each other. Access to Azure files is allowed using a Shared Access Signature(SAS) while using REST protocol (please see below):

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10

https://docs.microsoft.com/en-us/azure/storage/common/storage-auth

**Quick Preview:**

Question 11: Correct
You have an Azure subscription that contains an Azure Storage account. You need to create an Azure container instance that will use a Docker image. The image contains a Microsoft SQL Server instance that requires persistent storage.

You need to configure a storage service for your container. What Azure service should you use?

- ●
  Azure Files
  **(Correct)**
- ○
  Azure Blob Storage
- ○
  Azure Queue Storage
- ○
  Azure Table Storage

**Explanation**
By default, Azure Container Instances are stateless. If the container crashes or stops, all of its state is lost. **To persist state beyond the lifetime of the container, you must mount a volume from an external store**. Azure Container Instances can mount an Azure file share created with Azure Files.

Azure Files offers fully managed file shares hosted in Azure Storage that are accessible via the industry standard Server Message Block (SMB) protocol. Using an Azure file share with

Azure Container Instances provides file-sharing features similar to using an Azure file share with Azure virtual machines.

A standard Docker container volume is normally a directory stored on the Docker host machine. This makes the container dependent on the files on a particular host and thus makes it hard to migrate and scale out easily. With the Azure File Storage plugin, we can mount Azure File Storage shares as directories on your host’s file system and make it available to containers, which can now all make use of the Docker volume created through the plugin.

**Reference:**

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-volume-azure-files

**Quick Preview:**

Question 12: **Correct**

You have deployed in Azure an application App1, on two Azure virtual machines named VM1 and VM2. You plan to implement an Azure Availability Set for App1. The solution must ensure that App1 is available during planned maintenance of the servers hosting VM1 and VM2.

What should you include in the Availability Set?

- ○ one update domain
- ○ two fault domains
- ○ one fault domain
- ● two update domains **(Correct)**

**Explanation**

From time to time, Microsoft runs planned maintenance events in order to update their hardware and software. Sometimes, the servers need to be rebooted during the maintenance events, which means that VMs running on these servers will be rebooted as well.

In order to avoid having both VMs rebooted at the same time, you can include two update domains in your availability set configuration. Each VM will be part of a different update domain. A rebooted update domain is given 30 minutes to recover before maintenance is initiated on a different update domain.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/manage-availability

**Quick Preview:**

Question 13: Correct
You have an Azure subscription that contains the resources shown in the following table:
Larger image

You need to configure Azure Backup reports for Recovery-Vault-1.You are configuring the Diagnostics settings for the AzureBackupReports log.

Which storage accounts can you use for the Azure Backup reports of Recovery-Vault-1?

- ○ Storage1 only
- ○ Storage2 only
- ● Storage3 only **(Correct)**
- ○ Storage1, Storage2 and Storage3

**Explanation**
The storage account needs to be in the same region where you deploy the Recovery Services Vault.

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/backup-afs#create-a-recovery-services-vault

**Quick Preview:**

Question 14: Correct
You have an Azure subscription that contains the resources shown in the following table:
Larger image

You need to configure Azure Backup reports for Recovery-Vault-1.You are configuring the Diagnostics settings for the AzureBackupReports log.

Which Log Analytics workspaces can you use for the Azure Backup reports of Recovery-Vault-1?

- ○ LAW1

- ○ LAW2
- ○ LAW3
- ● LAW1, LAW2 and LAW3
  (Correct)

**Explanation**
The Log analytics Workspace is independent of the location or subscription.

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/configure-reports

**Quick Preview:**

Question 15: Correct
You have an Azure subscription named Subscription1. In Subscription1, you create an Azure file share named share1.

You create a shared access signature (SAS) named SAS1 as shown in the following exhibit:

Larger image

If on November 2, 2020, you run Microsoft Azure Storage Explorer on a computer that has an IP address of 134.92.112.1 and you use SAS1 to connect to the storage account, you `...........................`

- ○ `will be prompted for credentials`
- ● `will have no access`
  (Correct)
- ○ `will have read, write and list access`
- ○ `will have read-only access`

**Explanation**
The "Allowed IP Addresses" field doesn't include the IP address of the computer you are using to access the storage account. The range defined is ***134.92.112.10-134.92.112.50***, so starting from ***.10*** in the last octet and up to ***.50***, while the computer IP address is **134.92.112.1**, so ***.1*** in the last octet.

Question 16: Incorrect
You have an Azure subscription named Subscription1. In Subscription1, you create an Azure file share named share1.

You create a shared access signature (SAS) named SAS1 as shown in the following exhibit:

Larger image

If on November 10, 2020, you run the ***net use*** command on a computer that has an IP address of 134.92.112.50 and you use SAS1 to connect to share1,
you ............................

- ○
  will be prompted for credentials
- ○
  will have no access
  (Correct)
- ●
  will have read, write and list access
  (Incorrect)
- ○
  will have read-only access

**Explanation**
**Explanation:**

We can access Azure files using two different protocols REST or SMB.

The authentication methods you can use are different depending on the protocol you are using to access, as you can see in the quick preview at the end of the explanation.

In the scenario run **net use** command, and to correctly answer this question, we need to know than net use is sing SMB protocol. The SMB protocol is used Mapping a network drive using any method: Net use, Samba in Linux or Mac-OS, Map a drive from windows explorer,etc.

And as you can see on the image, Shared Access Signatures are not supported to access Azure Files using SMB protocol.

Does not matter if the SAS is generated for the time and the IP we are trying to access, because SMB access cannot use SAS as Authentication method.

So the correct answer is **Will have no access**.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-auth

**Quick Preview:**

Question 17: Correct

***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.***

You have an Azure subscription named Subscription-Dev. Subscription-Dev contains a resource group named RG-01. RG-01 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG-01.

Solution: From the RG-01 blade, you click ***Automation script***.

Does this meet the goal?

- ○ Yes
- ● No (Correct)

**Explanation**

No, Automation script will not help in this case. Instead, you can select Deployments inside RG-01 resource group and see a history of your deployments, inside the resource group.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deployment-history?tabs=azure-portal

**Quick Preview:**

Question 18: Correct

***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.***

You have an Azure subscription named Subscription-Dev. Subscription-Dev contains a resource group named RG-01. RG-01 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG-01.

Solution: From the RG-01 blade, you click ***Deployments.***

Does this meet the goal?

- ● Yes (Correct)
- ○ No

**Explanation**
While you are in your RG-01 resource group blade, click ***Deployments***. You will be able to see a history of your deployments for RG-01 resource group.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deployment-history?tabs=azure-portal

**Quick Preview:**

Question 19: Correct
***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.***

You have an Azure subscription named Subscription-Dev. Subscription-Dev contains a resource group named RG-01. RG-01 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG-01.

Solution: From the Subscriptions blade, you select the subscription, and then click ***Programmatic deploymen***t.

Does this meet the goal?

- ○ Yes
- ● No (Correct)

**Explanation**
While you are in your RG-01 resource group blade, click ***Deployments***. You will be able to see a history of your deployments for RG-01 resource group.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deployment-history?tabs=azure-portal

**Quick Preview:**

Question 20: Correct

***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.***

You have an Azure subscription named Subscription-Dev. Subscription-Dev contains a resource group named RG-01. RG-01 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG-01.

Solution: From the Subscriptions blade, you select the subscription, and then click **Resource providers**.

Does this meet the goal?

- ○ Yes
- ● No (Correct)

**Explanation**

No, ***Resource providers*** will not help in this case. Instead, you can select Deployments inside RG-01 resource group and see a history of your deployments, inside the resource group.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deployment-history?tabs=azure-portal

**Quick Preview:**

Question 21: Correct

You want to monitor the metrics and the logs of your Linux virtual machine VM-01.

Which of the following Azure services would you use for this task?

- ○ Azure HDInsight
- ● Linux Diagnostic Extension (LAD) 3.0 **(Correct)**
- ○ AzurePerformanceDiagnostics extension
- ○ Azure Analysis Services

**Explanation**

You can use extensions to configure diagnostics on your VMs to collect additional data metrics. The basic host metrics are directly available in Azure Monitor, but to see more granular and VM-specific metrics and logs information, you need to install an extension on the VM.

There are several extensions than can help to extend Azure Monitor Capabilities. **Linux Diagnostic Extension (LAD) 3.0** is one of these extensions, specific to Linux VMs.

Azure Performance Diagnostics Extension is not a correct answer. This extension helps you troubleshoot performance issues that can affect a Windows or Linux virtual machine (VM). Supported troubleshooting scenarios include quick checks on known issues and best practices, and complex problems that involve slow VM performance or high usage of CPU, disk space, or memory.

**Reference**

Linux Diagnostic Extension (LAD) 3.0: https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/diagnostics-linux

Overview of Azure Monitor Agents: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview

Azure Performance Diagnostics: https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/performance-diagnostics

**Quick Preview:**

Question 22: Correct

You are currently running in your Azure subscription a virtual machine named VM-01. You install and configure a web server and a DNS server on VM-01. VM-01 has the inbound network security rules shown in the following exhibit:

Larger image

Select the option that completes correctly the following sentence:

Internet users .......... .

- ○ can connect to only the DNS server on VM-01
- ● can connect to only the web server on VM-01
  (Correct)
- ○ can connect to the web server and DNS server on VM-01
- ○ cannot connect to the web server and DNS server on VM-01

**Explanation**

NSG rules are processed from top to bottom, so Rule_1 is processed first, then Rule_2, Rule_3 ... and so on.

DNS traffic is UDP/TCP port 53 and the first rule, Rule_1, denies this traffic, as configured action is ***Deny***. Web traffic is HTTP port 80 (or it could be HTTPS), so this is TCP port 80 (or TCP 443 for HTTPS traffic). Web traffic is explicitly permitted by Rule_3.

Conclusion: considering current inbound rules, only traffic to web server running on VM-01 is allowed.

**Reference:**

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

**Quick Preview:**

Question 23: Correct

You are currently running in your Azure subscription a virtual machine named VM-01. You install and configure a web server and a DNS server on VM-01. VM-01 has the inbound network security rules shown in the following exhibit:

Larger image

Select the option that completes correctly the following sentence:

If you delete Rule_1, Internet users .......... .

- ○ can connect to only the DNS server on VM-01
- ○

can connect to the web server and the DNS server on VM-01

- ●
  can connect to only the web server on VM-01
  **(Correct)**

- ○
  cannot connect to the web server and the DNS server on VM-01

**Explanation**

NSG rules are processed from top to bottom, so Rule_1 is processed first, then Rule_2, Rule_3 ... and so on.

If you delete Rule_1, as Web traffic is HTTP port 80 (or it could be HTTPS), so this is TCP port 80 (or TCP port 443 for HTTPS traffic) is explicitly allowed by Rule_3.

But what about access to DNS?

First you need to know than DNS works on port 53 using both protocols, UDP and TCP, but TCP is used only in specific situations:

- DNS primarily uses the User Datagram Protocol (UDP) on port number 53 to serve requests.

- DNS queries consist of a single UDP request from the client followed by a single UDP reply from the server.

- When the length of the answer exceeds 512 bytes the packet is truncated and a truncate bit (TC) is activated in the answer and the query is sent again using the Transmission Control Protocol (TCP).

TCP is also used for tasks such as zone transfers, which needs coherence and imply big packets.

- Now a days most DNS servers and clients implement EDNS (Extension Mechanism for DNS), allowing larger packets, up to 4096 bytes. This was Included in RFC-6891 in 2013.

Although you can enforce the use of TCP, by default, and tested in January 2021, from Windows 10 and Ubuntu 20.04 LTS in the scenario described in the question you don’t get responses from DNS Sever.

**Conclusion: after removing Rule_1, you “can connect to only the web server on VM-01”**

**Reference:**

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

https://tools.ietf.org/html/rfc6891

**Quick Preview:**

Question 24: Correct
You plan to deploy three Azure virtual machines named VM-01, VM-02, and VM-03. You need to ensure that at least two virtual machines are available if a single Azure datacenter becomes unavailable.

Which VM availability option should you choose?

- ○ all three VMs deployed in a single Availability Zone
- ○ all VMs deployed in a single Availability Set
- ● each VM deployed in a separate Availability Zone **(Correct)**
- ○ each VM deployed in a separate Availability Set

**Explanation**
Availability sets protect your applications from outages within an Azure data center, so an Availability Zone. An Availability Zone is actually a data center. As per the question, we need to make sure that we have at least two VMs available if a single Azure datacenter becomes unavailable.

Deploying the VMs in three different Availability Zones will meet the requirements.

**Reference:**

https://docs.microsoft.com/en-us/azure/availability-zones/az-overview#availability-zones

**Quick Preview:**

Question 25: Correct
You have an Azure virtual machine named VM-01 that runs Windows Server 2019. You save VM-01 as a template named ***VM-Template*** to the Azure Resource Manager library. You plan to deploy a virtual machine named VM-02 from ***VM_Template***, using Azure Portal

What can you configure during the deployment of VM-02?

- ○ operating system
- ○

administrator username

- ○<br>virtual machine size
- ●<br>resource group<br>**(Correct)**

**Explanation**
After you deploy VM-01, you can save the template and reuse it to deploy other virtual machines, with the same configuration as VM-01. During the deployment of VM-02, you can change the resource group, if you need to.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/ps-template

**Quick Preview:**

Question 26: Correct
You have an Azure subscription that contains an Azure virtual machine named VM-01. VM-01 runs an application that does not support multiple active instances.

At the end of each month, CPU usage for VM-01 peaks when the application runs. You need to create a scheduled runbook to increase the processor performance of VM-01 at the end of each month.

What task should you include in the runbook?

- ○<br>Add the Azure Performance Diagnostics agent to VM-01
- ●<br>Modify the VM size property of VM-01<br>**(Correct)**
- ○<br>Add VM-01 to a scale set
- ○<br>Increase the vCPU quota for the subscription
- ○<br>Add a Desired State Configuration (DSC) extension to VM-01

**Explanation**
Virtual Machine Scale Sets can be used with the Azure Desired State Configuration (DSC) extension handler. Virtual machine scale sets provide a way to deploy and manage large numbers of virtual machines, and can elastically scale in and out in response to load. DSC is used to configure the VMs as they come online so they are running the production software.

BUT, the questions states that the application running on VM-01 does not support multiple active instances, so does not support running on multiple VMs. So this leads us to excluding options C and E.

Option A is also incorrect, Azure Performance Diagnostics agent can help when you need advanced monitoring capabilities.

Option D is also incorrect. Increasing the quota of a subscription doesn't mean you are increasing the vCPU or your VM.

The only option left is option B - Modify the VM size property of VM-01. When you have a CPU/performance issue, then the solution is to scale up (increase VM size).

Question 27: Correct

You have an Azure virtual machine named **VM-W2019** that runs Windows Server 2019. The virtual machine was deployed using default options during the setup. You sign in to **VM-W2019** and perform the following actions:

- Create files on drive C

- Create files on drive D

- Modify the screen saver timeout

- Change the desktop background

You plan to redeploy **VM-W2019**. Which changes will be lost after you redeploy **VM-W2019**?

- ○ the modified screen saver timeout
- ○ the new desktop background
- ● the new files on drive D **(Correct)**
- ○ the new files on drive C

**Explanation**

If you deploy a Windows VM and keep the default options throughout the setup, you will get a VM with two disks attached. The D drive is the temporary disk and any files deployed on D drive will be lost during a redeploy. The screensaver, wall paper and any new files on C drive are available after a redeploy.

The data on these temporary disks may not remain through standard VM lifecycle events. This is because the data for the temporary disks is stored on the host operating system running the hypervisor software while the data for persistent disks is stored in Microsoft

Azure Storage. The temporary disk is very useful for data which, you guessed it, is temporary in nature

**Reference:**

https://azure.microsoft.com/en-gb/blog/virtual-machines-best-practices-single-vms-temporary-storage-and-uploaded-disks/

**Quick Preview:**

Question 28: Correct
You have an on-premises virtual machine named VM-01. Some settings for VM-01 are shown below:
Larger image

You need to ensure that you can use the disks attached to VM-01 as a template for Azure virtual machines.

What should you modify on VM-01?

- ○ memory
- ○ network adapters
- ● hard drive (Correct)
- ○ processor
- ○ SCSI controller

**Explanation**
Before you upload a Windows virtual machine (VM) from on-premises to Azure, you must prepare the virtual hard disk (VHD or VHDX). Azure supports both generation 1 and generation 2 VMs that are in VHD file format and that have a fixed-size disk.

From the exhibit we see that the disk is in the VHDX format, so the disk needs to be converted to VHD format.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image

**Quick Preview:**

Question 29: Correct

You are running a virtual machine scale set in your Azure subscription. The scale set contains four instances that have the following configurations:

***Operating system***: Windows Server 2016

***Size***: Standard_D1_v2

You run the ***Get-AzVmss*** cmdlet as shown in the following exhibit:

Larger image

When an administrator changes the virtual machine size, the size will be changed on up to .......... virtual machines simultaneously.

- ○ 0
- ○ 1
- ○ 2
- ● 4 **(Correct)**

**Explanation**

Scale sets have two definitions: The definition model that is updated every time we apply a change, and the instance view model, that corresponds with what is really deployed.

Scale sets have an "upgrade policy" that determine how VMs are brought up-to-date with the latest scale set model, so how the modifications we make over the definition model will apply to the instance view model. There are three modes for the upgrade policy:

**Automatic** - In this mode, scale set updates automatically. The scale set makes no guarantees about the order of VMs being brought down. The scale set may take down all VMs at the same time.

**Rolling** - In this mode, the scale set rolls out the update in batches with an optional pause time between batches according wit the parameters we can setup.

**Manual** - In this mode, when you update the scale set model, nothing happens to existing VMs. You have to manage manually, usually deleting the machines, and the new replacements are updated.

Additionally if you select the Rolling mode the following screen shows the options you can setup:

In the exhibit for our scenario, we can see ***EnableAutomaticUpdates: false***, but this output is for ***VitrualMachineProfile.OSProfile.WindowsConfiguration.***

On the other hand, the output for the filter ***Select -ExpandProperty UpgradePolicy,*** shows clearly, that the mode is set to ***Automatic.***

So according to automatic Mode all the VMs in the VMSS can be updated at the same time, and because the VMSS currently has 4 instances, the correct answer is: ***When an administrator changes the virtual machine size, the size will be changed on up to 4 virtual machines simultaneously.***

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-upgrade-scale-set#how-to-bring-vms-up-to-date-with-the-latest-scale-set-model

**Quick Preview:**

Question 30: Correct

You are running a virtual machine scale set in your Azure subscription. The scale set contains four instances that have the following configurations:

***Operating system***: Windows Server 2016

***Size***: Standard_D1_v2

You run the ***Get-AzVmss*** cmdlet as shown in the following exhibit:

Larger image

When a new version of the Windows Server 2016 image is released, the new build will be deployed to up to .......... virtual machines simultaneously.

- ● 0 **(Correct)**
- ○ 1
- ○ 2
- ○ 4

**Explanation**

Taking a closer look at the exhibit presented, we need to make a clear distinction between two different configurations, as highlighted below:

The simplest way to understand where these configurations are coming from, is by taking a look in the Azure portal, under VMSS setup -> Management tab:

**Number 1** refers to Operating system upgrades, where we have the possibility to either enable or not this functionality.

**Number 2** refers to your application deployed in the VMSS, and you have three options available: Automatic, Manual or Rolling.

As this question is talking about Operating system upgrades, and the automatic updates for Operating system (1) is set to false, the operating system will not be updated automatically, and therefore **the correct answer is 0.**

If this parameter was set to true, the answer will be 1, because the upgrade orchestrator identifies the batch of VM instances to upgrade, with any one batch having a maximum of 20% of the total instance count, subject to a minimum batch size of one virtual machine. This means that maximum 20% of your virtual machine scale set will be deployed at once, so this is 0.8 out of 4 VMs, and a minimum of one virtual machine. So the OS upgrade will be done by upgrading one virtual machine at a time.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-automatic-upgrade#how-does-automatic-os-image-upgrade-work

**Quick Preview:**

Question 31: Correct

***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.***

You have a computer named Computer-01 that has a point-to-site VPN connection to an Azure virtual network named AZ-104-vNET. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer-02. You need to ensure that you can establish a point-to-site VPN connection to AZ-104-vNET from Computer-02.

***Solution:*** You modify the Azure Active Directory (Azure AD) authentication policies.

Does this meet the goal?

- ○ Yes
- ● No (Correct)

**Explanation**
Point-to-Site VPNs connections use certificates to authenticate.

Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client certificate is not installed, authentication fails.

**Reference:**

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site

**Quick Preview:**

Question 32: Correct
***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.***

You have a computer named Computer-01 that has a point-to-site VPN connection to an Azure virtual network named AZ-104-vNET. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer-02. You need to ensure that you can establish a point-to-site VPN connection to AZ-104-vNET from Computer-02.

***Solution:*** You join Computer-02 to Azure Active Directory (Azure AD).

Does this meet the goal?

- ○ Yes
- ● No (Correct)

**Explanation**
Point-to-Site VPNs connections use certificates to authenticate.

Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client certificate is not installed, authentication fails.

**Reference:**

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site

**Quick Preview:**

Question 33: Correct

***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.***

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?

- ○ Yes
- ● No **(Correct)**

**Explanation**

Azure Locks are used to prevent accidental changes in an Azure environment. Azure Locks can't help for this task, more information about Azure Locks below.

You can set the lock level to **CanNotDelete** or **ReadOnly**. In the portal, the locks are called **Delete** and **Read-only** respectively.

**CanNotDelete** means authorized users can still read and modify a resource, but they can't delete the resource.

**ReadOnly** means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the **Reader** role.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

**Quick Preview:**

Question 34: Correct

***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.***

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?

- ○ Yes
- ● No **(Correct)**

**Explanation**

Unregistering Microsoft.ClassicNetwork provider has nothing to do with what is being asked. Instead, you could configure a custom policy definition, and then assign the policy to the subscription.

**Reference:**

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

https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-custom-policy-definition

**Quick Preview:**

Question 35: Correct

***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.***

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 assign a built-in policy definition to the subscription.

Does this meet the goal?

- ○ Yes
- ● No (Correct)

**Explanation**
Built-in policies don't include creating rules in NSGs with 8080 port number. Instead, you could configure a custom policy definition, and then assign the policy to the subscription.

**Reference:**

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

https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-custom-policy-definition

**Quick Preview:**

Question 36: Correct
***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.***

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?

- ● Yes (Correct)
- ○ No

**Explanation**
Indeed, configuring a custom policy definition and then assigning the policy to the subscription can solve the task.

**Reference:**

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

https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-custom-policy-definition

**Quick Preview:**

Question 37: Correct
You try to connect to a Windows Server VM running in Azure, but the connection fails. You begin investigating the problem by taking a look at the Networking settings:
Larger image

You need to establish a Remote Desktop connection to VM-01. What should you do to fix the problem?

- ○ Change the priority of the RDP rule
- ○ Attach another network interface
- ○ Delete the DenyAllInBound rule
- ● Start VM-01 (Correct)

**Explanation**
Taking a closer look at the information available at the network interface level should provide the resolution.

In this case, the NIC Public IP is not available, which means that the VM is not running.

After powering on the VM, the public IP will be populated and we will be able to connect to the Windows Server VM. The first rule, Allow_RDP, allows RDP traffic to the VM.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-public-ip-address

Question 38: Correct

You are running four VMs in your Azure subscription. The virtual machines are deployed as follows:

Larger image

A DNS service is installed on VM-01. You configure the DNS servers settings for each virtual network to use 10.1.0.100 as their DNS server. You need to ensure that all the virtual machines can resolve DNS names by using the DNS service on VM-01.

What should you do?

- ○ Configure a conditional forwarder on VM-01
- ○ Add service endpoints on vNET1
- ○ Add service endpoints on vNET2 and vNET3
- ● Configure peering between vNET1, vNET2 and vNET3 **(Correct)**

**Explanation**

Virtual network peering enables you to seamlessly connect networks in Azure Virtual Network. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines uses the Microsoft backbone infrastructure.

Once you set up virtual network peerings between all virtual networks, VM-02, VM-03 and VM-04 will be able to reach VM-01, the DNS server, which fulfils the task.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

**Quick Preview:**

Question 39: Correct

You have an Azure subscription that contains the Azure virtual machines shown in the following table:

Larger image

You add inbound security rules to a network security group (NSG) named NSG-01 as shown in the following table:

Larger image

**You run Azure Network Watcher as shown in the following exhibit:**
Larger image

You run Network Watcher again as shown in the following exhibit:

Larger image

Please evaluate the following statement and decide if it's true or false.

NSG-01 limits VM-01 traffic.

- ○ True
- ● False (Correct)

**Explanation**
As specified in the question, the two rules defined are inbound rules. The question doesn't specify to what VM is NSG-01 applied, just that these are inbound rules. If we take a look at the two rules again ...

... we see that the first rule has 10.0.0.0/24 as the source IP address. So these rules can't be applied as inbound rules to VM-01.

It would sound as "I am blocking traffic coming inbound from ... myself". So conclusion is that these rules are applied to VM-02, again as inbound rules.

Finally, let's take a look at the statement that we need to evaluate:

"NSG-01 limits VM-01 traffic." and the statement is False. As NSG-01 is applied to VM-02, NSG-01 limits traffic to VM-02 and not VM-01 traffic.

Question 40: Incorrect
You have an Azure subscription that contains the Azure virtual machines shown in the following table:
Larger image

You add inbound security rules to a network security group (NSG) named NSG-01 as shown in the following table:

Larger image

You run Azure Network Watcher as shown in the following exhibit:
Larger image

You run Network Watcher again as shown in the following exhibit:

Larger image

Please evaluate the following statement and decide if it's true or false.

NSG-01 may be applied to VM-02.

- ○ Yes **(Correct)**
- ● No **(Incorrect)**

**Explanation**
As specified in the question, the two rules defined are inbound rules. The question doesn't specify to what VM is NSG-01 applied, just that these are inbound rules. If we take a look at the two rules again ...

... we see that the first rule has 10.0.0.0/24 as the source IP address. So these rules can not be applied as inbound rules to VM-01.

It would sound as "I am blocking traffic coming inbound from ... myself".

If it was applied to VM-02, TCP traffic from VM-01 on ports 80 and 443 (HTTP. HTTPS) will be allowed, and any other TCP traffic will be denied, aligned with the Network Watcher screen testing TCP-8080 from VM-01 to VM-02.

So conclusion is that these rules may be applied to VM-02, as inbound rules, as the questions states, and statement "NSG-01 my be applied to VM-02." is True.

**References:**

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

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

Question 41: Correct
You are running three virtual machines in Azure, deployed in Subnet-01, inside vNET1 virtual network. Each virtual machine has a public IP address. The virtual machines host several applications that are accessible over port 443 to users 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 other applications can still be accessed by the Internet users.

What should you do?

- ○ Modify the address space of the local network gateway
- ● Create a deny rule in a network security group (NSG) that is linked to Subnet-01 **(Correct)**
- ○ Remove the public IP addresses from the virtual machines
- ○ Modify the address space of Subnet-01

**Explanation**
Here's how the overall picture looks like:

The question states that only RDP traffic coming from the Internet should be denied. RDP traffic coming from the on-premises data center needs to be permitted, so this RDP traffic will traverse through the site-to-site VPN tunnel established between Azure vNET1 and on-prem DC.

In the NSG, you would need to define two rules actually. In the first rule, with a higher priority (lower priority number), you would ***Allow*** RDP traffic from on-prem DC. In the second rule, you would deny RDP traffic from any location.

The network security group would like this:

In this example, I have considered that the IP subnet used in the on-prem DC is 192.168.0.0/24, so that is the source of the traffic coming to our three VMs. So this traffic is permitted, but RDP traffic coming from any other source will be denied by the second rule, so this includes traffic from the internet as requested by the question.

**Reference:**

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

Question 42: Correct
You have an Azure subscription that contains the resources in the following table:
Larger image

NIC1 network interface card attaches VM1 to Subnet1. Subnet1 is associated to VNet1. You need to apply ASG1 to VM1.

What should you do?

- ●
  Associate NIC1 to ASG1
  **(Correct)**
- ○
  Modify the properties of ASG1
- ○
  Modify the properties of NSG1

**Explanation**
Network interface cards (NICs) can be associated to Application Security Groups (ASGs). Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups. You can reuse your security policy at scale without manual maintenance of explicit IP addresses.

You can take a look at the following schema, right from Azure documentation:

So, where do you apply the ASG? Where can you find it in Azure portal? The answer below ... first ***Networking***, then select ***Application Security Groups*** and select ***Configure the application security groups***.

You can then select an existing Application Security Group where you want to include your VM NIC.
Question 43: Correct
You have an Azure subscription named Subscription1 that contains an Azure virtual network named VNet1. VNet1 connects to your on-premises network by using Azure ExpressRoute. You plan to prepare the environment for automatic failover in case of ExpressRoute failure.

You need to connect VNet1 to the on-premises network by using a site-to-site VPN. The solution must minimize cost.

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

- ☑

Create a connection
**(Correct)**

- ☑
  Create a local site VPN gateway
  **(Correct)**
- ☑
  Create a VPN gateway that uses the VpnGw1 SKU
  **(Correct)**
- □
  Create a gateway subnet
- □
  Create a VPN gateway that uses the Basic SKU

**Explanation**
Although the question asks that the solution must minimize cost, Basic SKU is not supported when you need to run both ExpressRoute and site-to-site VPN. So we need to use ***VpnGw1*** SKU.

Because ExpressRoute is already in place, aGateway Subnet already exists, so no need to create a new one.

**Reference:**

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager

**Quick Preview:**

Question 44: Correct
You have an Azure web app named webapp1. Users report that they often experience HTTP 500 errors when they connect to webapp1.

You need to provide the developers of webapp1 with real-time access to the connection errors. The solution must provide all the connection error details.

What should you do first?

- ●
  From webapp1, enable Web server logging
  **(Correct)**
- ○
  From Azure Monitor, create a workbook
- ○
  From Azure Monitor, create a Service Health alert
- ○

From webapp1, turn on Application Logging

**Explanation**
As opposed to Application Logging option, when enabling the ***web server logging*** option, each log message will include : HTTP method, resource URI, client IP, client port, user agent and ***response code***, which for this questions is relevant - error code 500.

**Reference:**

https://docs.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs

https://docs.microsoft.com/en-us/archive/blogs/azureossds/how-to-identifyreview-errors-on-php-applications-in-azure-web-apps-using-log-stream-service

**Quick Preview:**

Question 45: Correct
You have an Azure subscription that has a Recovery Services vault named Vault1. The subscription contains the virtual machines shown in the following table:
Larger image

You plan to schedule backups to occur every night at 23:00. Which virtual machines can you back up by using Azure Backup?

- ○
  VM1 and VM3 only
- ●
  VM1, VM2, VM3 and VM4
  **(Correct)**
- ○
  VM1 and VM2 only
- ○
  VM1 only

**Explanation**
Azure Backup supports backup the following OS:

- Windows Server 64-bit operating system from Windows Server 2008

- Windows 10 operating system 64-bit

- Ubuntu Server 64-bit operating system from Ubuntu 12.04

Azure Backup supports backup of VM that are shutdown or offline.

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/endorsed-distros

**Quick Preview:**

Question 46: Correct
You have an Azure subscription named Subscription1 that contains the resources shown in the following table:
Larger image

You create virtual machines in Subscription1 as shown in the following table:
Larger image

You plan to use Vault1 for the backup of as many virtual machines as possible.

Which virtual machines can be backed up to Vault1?

- ○ VM1 only
- ○ VM3 and VMC only
- ○ VM1, VM2, VM3, VMA, VMB, and VMC
- ● VM1, VM3, VMA, and VMC only **(Correct)**
- ○ VM1 and VM3 only

**Explanation**
To create a vault to protect virtual machines, the vault must be in the same region as the virtual machines. If you have virtual machines in several regions, create a Recovery Services vault in each region.

**Reference:**

https://docs.microsoft.com/bs-cyrl-ba/azure/backup/backup-create-rs-vault

Question 47: Correct
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.

- □ the **kubectl** command
- ☑ the ***az aks*** command **(Correct)**
- □ the ***Set-AzVm*** cmdlet
- ☑ the Azure portal **(Correct)**
- □ the ***Set-AzAks*** cmdlet

**Explanation**

Let’s review each possible answer in order to discover if it’s a correct option or not:

**the kubectl command.**

kubetcl command is mainly used to horizontally scale pods. Kubernetes as deployed some integrations with main cloud providers, to autoscale nodes, based in a yaml configuration file.

In the first link provided you have detailed information about this process.

This option is deployed by Kubernetes, and not supported by Microsoft, so if we have two better options we will discard this one.

**the az aks command.**

This option is correct and represents the way to autoscale a AKS Cluster using Az CLI commands. You can find all the information in the second link provided.

To setup AKS cluster autoscaler when creating it use az **aks create** command:

To setup an existing AKS cluster to autoscale, use **az aks update** command:

**the Set-AzVm cmdlet.**

This Az Powershell cmdlet is not the appropriate to aks cluster autoscaler. The correspondent Az PowerShell cmdlet is Set-AzAksCluster.

**the Azure portal.**

Currently, June 2021, it is not possible to enable autoscale when creating an AKS Cluster, but once created you can enable autoscale. To do that, go to your AKS cluster, and from the left side menu go to agent pools. Select the agent pool you want to scale:

In the Overview screen click on the Disabled link next to autoscale:

And finally in the scale screen, select Autoscale and setup min and max node count:

**the Set-AzAks cmdlet.**

This Az Powershell cmdlet is not  appropriate to aks cluster autoscaler. The correspondent Az PowerShell cmdlet is Set-AzAksCluster.

**Reference:**

https://github.com/kubernetes/autoscaler/tree/master/cluster-autoscaler/cloudprovider/azure

https://docs.microsoft.com/en-us/azure/aks/cluster-autoscaler

**Quick Preview:**

Question 48: Correct

You create the following resources in an Azure subscription:

- An Azure Container Registry instance named Registry1

- An Azure Kubernetes Service (AKS) cluster named Cluster1

You create a container image named App1 on your administrative workstation.

You need to deploy App1 to Cluster1.

What should you do first?

- ○ Run the docker push command
- ○ Create an App Service plan
- ● Run the ***az acr build*** command **(Correct)**
- ○ Run the ***az aks create*** command

**Explanation**

You should sign in and push a container image to Container Registry. Run the ***az acr build*** command to build and push the container image.

```
az acr build \

--image contoso-website \

--registry $ACR_NAME \

--file Dockerfile .
```

**Reference:**

https://docs.microsoft.com/en-us/learn/modules/aks-deploy-container-app/5-exercise-deploy-app

Question 49: Correct

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

Larger image

You need to configure a proximity placement group for VMSS1.

Which proximity placement groups should you use?

- ● Proximity2 only **(Correct)**
- ○ Proximity1, Proximity2, and Proximity3
- ○ Proximity1 only
- ○ Proximity1 and Proximity3 only

**Explanation**

We only can use Proximity2 only, because is the only Proximity Group in the same location (region), as our VMSS1.

It doesn’t matter if VMSS1 and Proximity2 are in the same Resource group, but is mandatory they are in the same location.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/proximity-placement-groups-portal

https://azure.microsoft.com/en-us/blog/introducing-proximity-placement-groups/

**Quick Preview:**

Question 50: Correct

You have an Azure subscription named Subscription1 that contains an Azure virtual machine named VM1. VM1 is in a resource group named RG1. VM1 runs services that will be used to deploy resources to RG1.

You need to ensure that a service running on VM1 can manage the resources in RG1 by using the identity of VM1.

What should you do first?

- ●
  From the Azure portal, modify the Managed Identity settings of VM1
  (Correct)
- ○
  From the Azure portal, modify the Access control (IAM) settings of RG1
- ○
  From the Azure portal, modify the Access control (IAM) settings of VM1
- ○
  From the Azure portal, modify the Policies settings of RG1

**Explanation**

Managed identities for Azure resources provides Azure services with an automatically managed identity in Azure Active Directory. You can use this identity to authenticate to any service that supports Azure AD authentication, without having credentials in your code.

You can enable and disable the system-assigned managed identity for a VM using the Azure portal.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/qs-configure-portal-windows-vm

**Quick Preview:**

Question 51: Correct

You have an Azure subscription that contains a resource group named AZ-104-RG. You use AZ-104-RG to validate an Azure deployment.

AZ-104-RG contains the following resources:

Larger image

You need to delete AZ-104-RG.

What should you do before deleting AZ-104-RG?

- ○ Modify the backup configurations of VM1 and modify the resource lock type of VNET1
- ○ Remove the resource lock from VNET1 and delete all data in Vault1
- ● From Recovery Services Vault Vault1, stop the backup of VM1, and remove the resource lock from VNET1
  **(Correct)**
- ○ Turn off VM1 and delete all data in Vault1

**Explanation**

There are two things that you need to do before deleting AZ-104-RG: delete the lock and stop the backup of VM1 from the Recovery Services vault.

First, you need to remove the Delete lock from VNET1, modifying the lock (to read-only lock type) will not help.

Here's how the Delete lock configuration looks like:

and when you try to delete the whole resource group - AZ-104-RG - you will receive an error, just like below:

Once you delete the lock and try again to delete the resource group, you will still get an error. This error appears because you can't delete a Recovery Services Vault that contains protected data sources, like backup data.

In order to delete a vault, there are several steps that need to be performed first, as follows:

- Disable the soft delete feature; soft delete still keeps the deleted data available for some time, before complete removal

***- Stop any ongoing backups***

- Ensure all registered storage accounts are deleted

- And last, delete the actual vault

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

**Quick Preview:**

Question 52: **Correct**
***Case study***

***This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.***

***To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.***

***Overview***

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market. Contoso products are manufactured by using blueprint files that the company authors and maintains.

***Existing Environment***

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

- File servers

- Domain controllers

- Microsoft SQL Server servers

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

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

- A SQL database

- A web front end

- A processing middle tier

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

### *Requirements*

### *Planned Changes*

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.

- Move the existing product blueprint files to Azure Blob storage.

- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

### *Technical Requirements*

- Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.

- Minimize the number of open ports between the App1 tiers.

- Ensure that all the virtual machines for App1 are protected by backups.

- Copy the blueprint files to Azure over the Internet.

- Ensure that the blueprint files are stored in the archive storage tier.

- Ensure that partner access to the blueprint files is secured and temporary.

- Prevent user passwords or hashes of passwords from being stored in Azure.

- Use unmanaged standard storage for the hard disks of the virtual machines.

- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

- Minimize administrative effort whenever possible.

### *User Requirements*

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.

- Designate a new user named Admin1 as a local admin on all joined devices

- Admin1 must receive email alerts regarding service outages.

- Ensure that a new user named User3 can create network objects for the Azure subscription.

You need to configure the Device settings to meet the technical requirements and the user requirements.

Larger image

Which two settings should you modify?

- ☑ 1. **(Correct)**
- □ 2.
- □ 3.
- □ 4.
- □ 5.
- ☑ 6. **(Correct)**

**Explanation**
Requirements to cover and their coverage:

**Technical requirements:**

- *Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.*

Already covered because the *Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication* is selected to **Yes**.

**User Requirements:**

- *Ensure that only users who are part of a group named Pilot can join devices to Azure AD.*

To cover this requirement we need to chose selected in *Users may join devices to Azure AD*, and then add the Pilot group to selected list. This is answer **1**.

- *Designate a new user named Admin1 as a local admin on all joined devices*

To cover this requirement, we need to modify *Additional local administrators on Azure AD joined devices* to selected and create a new user Admin1. This is Answer **6**

Question 1: Skipped

You have an Azure Active Directory (Azure AD) tenant named az104exam.com that contains the users shown in the following table:

Larger image

User 3 is the owner of ***Admins_Group***. ***Secondary_Group*** is a member of ***Admins_Group***.

You configure an access review named Review-01 as shown in the following exhibit:

Larger image

Please evaluate if the following statement is `True` or `False`:

User 3 can perform an access review of User 1.

- ○ True
- ○ False (Correct)

**Explanation**

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

After taking a closer look at the configured Access Review, we can see that an access review can be performed:

- by the group owner, which is User 3

- on Admins_Group

- on Guest users only

As User 1 is a Member of Admins_Group (and not a Guest user), User 3 can't review User 1's access, so the statement is False.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

**Quick Preview:**

Question 2: Skipped

You have an Azure Active Directory (Azure AD) tenant named az104exam.com that contains the users shown in the following table:

Larger image

User 3 is the owner of ***Admins_Group***. ***Secondary_Group*** is a member of ***Admins_Group***.

You configure an access review named Review-01 as shown in the following exhibit:

Larger image

Please evaluate if the following statement is `True` or `False`:

User 3 can perform an access review of User 4.

- ○ True
- ○ False (Correct)

**Explanation**

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

After taking a closer look at the configured Access Review, we can see that an access review can be performed:

- by the group owner, which is User 3

- on Admins_Group

- on Guest users only

User 4 is a Member of Secondary_Group, which is a member of Admins_Group. Still, User 4 is not a Guest user, so User 3 can't review User 4's access, so the statement is False.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

**Quick Preview:**

Question 3: Skipped

You have an Azure Active Directory (Azure AD) tenant named az104exam.com that contains the users shown in the following table:

Larger image

User 3 is the owner of ***Admins_Group***. ***Secondary_Group*** is a member of ***Admins_Group***.

You configure an access review named Review-01 as shown in the following exhibit:

Larger image

Please evaluate if the following statement is `True` or `False`:

User 3 can perform an access review of User 5.

- ○ True (Correct)
- ○ False

**Explanation**

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

After taking a closer look at the configured Access Review, we can see that an access review can be performed:

- by the group owner, which is User 3

- on Admins_Group

- on Guest users only

User 5 is a Guest of Secondary_Group, which is a member of Admins_Group.

And User 3, who is performing the review, can perform the review on Admins_Group and any groups included in the Admins_Group, and this includes the Secondary_Group.

Nested groups are not fully supported in Azure AD, but inheritance for access reviews is already implemented and available, **so the statement is True.**

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-membership-azure-portal

**Quick Preview:**

Question 4: Skipped
You have the Azure management groups shown in the following table:
Larger image

You add Azure subscriptions to the management groups as shown in the following table:
Larger image

You create the Azure policies shown in the following table:
Larger image

Please evaluate the following statement if it's `True` or `False`:

You can create a virtual network in Subscription1.

- ○ True
- ○ False (Correct)

**Explanation**
First, let's have a complete view over the setup:

Azure Policy establishes conventions for resources. Policy definitions describe resource compliance conditions and the effect to take if a condition is met. In this scenario, a Policy has been applied at the Tenant Root Group and this is the ***Not Allowed Resource Types*** policy, which restricts creating any virtual networks.

Where does this policy apply? At what level or scope in the Azure hierarchy? Once the policy is applied at the Tenant Root Group,  so this is the assignment, the policy assignment is inherited by all child resources. If a policy assignment is applied to a resource group, it's applicable to all the resources in that resource group. In this case, being applied at ROOT level, it's inherited by all child resources: management groups, subscriptions, resource groups and resources.

It really doesn't matter that the ***Allowed Resource Types*** policy is applied on Management Group 12, it has no effect. The most restrictive policy always wins, so a virtual network deployment is not allowed anywhere in the presented Azure hierarchy.

So now, the statement to evaluate: ***You can create a virtual network in Subscription1***. This action will be denied, so the statement is False. The error in Azure portal would look like this:

**Reference:**

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

**Quick Preview:**

Question 5: Skipped
You have the Azure management groups shown in the following table:

Larger image

You add Azure subscriptions to the management groups as shown in the following table:

Larger image

You create the Azure policies shown in the following table:

Larger image

Please evaluate the following statement if it's `True` or `False`:

You can create a virtual machine in Subscription2.

- ○ True
- ○ False (Correct)

**Explanation**
First, let's have a complete view over the setup:

Azure Policy establishes conventions for resources. Policy definitions describe resource compliance conditions and the effect to take if a condition is met. In this scenario, a Policy has been applied at the Tenant Root Group and this is the ***Not Allowed Resource Types*** policy, which restricts creating any virtual networks.

Where does this policy apply? At what level or scope in the Azure hierarchy? Once the policy is applied at the Tenant Root Group,  so this is the assignment, the policy assignment is inherited by all child resources. If a policy assignment is applied to a resource group, it's applicable to all the resources in that resource group. In this case, being applied at ROOT level, it's inherited by all child resources: management groups, subscriptions, resource groups and resources.

But we have to be careful with the ***Allowed Resource Types*** policy applied on Management Group 12, because when we setup an Allowed Resource Types policy, **all the resources not specifically allowed, in the policy, are denied**.

Therefore, this policy associated to ManagementGroup12, is not allowing creation of Virtual Networks, because the policy applied at Tenant Root Group level is more restrictive, and **the most restrictive policy always wins**. But still, this policy associated to ManagementGroup12 will generate an implicit deny to all other resources different from Virtual Networks.

The result of both policies combined is that we cannot create resources of any type in ManagementGroup12.

So now, the statement to evaluate: ***You can create a virtual machine in Subscription2*** is **False** as Subscription2 is part of ManagementGroup12, and we cannot create resources of any type in ManagementGroup12.

**Reference:**

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

**Quick Preview:**

Question 6: Skipped

You have the Azure management groups shown in the following table:

Larger image

You add Azure subscriptions to the management groups as shown in the following table:

Larger image

You create the Azure policies shown in the following table:

Larger image

Please evaluate the following statement if it's `True` or `False`:

You can add Subscription1 to ManagementGroup11.

- ○ True (Correct)
- ○

False

**Explanation**
First, let's have a complete view over the setup:

Azure Policy establishes conventions for resources. Policy definitions describe resource compliance conditions and the effect to take if a condition is met. In this scenario, a Policy has been applied at the Tenant Root Group and this is the ***Not Allowed Resource Types*** policy, which restricts creating any virtual networks.

Where does this policy apply? At what level or scope in the Azure hierarchy? Once the policy is applied at the Tenant Root Group,  so this is the assignment, the policy assignment is inherited by all child resources. If a policy assignment is applied to a resource group, it's applicable to all the resources in that resource group. In this case, being applied at ROOT level, it's inherited by all child resources: management groups, subscriptions, resource groups and resources.

It really doesn't matter that the ***Allowed Resource Types*** policy is applied on Management Group 12, it has no effect. The most restrictive policy always wins, so a virtual network deployment is not allowed anywhere in the presented Azure hierarchy.

So now, the statement to evaluate: ***You can add Subscription1 to ManagementGroup11.***

**Yes, this is possible**. You can navigate to ManagementGroup11 and then select ***Add subscription.*** Subscription 1 is currently a child resource of ManagementGroup21, so by adding Subscription 1 to ManagementGroup11, you are actually moving Subscription 1 between the two management groups. So again, ***yes, you can add Subscription 1 to ManagementGroup11, by actually moving the subscription between the two management groups.***

Any resource in Azure has only one parent scope, so Subscription 1 can't be a child resource to both management groups.

**Reference:**

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

**Quick Preview:**

Question 7: Skipped

You plan to assign the following Azure policy definition, as shown in the following exhibits:

Larger image

Larger image

Larger image

What is the effect of the policy?

- ○ You are prevented from creating Azure SQL servers anywhere in X-A-A-S subscription
- ○ You can create Azure SQL servers in RG-01 resource group only (Correct)
- ○ You are prevented from creating Azure SQL Servers in RG-01 resource group only
- ○ You can create Azure SQL servers in any resource group within X-A-A-S subscription

**Explanation**

The policy definition ***Not allowed resource types*** is applied at the X-A-A-S subscription scope, so this means it applies to all child resources, so all resource groups included in X-A-A-S subscription.

What resources are users denied to create? ***Microsoft SQL servers !***

Also, ***Exclusions*** are also included in the policy definition. This means that the policy is applied for entire X-A-A-S subscription, except for RG-01 resource group.

The end result is that you can create Azure SQL servers in RG-01 resource group only.

**Reference:**

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

**Quick Preview:**

Question 8: Skipped

You have an Azure subscription that contains the resources shown in the following table:
Larger image

You assign a policy to RG6 as shown in the following table:
Larger image

To RG6, you apply the tag: RGroup: RG6.

Which tags apply to VNET1 ?

- ○ None
- ○ Department: D1 only (Correct)
- ○ Department: D1 and RGroup: RG6 only
- ○ Department: D1 and Label:Value1 only
- ○ Department: D1, RGroup: RG6 and Label:Value1

**Explanation**
vNET1 is already part of RG6 resource group. The Policy applied to RG6 will not automatically add the tag to the existing resources in the scope. In order to add a tag to existing resources, you would need to run a Remediation task. Also, tags are not inherited from the resource group parent scope.

As a result, in this scenario vNET1 will have only the Department:D1 tag attached.

**Reference:**

https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

**Quick Preview:**

Question 9: Skipped

You have an Azure subscription that contains the resources shown in the following table:
Larger image

You assign a policy to RG6 as shown in the following table:
Larger image

To RG6, you apply the tag: RGroup: RG6. You deploy a virtual network named VNET2 to RG6.

Which tags apply to VNET2?

- ○ None
- ○ RGroup:R6 only
- ○ Label:Value1 only (Correct)
- ○ RGroup:R6 and Label:Value1

**Explanation**
First thing to keep in mind is that tags are not inherited by resources from the resource group parent scope. So this means that when deploying VNET2, the virtual network will not inherit RGroup:RG6 label from RG6 resource group.

The policy assigned to RG6 will attach ***Label:Value1*** label to all newly created resources in RG6. As a result of this policy assignment, Label:Value1 will be attached to VNET2.

The policy definition ***Apply tag and its default value*** presented in this scenario is a custom policy, as this policy definition is not a built-on policy. You can take a look at the available built-in policies by following the URL below. Because it's not a built-in policy and in order to avoid any other assumptions, please consider the actions performed by the policy as the policy name suggests.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies

**Quick Preview:**

Question 10: Skipped
You recently created a new Azure subscription that contains a user named Admin1.

Admin1 attempts to deploy an Azure Marketplace resource by using an Azure Resource Manager template. Admin1 deploys the template by using Azure PowerShell and receives the following error message:

“User failed validation to purchase resources. Error message: Legal terms have not been accepted for this item on this subscription. To accept legal terms, please go to the Azure portal (http://go.microsoft.com/fwlink/? LinkId=534873) and configure programmatic deployment for the Marketplace item or create it there for the first time.”

You need to ensure that Admin1 can deploy the Marketplace resource successfully. What should you do?

- ○ From Azure PowerShell, run the Set-AzApiManagementSubscription cmd
- ○ From the Azure portal, register the Microsoft.Marketplace resource provider
- ○ From Azure PowerShell, run the Set-AzMarketplaceTerms cmd (Correct)
- ○ From the Azure portal, assign the Billing administrator role to Admin1

**Explanation**
The ***Set-AzMarketplaceTerms*** cmdlet saves the terms object for given publisher id(Publisher), offer id(Product) and plan id(Name) tuple.

**Reference:**

https://docs.microsoft.com/en-us/powershell/module/Az.MarketplaceOrdering/Set-AzMarketplaceTerms?view=azps-5.0.0&viewFallbackFrom=azps-4.6.0

**Quick Preview:**

Question 11: Skipped
You have an Azure subscription named X-A-A-S-Primary that contains the resources shown in the following table:
Larger image

You create a new Azure subscription named X-A-A-S-Secondary and want to move all existing resources to this new subscription.

Which of the resources can be moved to X-A-A-S-Secondary subscription?

- ○
  VM1, Storage1, VNET1, and VM1Managed only
- ○
  VM1 and VM1Managed only
- ○
  VM1, Storage1, VNET1, VM1Managed, and RVAULT1
  (Correct)
- ○
  RVAULT1 only

**Explanation**
You can move a VM and its associated resources to a different subscription by using the Azure portal. You can also move an Azure Site Recovery (ASR) Vault to either a new resource group within the current subscription or to a new subscription.

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/backup-azure-move-recovery-services-vault?toc=/azure/azure-resource-manager/toc.json

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources#microsoftrecoveryservices

**Quick Preview:**

Question 12: Skipped
You have an on-premises server that contains a folder named ***D:\Important_Data***.

You need to copy the contents of ***D:\Important_Data*** to the ***public*** container in an Azure Storage account named ***az104data***.

Which command should you run?

- ○
  https://az104data.blob.core.windows.net/public
- ○
  azcopy sync D:\Important_Data https://az104data.blob.core.windows.net/public --snapshot
- ○
  azcopy copy D:\Important_Data https://az104data.blob.core.windows.net/public --recursive
  (Correct)

- ○ az storage blob copy start-batch D:\Important_Data https://az104data.blob.core.windows.net/public

**Explanation**

The ***azcopy copy*** command copies a directory (and all of the files in that directory) to a blob container. The result is a directory in the container by the same name.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-blobs

**Quick Preview:**

Question 13: Skipped

You have an Azure subscription named X-A-A-S-Primary that contains the storage accounts displayed in the following table:

Larger image

You want to use the Azure Import/Export service to export data from X-A-A-S-Primary subscription.

Which storage account can be used to export the data?

- ○ Storage1
- ○ Storage2
- ○ Storage3
- ○ Storage4 (Correct)

**Explanation**

Azure Import/Export service supports the following of storage accounts:

- Standard General Purpose v2 storage accounts (recommended for most scenarios)

- Blob Storage accounts

- General Purpose v1 storage accounts (both Classic or Azure Resource Manager deployments),

Azure Import/Export service supports the following storage types:

- Import supports Azure Blob storage and Azure File storage

- Export supports Azure Blob storage

**Reference:**

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

**Quick Preview:**

Question 14: Skipped

You have Azure Storage accounts as shown in the following exhibit:

Larger image

You can use .......... for Azure Table Storage.

Please select the answer choice that completes the above statement correctly.

- ○ only storageaccount1az104
- ○ only storageaccount2az104
- ○ only storageaccount3az104
- ○ storageaccount1az104 and storageaccount2az104 **(Correct)**
- ○ storageaccount2az104 and storageaccount3az104

**Explanation**

Azure Table Storage storage service is supported only by General-purpose V2 and General-purpose V1 storage account types.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview

**Quick Preview:**

Question 15: Skipped

You have Azure Storage accounts as shown in the following exhibit:
Larger image

You can use .......... for Azure Blob Storage.

Please select the answer choice that completes the above statement correctly.

- ○
  storageaccount3az104
- ○
  storageaccount2az104 and storageaccount3az104
- ○
  storageaccount1az104 and storageaccount3az104
- ○
  all storage accounts
  (Correct)

**Explanation**
Azure Blob Storage storage service is supported by almost all storage account types:

- General-purpose V2

- General-purpose V1

- BlobStorage

- BlockBlobStorage

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview

**Quick Preview:**

Question 16: Skipped
You are using an Azure subscription with data deployed in the following Azure services:
Larger image

You plan to export data by using Azure Import/Export job named DataExport.

Which data can be exported by using DataExport?

- ○ DB1
- ○ Container1 (Correct)
- ○ Share1
- ○ Table1

**Explanation**

Azure Import/Export service supports the following storage types:

- Import supports Azure Blob storage and Azure File storage

- Export supports Azure Blob storage

**Reference:**

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

**Quick Preview:**

Question 17: Skipped

You have an Azure Storage account named MyStorageAccount.

You have deployed and Azure App Service app named App-01 and an app named App-02 that runs in an Azure container instance. Each app uses a managed identity.

You need to ensure that App-01 and App-02 can read blobs from MyStorageAccount. The solution must meet the following requirements:

- Minimize the number of secrets used.

- Ensure that App-02 can only read from MyStorageAccount for the next 30 days.

What should you configure in MyStorageAccount for App-01?

- ○ Access keys
- ○

Advanced security

- ○
  Access control (IAM)
  (Correct)
- ○
  Shared access signatures (SAS)

**Explanation**

Each App uses a managed identity, and for App1 the requirements are "***read Blobs and minimize the use of secrets***".

Blobs and Queues support Azure AD with managed identities for Azure resources, therefore the use of IAM, fully apply to App1, without using any secret.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-auth-aad-msi

**Quick Preview:**

Question 18: Skipped

You have an Azure Storage account named MyStorageAccount.

You have deployed and Azure App Service app named App-01 and an app named App-02 that runs in an Azure container instance. Each app uses a managed identity.

You need to ensure that App-01 and App-02 can read blobs from MyStorageAccount. The solution must meet the following requirements:

- Minimize the number of secrets used.

- Ensure that App-02 can only read from MyStorageAccount for the next 30 days.

What should you configure in MyStorageAccount for App-02?

- ○
  Access keys
- ○
  Advanced security
- ○
  Access control (IAM)
- ○
  Shared access signatures (SAS)
  (Correct)

**Explanation**

A shared access signature (SAS) provides secure delegated access to resources in your storage account without compromising the security of your data. With a SAS, you have granular control over how a client can access your data.

You can control what resources the client may access, what permissions they have on those resources, and how long the SAS is valid, among other parameters.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

**Quick Preview:**

Question 19: Skipped

You have an Azure subscription named Dev-Test-Sub that is used by several departments at your company. Dev-Test-Sub contains the resources in the following table:

Larger image

Another administrator deploys a virtual machine named VM-01 and an Azure Storage account named Storage-02 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?

- ○ VM-01
- ○ RG1 (Correct)
- ○ Storage-02
- ○ Container1

**Explanation**

Deployment history is available starting from the resource group ***Overview*** page:

After you select ***Deployments***, you can see a list of your last deployed resources.

After you select the deployment, you can examine the template that was used to deploy the Azure resources, by selecting ***Template*** from the resource's menu:

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deployment-history?tabs=azure-portal

**Quick Preview:**

Question 20: Skipped

You have an Azure web app named App-01. App-01 has the deployment slots shown in the following table:

Larger image

In Webapp-01-Test, you test several changes to App-01. You back up App-01. You swap Webapp-01-Test for Webapp-01-Prod and discover that App-01 is experiencing performance issues.

You need to revert to the previous version of App-01 as quickly as possible. What should you do?

- ○ Redeploy App-01
- ○ Swap the slots (Correct)
- ○ Clone App-01
- ○ Restore the backup of App-01

**Explanation**

When you swap deployment slots, Azure swaps the Virtual IP addresses of the source and destination slots, thereby swapping the URLs of the slots. We can easily revert the deployment by swapping back.

**Reference:**

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

**Quick Preview:**

Question 21: Skipped
You have an Azure subscription named New-Subscription. New-Subscription contains two Azure virtual machines VM-01 and VM-02. VM-01 and VM-02 run Windows Server 2016. VM-01 is backed up daily by Azure Backup without using the Azure Backup agent.

VM-01 data has been compromised by a Ransomware attack, that encrypted all the data. VM-01 is not working, you need to restore the latest backup of VM-01.

To which location can you restore the backup?

You can perform a file recovery of VM-01 to ........... .

Please select the answer that completes the statement correctly.

- ○
  VM-01 only
- ○
  VM-02 only
  (Correct)
- ○
  VM-01 or a new Azure virtual machine only
- ○
  VM-01 and VM-02
- ○
  A new Azure virtual machine only
- ○
  Any Windows computer that has Internet connectivity

**Explanation**
When recovering files, you can't restore files to a previous or future operating system version. For example, you can't restore a file from a Windows Server 2016 VM to Windows Server 2012 or a Windows 8 computer. You can restore files from a VM to the same server operating system, or to the compatible client operating system. ***This clarifies why VM-02 is the valid option.***

Why is not VM-01 a valid answer as well ?

VM-01 has been compromised by a Ransomware attack that encrypted all the data, and in order to perform a file recovery we would need access at VM-01 level, which is not available. Data has been encrypted on VM-01, so we can't access VM-01 in order to perform the file recovery.

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/backup-azure-restore-files-from-vm

**Quick Preview:**

Question 22: Skipped

You have an Azure subscription named New-Subscription. New-Subscription contains two Azure virtual machines VM-01 and VM-02. VM-01 and VM-02 run Windows Server 2016. VM1 is backed up daily by Azure Backup without using the Azure Backup agent.

VM-01 data has been compromised by a Ransomware attack, that encrypted all the data. You need to restore the latest backup of VM-01.

To which location can you restore the backup?

You can restore VM-01 to .......... .

Please select the answer that completes the statement correctly.

- ○ VM-01 only
- ○ VM-01 or a new Azure virtual machine only **(Correct)**
- ○ VM-01 and VM-02
- ○ Any Windows computer that has Internet connectivity

**Explanation**

You can restore VM-01 to VM-01 by replacing the current encrypted disks or by using the backup data and creating a new virtual machine.

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms

**Quick Preview:**

Question 23: Skipped

***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.***

You have an Azure virtual machine named VM1 that runs Windows Server 2016. You need to create an alert in Azure when more than two error events are logged to the System event log on VM1 within an hour.

***Solution:*** You create an Azure Log Analytics workspace and configure the data settings. You add the Microsoft Monitoring Agent VM extension to VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

Does this meet the goal?

- ○ Yes
- ○ No (Correct)

**Explanation**

This question is a bit tricky. The Microsoft Monitoring Agent is actually installed and NOT added to a VM.

So the full solution path would be:

You create an Azure Log Analytics workspace and configure the data settings. You ***install*** the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/azure-monitor-agent-overview?tabs=CLI1%2CCLI2

**Quick Preview:**

Question 24: Skipped

***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.***

You have an Azure virtual machine named VM1 that runs Windows Server 2016. You need to create an alert in Azure when more than two error events are logged to the System event log on VM1 within an hour.

***Solution:*** You create an Azure Log Analytics workspace and configure the data settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

Does this meet the goal?

- ○ Yes (Correct)
- ○ No

**Explanation**

Alerts in Azure Monitor can identify important information in your Log Analytics repository. They are created by alert rules that automatically run log searches at regular intervals, and if results of the log search match particular criteria, then an alert record is created and it can be configured to perform an automated response.

The Log Analytics agent collects monitoring data from the guest operating system and workloads of virtual machines in Azure, other cloud providers, and on-premises. It collects data into a Log Analytics workspace.

**References:**

https://docs.microsoft.com/en-us/azure/azure-monitor/learn/tutorial-response

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview

**Quick Preview:**

Question 25: Skipped

***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.***

You have an Azure virtual machine named VM1 that runs Windows Server 2016. You need to create an alert in Azure when more than two error events are logged to the System event log on VM1 within an hour.

***Solution:*** You create an Azure storage account and configure shared access signatures (SASs). You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the storage account as the source.

Does this meet the goal?

- ○

Yes

- ○ No (Correct)

**Explanation**
Events are not be stored in a pure storage account. Instead, you create an Azure Log Analytics workspace and configure the data settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview

**Quick Preview:**

Question 26: Skipped
***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.***

You have an Azure virtual machine named VM1 that runs Windows Server 2016. You need to create an alert in Azure when more than two error events are logged to the System event log on VM1 within an hour.

***Solution:*** You create an event subscription on VM1. You create an alert in Azure Monitor and specify VM1 as the source.

Does this meet the goal?

- ○ Yes
- ○ No (Correct)

**Explanation**
Proposed solution is not related to what needs to be implemented.

Azure Event Grid allows you to easily build applications with event-based architectures. A subscription tells Event Grid which events on a topic you're interested in receiving.

Instead, you create an Azure Log Analytics workspace and configure the data settings. You install the Microsoft Monitoring Agent on VM1. You create an alert in Azure Monitor and specify the Log Analytics workspace as the source.

**Reference:**

https://docs.microsoft.com/en-us/azure/event-grid/concepts

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview

**Quick Preview:**

Question 27: Skipped

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

Larger image

VNET1 is in RG1. VNET2 is in RG2. There is no connectivity between VNET1 and VNET2. An administrator named Admin1 creates an Azure virtual machine named VM1 in RG1. VM1 uses a disk named Disk1 and connects to VNET1. Admin1 then installs a custom application in VM1.

You need to move the custom application to VNET2. The solution must minimize administrative effort.

Which two actions should you perform? (SELECT TWO)

- □ First action: Create a network interface in RG2
- □ First action: Detach a network interface
- □ First action: Delete VM1 (Correct)
- □ First action: Move a network interface to RG2
- □ Second action: Attach a network interface
- □ Second action: Create a network interface in RG2
- □

Second action: Create a new virtual machine
(Correct)

- □
Second action: Move VM1 to RG2

**Explanation**
We cannot just move a virtual machine between networks. What we need to do is identify the disk used by VM1, delete the VM1 itself while retaining the disk, and recreate the VM in the target virtual network - VNET2 and then attach the original disk to it.

Although it may seem easier to create a network interface in RG2, detach the NIC card or move the NIC card to RG2, that's not a solution. Why? If you are thinking of attaching a new network interface card to VM1, and the new NIC card to be deployed in VNET2, this is not possible. You can attach a new NIC card to VM1, but the new NIC card has to be in the same VNET, so VNET1.

**Reference:**

https://docs.microsoft.com/en-us/archive/blogs/canitpro/step-by-step-move-a-vm-to-a-different-vnet-on-azure

**Quick Preview:**

Question 28: Skipped
You download an Azure Resource Manager template based on an existing virtual machine. The template will be used to deploy 100 virtual machines.

You need to modify the template to reference an administrative password. You must prevent the password from being stored in plain text.

What should you create to store the password?

- ○
an Azure Key Vault and an access policy
(Correct)
- ○
an Azure Storage account and an access policy
- ○
a Recovery Services vault and a backup policy
- ○
Azure Active Directory (AD) Identity Protection and an Azure policy

**Explanation**

You can use a template that allows you to deploy a simple Windows VM by retrieving the password that is stored in a Key Vault. Therefore, the password is never put in plain text in the template parameter file.

**Reference:**

https://azure.microsoft.com/en-us/resources/templates/101-vm-secure-password/

https://docs.microsoft.com/en-us/azure/key-vault/general/overview

**Quick Preview:**

Question 29: Skipped

You have the App Service plans shown in the following table:
Larger image

You plan to create the Azure web apps shown in the following table:
Larger image

You need to identify which App Service plans can be used for the web apps.

What should you identify? (SELECT TWO)

- □ WebApp 1 - ASP1 only
- □ WebApp 1 - ASP3 only
- □ WebApp 1 - ASP1 and ASP2 only
- □ WebApp 1 - ASP1 and ASP3 only (Correct)
- □ WebApp 1 - ASP1, ASP2 and ASP3
- □ WebApp 2 - ASP1 only (Correct)
- □ WebApp 2 - ASP3 only
- □ WebApp 2 - ASP1 and ASP2 only

- □ WebApp 2 - ASP1 and ASP3 only
- □ WebApp 2 - ASP1, ASP2 and ASP3

**Explanation**

The WebApp and the App Service Plan need to be in the same region. .NET Core apps (or ASP NET Core apps) can run on both Windows or Linux environments, so the answer for WebApp1 is ASP1 and ASP3.

For WebApp2, we have ASP1 and ASP3 as a first choice, because of location restriction. Again, webapp and App Service Plan need to exist in the same Azure region. But ASP.NET apps can be hosted on Windows only, so this results in only ASP1 App Service Plan option for WebApp2.

**Reference:**

https://docs.microsoft.com/en-us/azure/app-service/app-service-plan-manage

https://docs.microsoft.com/en-us/azure/app-service/quickstart-dotnetcore?pivots=platform-linux

https://docs.microsoft.com/en-us/azure/app-service/quickstart-dotnet-framework

**Quick Preview:**

Question 30: Skipped

You have the following peerings configured for vNET6, as shown in the following exhibit:

Larger image

Hosts on vNET6 can communicate with hosts on ........... .

Please select the option that completes the statement successfully.

- ○ vNET6 only (Correct)
- ○ vNET6 and vNET1 only
- ○ vNET6, vNET1 and vNET2 only
- ○ all the virtual networks in the subscription

**Explanation**
Peering status to both vNET1 and vNET2 is disconnected, hosts on vNET6 can communicate only to hosts on vNET6.

**Further learning:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

**Quick Preview:**

Question 31: Skipped
You have the following peerings configured for vNET6, as shown in the following exhibit:
Larger image

To change the status of the peering connection to vNET1 to ***Connected***, you must first .......... .

Please select the option that completes the statement successfully.

- ○ add a service endpoint
- ○ add a subnet
- ○ delete peering1 **(Correct)**
- ○ modify the address space

**Explanation**
If the peering status is ***Disconnected***, you need to delete the peering from both virtual networks and then recreate them.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-troubleshoot-peering-issues

**Quick Preview:**

Question 32: Skipped

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?

- ○ IP flow verify
- ○ Connection troubleshoot
- ○ Connection monitor (Correct)
- ○ NSG flow logs

**Explanation**
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.

**Incorrect Answers:**

A: The IP flow verify capability enables you to specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound). IP flow verify then tests the communication and informs you if the connection succeeds or fails. If the connection fails, IP flow verify tells you which security rule allowed or denied the communication, so that you can resolve the problem.

B: The connection troubleshoot capability enables you to test a connection between a VM and another VM, an FQDN, a URI, or an IPv4 address. The test returns similar information returned when using the connection monitor capability, but tests the connection at a point in time, rather than monitoring it over time, as connection monitor does.

D: The NSG flow log capability allows you to log the source and destination IP address, port, protocol, and whether traffic was allowed or denied by an NSG.

**Reference:**

https://docs.microsoft.com/en-us/azure/network-watcher/connection-monitor

**Quick Preview:**

Question 33: Skipped

You have an Azure subscription that contains a policy-based virtual network gateway named GW1 and a virtual network named VNet1. You need to ensure that you can configure a point-to-site connection from an on-premises computer to VNet1.

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

- □ Add a service endpoint to VNet1
- □ Reset GW1
- □ Create a route-based virtual network gateway (Correct)
- □ Add a connection to GW1
- □ Delete GW1 (Correct)
- □ Add a public IP address space to VNet1

**Explanation**

In order to deploy a point-to-site VPN, a Route-Based VPN gateway needs to be used. Point-to-site VPN types can't be deployed using policy-based virtual network gateways. For this reason, you would need to first delete existing virtual network gateway and create a new one, route-based type.

**Reference:**

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal

**Quick Preview:**

Question 34: Skipped

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

Larger image

In Azure, you create a private DNS zone named az104exam.com. You set the registration virtual network to VNET2.

The az104exam.com zone is configured as shown in the following exhibit:

Larger image

`True` or `False`.

The A record for VM5 will be registered automatically in the az104exam.com zone.

- ○ True
- ○ False (Correct)

**Explanation**
Azure DNS provides automatic registration of virtual machines from a single virtual network that's linked to a private zone as a registration virtual network. VM5 does not belong to the registration virtual network though, only VM6 does (an A record for VM6 will be registered automatically in the az104exam.com zone). For this reason, the statement is False.

**Reference:**

https://docs.microsoft.com/en-us/azure/dns/private-dns-overview

**Quick Preview:**

Question 35: Skipped
You have an Azure subscription that contains the resources in the following table:
Larger image

In Azure, you create a private DNS zone named az104exam.com. You set the registration virtual network to VNET2.

The az104exam.com zone is configured as shown in the following exhibit:

Larger image

`True` or `False`.

VM5 can resolve VM9.az104exam.com.

- ○ True

- ○ False (Correct)

**Explanation**
Forward DNS resolution is supported across virtual networks that are linked to the private zone as resolution virtual networks. VM5 does not belong to a resolution virtual network, only VM6. So VM6 will be able to resolve VM9.az104exam.com, but not VM5.

**Reference:**

https://docs.microsoft.com/en-us/azure/dns/private-dns-overview

**Quick Preview:**

Question 36: Skipped
You have an Azure subscription that contains the resources in the following table:
Larger image

In Azure, you create a private DNS zone named az104exam.com. You set the registration virtual network to VNET2.

The az104exam.com zone is configured as shown in the following exhibit:

Larger image

`True` or `False`.

VM6 can resolve VM9.az104exam.com.

- ○ True (Correct)
- ○ False

**Explanation**
VM6 belongs to registration virtual network, and an A (Host) record exists for VM9 in the DNS zone. By default, registration virtual networks also act as resolution virtual networks, in the sense that DNS resolution against the zone works from any of the virtual machines within the registration virtual network.

**Reference:**

https://docs.microsoft.com/en-us/azure/dns/private-dns-overview

**Quick Preview:**

Question 37: Skipped

You have an Azure subscription that contains a virtual network named VNet1. VNet1 uses an IP address space of 10.0.0.0/16 and contains the subnets in the following table:

Larger image

Subnet1 contains a virtual appliance named VM1 that operates as a router. You create a routing table named RT1. You need to route all inbound traffic from the VPN gateway to VNet1 through VM1.

How should you configure RT1? To answer, select the appropriate options in the below answer area. (SELECT THREE)

- □ Address prefix - 10.0.0.0/16 (Correct)
- □ Address prefix - 10.0.1.0/24
- □ Address prefix - 10.0.254.0/24
- □ Next hop type - Virtual appliance (Correct)
- □ Next hop type - Virtual network
- □ Next hop type - Virtual network gateway
- □ Assigned to - GatewaySubnet (Correct)
- □ Assigned to - Subnet0
- □ Assigned to - Subnet1 and Subnet2

**Explanation**

Implicitly mentioned, or just indicated by the name "Gateway Subnet") ---- All the incoming traffic to VNet1 goes through the "Gateway Subnet". Therefore, to control the traffic, a Routing Table needs to be assigned to the "Gateway Subnet".

All the traffic needs to be controlled by the Network Virtual Appliance (NVA). Therefore, the next hop is "Virtual Appliance" (when deploying, also putting in its IP).

The NVA needs to control the traffic for ALL Virtual Network (VNet1). Therefore, the (target) Address Prefix needs to be the entire Address Range for the VNet1.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

Question 38: Skipped
You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines. You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- ○ Floating IP (direct server return) to **Enabled**
- ○ Floating IP (direct server return) to **Disabled**
- ○ a health probe
- ○ Session persistence to **Client IP and Protocol** **(Correct)**

**Explanation**
With Sticky Sessions (or source IP affinity) when a client starts a session on one of your web servers, session stays on that specific server. To configure An Azure Load-Balancer For Sticky Sessions set Session persistence to Client IP.

**Reference:**

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-distribution-mode

**Quick Preview:**

Question 39: Skipped

You have an Azure subscription that contains the virtual machines shown in the following table:

Larger image

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 Subnet1. NSG2 is associated to the network interface of VM2.

Please evaluate if the following statement is `True` or `False`.

From the Internet, you can connect to VM1 using Remote Desktop.

- ○ True
- ○ False (Correct)

**Explanation**

VM1 is part of Subnet1 and NSG1 is applied at Subnet1 scope. NSG1 is using default inbound rules, which don't allow RDP traffic. In order to allow RDP traffic, a custom inbound rule needs to be added.

**Reference:**

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

**Quick Preview:**

Question 40: Skipped
You have an Azure subscription that contains the virtual machines shown in the following table:
Larger image

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 Subnet1. NSG2 is associated to the network interface of VM2.

Please evaluate if the following statement is `True` or `False`.

From the Internet, you can connect to VM2 using Remote Desktop.

- ○ True (Correct)
- ○ False

**Explanation**

VM2 is part of Subnet2 and NSG2 is applied at Subnet2 scope. NSG2 is using default inbound rules and a custom inbound rule has been added as well. The custom inbound rule actually allows RDP traffic inbound, so you will be able to RDP to VM2.

NSG2 looks similar to the following network security group:

**Reference:**

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

**Quick Preview:**

Question 41: Skipped

You have an Azure subscription that contains the virtual machines shown in the following table:

Larger image

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 Subnet1. NSG2 is associated to the network interface of VM2.

Please evaluate if the following statement is `True` or `False`.

From VM1, you can connect to VM2 by using Remote Desktop.

- ○ True (Correct)
- ○ False

**Explanation**

VM1 and VM2 are deployed in the same VNET and traffic inside a VNET is permitted by the first rule declared in the default inbound port rules. This results in the statement being True.

**Reference:**

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

**Quick Preview:**

Question 42: Skipped

You have a virtual network named VNET1 that contains the subnets shown in the following table:

Larger image

You have three Azure virtual machines that have the network configurations shown in the following table:

Larger image

For NSG1, you create the inbound security rule shown in the following table:

Larger image

For NSG2, you create the inbound security rule shown in the following table:

Larger image

Please evaluate if the following statement is `True` or `False`.

VM2 can connect to TCP port 1433 services on VM1.

- ○ True
- ○ False (Correct)

**Explanation**

TCP 1433 traffic originated from VM2 and going to VM1 is first evaluated by NSG1, applied at Subnet1 scope. NSG1 allows the traffic, so the traffic will next be evaluated by NSG2. NSG2 denies the traffic, so the statement is False.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works

**Quick Preview:**

Question 43: Skipped

You have a virtual network named VNET1 that contains the subnets shown in the following table:

Larger image

You have three Azure virtual machines that have the network configurations shown in the following table:

Larger image

For NSG1, you create the inbound security rule shown in the following table:

Larger image

For NSG2, you create the inbound security rule shown in the following table:

Larger image

Please evaluate if the following statement is `True` or `False`.

VM1 can connect to the TCP port 1433 services on VM2.

- ○ True (Correct)
- ○ False

**Explanation**

Traffic from VM1 going to VM2 would first be evaluated by an NSG applied at Subnet2 scope, because VM2 is attached to Subnet2. But these is no NSG applied at Subnet2, so traffic should then be evaluated by any NSG applied at VM2. No NSG is applied at VM2, so traffic can arrive at VM2.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works

**Quick Preview:**

Question 44: Skipped

You have a virtual network named VNET1 that contains the subnets shown in the following table:

Larger image

You have three Azure virtual machines that have the network configurations shown in the following table:

Larger image

For NSG1, you create the inbound security rule shown in the following table:

Larger image

For NSG2, you create the inbound security rule shown in the following table:

Larger image

Please evaluate if the following statement is `True` or `False`.

VM2 can connect to the TCP port 1433 service on VM3.

- ○ True (Correct)
- ○ False

**Explanation**

VM3 is attached to Subnet2.

No NSG is applied at either Subnet2 or VM3 scope, so traffic is allowed and the statement is true.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works

**Quick Preview:**

Question 45: Skipped

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

Larger image

You have a Recovery Services vault that protects VM1 and VM2. You need to protect VM3 and VM4 by using Recovery Services.

What should you do first?

- ○ Create a new Recovery Services vault (Correct)
- ○ Create a storage account
- ○ Configure the extensions for VM3 and VM4
- ○

Create a new backup policy

**Explanation**

The Recovery Services vault must be deployed in the same region where the VM that you want to protect is deployed. For this example, a new Recovery Services vault must be created in North Europe region.

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/backup-create-rs-vault

**Quick Preview:**

Question 46: Skipped

***Case study***

***This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.***

***To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.***

***Overview***

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market. Contoso products are manufactured by using blueprint files that the company authors and maintains.

***Existing Environment***

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

- File servers

- Domain controllers

- Microsoft SQL Server servers

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

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

- A SQL database

- A web front end

- A processing middle tier

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

***Requirements***

***Planned Changes***

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.

- Move the existing product blueprint files to Azure Blob storage.

- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

***Technical Requirements***

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.

- Minimize the number of open ports between the App1 tiers.

- Ensure that all the virtual machines for App1 are protected by backups.

- Copy the blueprint files to Azure over the Internet.

- Ensure that the blueprint files are stored in the archive storage tier.

- Ensure that partner access to the blueprint files is secured and temporary.

- Prevent user passwords or hashes of passwords from being stored in Azure.

- Use unmanaged standard storage for the hard disks of the virtual machines.

- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

- Minimize administrative effort whenever possible.

***User Requirements***

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.

- Designate a new user named Admin1 as the service admin for the Azure subscription.

- Admin1 must receive email alerts regarding service outages.

- Ensure that a new user named User3 can create network objects for the Azure subscription.

**QUESTION 1**

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

- ○ a recovery plan
- ○ an Azure Backup Server
- ○ a backup policy
- ○ a Recovery Services vault **(Correct)**

**Explanation**
A Recovery Services vault is a logical container that stores the backup data for each protected resource, such as Azure VMs. When the backup job for a protected resource runs, it creates a recovery point inside the Recovery Services vault.

**From the Scenario:**

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.

- Minimize the number of open ports between the App1 tiers.

- Ensure that all the virtual machines for App1 are protected by backups.

Question 47: Skipped
***Case study***

***This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.***

***To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.***

***Overview***

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market. Contoso products are manufactured by using blueprint files that the company authors and maintains.

***Existing Environment***

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

- File servers

- Domain controllers

- Microsoft SQL Server servers

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

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

- A SQL database

- A web front end

- A processing middle tier

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

***Requirements***

***Planned Changes***

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.

- Move the existing product blueprint files to Azure Blob storage.

- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

***Technical Requirements***

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.

- Minimize the number of open ports between the App1 tiers.

- Ensure that all the virtual machines for App1 are protected by backups.

- Copy the blueprint files to Azure over the Internet.

- Ensure that the blueprint files are stored in the archive storage tier.

- Ensure that partner access to the blueprint files is secured and temporary.

- Prevent user passwords or hashes of passwords from being stored in Azure.

- Use unmanaged standard storage for the hard disks of the virtual machines.

- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

- Minimize administrative effort whenever possible.

***User Requirements***

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.

- Designate a new user named Admin1 as the service admin for the Azure subscription.

- Admin1 must receive email alerts regarding service outages.

- Ensure that a new user named User3 can create network objects for the Azure subscription.

**QUESTION 2**

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

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

**Explanation**

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

**From the Scenario:**

Planned Changes include: move the existing product blueprint files to Azure Blob storage.

Technical Requirements include: Copy the blueprint files to Azure over the Internet.

Question 48: Skipped

***Case study***

***This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.***

***To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.***

### *Overview*

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market. Contoso products are manufactured by using blueprint files that the company authors and maintains.

### *Existing Environment*

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

- File servers

- Domain controllers

- Microsoft SQL Server servers

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

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

- A SQL database

- A web front end

- A processing middle tier

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

### *Requirements*

### *Planned Changes*

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.

- Move the existing product blueprint files to Azure Blob storage.

- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

### *Technical Requirements*

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.

- Minimize the number of open ports between the App1 tiers.

- Ensure that all the virtual machines for App1 are protected by backups.

- Copy the blueprint files to Azure over the Internet.

- Ensure that the blueprint files are stored in the archive storage tier.

- Ensure that partner access to the blueprint files is secured and temporary.

- Prevent user passwords or hashes of passwords from being stored in Azure.

- Use unmanaged standard storage for the hard disks of the virtual machines.

- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

- Minimize administrative effort whenever possible.

***User Requirements***

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.

- Designate a new user named Admin1 as the service admin for the Azure subscription.

- Admin1 must receive email alerts regarding service outages.

- Ensure that a new user named User3 can create network objects for the Azure subscription.

**QUESTION 3 - `True` or `False`**

Contose requires a storage account that supports blob storage.

- ○ True (Correct)
- ○

False

**Explanation**
**From the Scenario:**

Contoso is moving the existing product blueprint files to **Azure Blob storage**.

Use unmanaged standard storage for the hard disks of the virtual machines. We use Page Blobs for these.

Question 49: Skipped
***Case study***

***This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.***

***To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.***

***Overview***

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market. Contoso products are manufactured by using blueprint files that the company authors and maintains.

***Existing Environment***

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

- File servers

- Domain controllers

- Microsoft SQL Server servers

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

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

- A SQL database

- A web front end

- A processing middle tier

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

***Requirements***

***Planned Changes***

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.

- Move the existing product blueprint files to Azure Blob storage.

- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

***Technical Requirements***

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.

- Minimize the number of open ports between the App1 tiers.

- Ensure that all the virtual machines for App1 are protected by backups.

- Copy the blueprint files to Azure over the Internet.

- Ensure that the blueprint files are stored in the archive storage tier.

- Ensure that partner access to the blueprint files is secured and temporary.

- Prevent user passwords or hashes of passwords from being stored in Azure.

- Use unmanaged standard storage for the hard disks of the virtual machines.

- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

- Minimize administrative effort whenever possible.

***User Requirements***

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.

- Designate a new user named Admin1 as the service admin for the Azure subscription.

- Admin1 must receive email alerts regarding service outages.

- Ensure that a new user named User3 can create network objects for the Azure subscription.

**QUESTION 3 - `True` or `False`**

Contose requires a storage account that supports Azure table storage.

- ○ True
- ○ False (Correct)

**Explanation**
**From the Scenario:**

Contoso is moving the existing product blueprint files to Azure Blob storage.

Ensure that the blueprint files are stored in the archive storage tier.

Use unmanaged standard storage for the hard disks of the virtual machines. We use Page Blobs for these.

Question 50: Skipped
You have an Azure DNS zone named adatum.com. You need to delegate a subdomain named research.adatum.com to a different DNS server in Azure.

What should you do?

- ○ Create an NS record named research in the adatum.com zone (Correct)
- ○ Create an PTR record named research in the adatum.com zone
- ○

Modify the SOA record of adatum.com

- ○ Create an A record named *.research in the adatum.com zone

**Explanation**

You can use the Azure portal to delegate a DNS subdomain. For example, if you own the ***adatum.com*** domain, you can delegate a subdomain called ***research*** to another, separate zone that you can administer separately from the ***adatum.com*** zone.

To delegate an Azure DNS subdomain, you must first delegate your public domain to Azure DNS, so this the ***adatum.com*** domain. Once your domain is delegated to your Azure DNS zone, you can delegate your subdomain, ***research.adatum.com***.

You would first need to create a zone for your subdomain, then note the name servers, and last to create an NS record for the new ***research.adatum.com*** subdomain (research zone).

**Reference:**

https://docs.microsoft.com/en-us/azure/dns/delegate-subdomain

**Quick Preview:**

Question 51: Skipped

You have an Azure subscription that contains the storage accounts shown in the following exhibit:

Larger image

Please select the answer choice that completes below statements, based on the information presented in the above exhibit (Select two).

You can create a premium file share in .......... .

You can use the Archive access tier in .......... .

- □ You can create a premium file share in - az104storage101 only
- □ You can create a premium file share in - az104storage104 only (Correct)
- □ You can create a premium file share in - az104storage101 and az104storage104 only
- □

You can create a premium file share in - az104storage101, az104storage102 and az104storage104 only

- □
  You can create a premium file share in - az104storage101, az104storage102, az104storage103 and az104storage104.
- □
  You can use the Archive access tier in - az104storage101 only
- □
  You can use the Archive access tier in - az104storage101 or az104storage103 only
  (Correct)
- □
  You can use the Archive access tier in - az104storage101, az104storage102 and az104storage103 only
- □
  You can use the Archive access tier in - az104storage101, az104storage102, az104storage103 and az104storage104
- □
  You can use the Archive access tier in - az104storage101, az104storage102 and az104storage104 only

**Explanation**

Azure Files offers standard file shares which are hosted on hard disk-based (HDD-based) hardware, and premium file shares, which are hosted on solid-state disk-based (SSD-based) hardware.

Azure file shares are deployed into *storage accounts*, and depending on which type of storage account you create, you can deploy Azure file shares on standard HDD hardware or premium SSD hardware.

Premium Azure file shares are available only on ***FileStorage*** Azure storage account types, so the only correct option for the first statement is ***az104storage104 only***.

Object storage data tiering between hot, cool, and archive is supported in Blob Storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts don't support tiering, nor does FileStorage storage account type.

For example, if you try to change the current tier to Archive tier for a GPv1 storage account, Azure will display the following information:

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-create-file-share?tabs=azure-portal https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers

**Quick Preview:**

Question 52: Skipped

***Case study***

***This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.***

***To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.***

***Overview***

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market. Contoso products are manufactured by using blueprint files that the company authors and maintains.

***Existing Environment***

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

- File servers

- Domain controllers

- Microsoft SQL Server servers

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

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

- A SQL database

- A web front end

- A processing middle tier

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

***Requirements***

***Planned Changes***

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.

- Move the existing product blueprint files to Azure Blob storage.

- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

***Technical Requirements***

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.

- Minimize the number of open ports between the App1 tiers.

- Ensure that all the virtual machines for App1 are protected by backups.

- Copy the blueprint files to Azure over the Internet.

- Ensure that the blueprint files are stored in the archive storage tier.

- Ensure that partner access to the blueprint files is secured and temporary.

- Prevent user passwords or hashes of passwords from being stored in Azure.

- Use unmanaged standard storage for the hard disks of the virtual machines.

- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

- Minimize administrative effort whenever possible.

***User Requirements***

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.

- Designate a new user named Admin1 as the service admin for the Azure subscription.

- Admin1 must receive email alerts regarding service outages.

- Ensure that a new user named User3 can create network objects for the Azure subscription.

**QUESTION 3 -** Please evaluate if the following statement is `True` or `False` :

Contoso requires a storage account that supports Azure File storage.

- ○ True
- ○ False (Correct)

**Explanation**
**From the Scenario:**

Contoso is moving the existing product blueprint files to Azure Blob storage.

Ensure that the blueprint files are stored in the archive storage tier.

Use unmanaged standard storage for the hard disks of the virtual machines. We use Page Blobs for these.

Question 1: Skipped
You have an Azure Active Directory (Azure AD) tenant that contains 5,000 user accounts. You create a new user account named AdminUser1.

You need to assign the User Administrator administrative role to AdminUser1.

What should you do from the user account properties?

- ○ From the Licenses blade, assign a new license
- ○ From the Directory role blade, modify the directory role (Correct)
- ○ From the Groups blade, invite the user account to a new group

**Explanation**

**Assign a role to a user**

1. Sign in to the Azure portal with an account that's a global admin or privileged role admin for the directory.

2. Select Azure Active Directory, select ***Users***, and then select a specific user from the list.

3. For the selected user, select ***Assigned roles***, select ***Add assignment***, and then pick the appropriate admin roles from the Directory roles list, such as ***User Administrator***

4. Press Select to save.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal

**Quick Preview:**

Question 2: Skipped
You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com that contains 100 user accounts.

You purchase 10 Azure AD Premium P2 licenses for the tenant.You need to ensure that 10 users can use all the Azure AD Premium features.

What should you do?

- ○ From the Licenses blade of Azure AD, assign a license (Correct)
- ○ From the Groups blade of each user, invite the users to a group
- ○ From the Azure AD domain, add an enterprise application
- ○ From the Directory role blade of each user, modify the directory role

**Explanation**
Azure AD Premium licenses need to be assigned to users (or groups of users).

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/license-users-groups

**Quick Preview:**

Question 3: Skipped
You have an Azure subscription named Subscription1 and an on-premises deployment of Microsoft System Center Service Manager.

Subscription1 contains a virtual machine named VM1. You need to ensure that an alert is set in Service Manager when the amount of available memory on VM1 is below 10 percent.

What should you do first?

- ○ Create an automation runbook
- ○ Deploy a function app
- ○ Deploy the IT Service Management Connector (ITSM) **(Correct)**
- ○ Create a notification

**Explanation**
The IT Service Management Connector (ITSMC) allows you to connect Azure and a supported IT Service Management (ITSM) product/service, such as the Microsoft System Center Service Manager.

With ITSMC, you can create work items in ITSM tool, based on your Azure alerts (metric alerts, Activity Log alerts and Log Analytics alerts).

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/itsmc-overview

**Quick Preview:**

Question 4: Skipped
You sign up for Azure Active Directory (Azure AD) Premium. You need to add a user named admin1@az104exam.com as an administrator on all the computers that will be joined to the Azure AD domain.

What should you configure in Azure AD?

- ○ Device settings from the Devices blade (Correct)
- ○ Providers from the MFA Server blade
- ○ User settings from the Users blade
- ○ General settings from the Groups blade

**Explanation**

When you connect a Windows device with Azure AD using an Azure AD join, Azure AD adds the following security principles to the local administrators group on the device:

- The Azure AD global administrator role

- The Azure AD device administrator role

- The user performing the Azure AD join

In the Azure portal, you can manage the device administrator role on the Devices page. To open the Devices page:

1. Sign in to your Azure portal as a global administrator or device administrator.

2. On the left navbar, click Azure Active Directory.

3. In the Manage section, click Devices.

4. On the Devices page, click Device settings.

5. To modify the device administrator role, configure Additional local administrators on Azure AD joined devices.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin

**Quick Preview:**

Question 5: Skipped

You have Azure Active Directory tenant named az104exam.com that includes following users:

Larger image

az104exam.com includes following Windows 10 devices:
Larger image

You create following security groups in az104exam.com:
Larger image

`True` or `False`.

User1 can add Device2 to Group1.

- ○ True
- ○ False (Correct)

**Explanation**
User1 has Cloud Device Administrator role attached, User 1 is not owner on Group1, so can't add devices.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

**Quick Preview:**

Question 6: Skipped
You have Azure Active Directory tenant named az104exam.com that includes following users:
Larger image

az104exam.com includes following Windows 10 devices:
Larger image

You create following security groups in az104exam.com:
Larger image

`True` or `False`.

User2 can add Device1 to Group1.

- ○
  True
  (Correct)
- ○
  False

**Explanation**

User2 is the owner of the "assigned group" Group1, and additionally User2 has User Administrator Role, so User2 has the appropriate role and assigned groups can be manually modified.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

Question 7: Skipped

You have Azure Active Directory tenant named az104exam.com that includes following users:

Larger image

az104exam.com includes following Windows 10 devices:

Larger image

You create following security groups in az104exam.com:

Larger image

`True` or `False`.

User2 can add Device2 to Group2.

- ○
  True
- ○
  False
  (Correct)

**Explanation**

It is "not" possible to "manually" add users/devices to a "Dynamic group".

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-create-rule

**Quick Preview:**

Question 8: Skipped

You have an Azure subscription that contains a resource group named RG26. RG26 is set to the West Europe location and is used to create temporary resources for a project. RG26 contains the resources shown in the following table:

Larger image

SQLD01 is backed up to RGV1. When the project is complete, you attempt to delete RG26 from the Azure portal. The deletion fails. You need to delete RG26.

What should you do first?

- ○ Delete VM1
- ○ Stop VM1
- ○ Stop the backup of SQLD01 **(Correct)**
- ○ Delete sa001

**Explanation**

RG26 delete will fail because of the Recovery Services vault, which will not get deleted. In order to have RGV1 deleted, you would need to first disable soft delete, stop backup and then initiate delete action.

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault

**Quick Preview:**

Question 9: Skipped

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1. VNet1 is in a resource group named RG1.

Subscription1 has a user named User1. User1 has the following roles:

- Reader

- Security Admin

- Security Reader

You need to ensure that User1 can assign the Reader role for VNet1 to other users.

What should you do?

- ○
  Remove User1 from the Security Reader role for Subscription1. Assign User1 the Contributor role for RG1.
- ○
  Assign User1 the Owner role for VNet1.
  **(Correct)**
- ○
  Remove User1 from the Security Reader and Reader roles for Subscription1.
- ○
  Assign User1 the Network Contributor role for RG1.

**Explanation**
Contributor role does not allow you to assign roles in Azure RBAC, you need to assign the Owner role.

**Reference:**

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

**Quick Preview:**

Question 10: Skipped
You have an Azure Active Directory (Azure AD) tenant named az104exam.onmicrosoft.com. Your company has a public DNS zone for x-a-a-s.com.

You add x-a-a-s.com as a custom domain name to Azure AD. You need to ensure that Azure can verify the domain name.

Which type of DNS record should you create?

- ○

MX
(Correct)

- ○ NSEC
- ○ PTR
- ○ RRSIG

**Explanation**
Both TXT and MX record types can be used for domain validation.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain

**Quick Preview:**

Question 11: Skipped

***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.***

You have an Azure 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 DevTest Labs User role to the Developers group.

Does this meet the goal?

- ○ Yes
- ○ No
(Correct)

**Explanation**
DevTest Labs User role only lets you connect, start, restart, and shutdown virtual machines in your Azure DevTest Labs.

The Logic App Contributor role lets you manage logic app, but not access to them. It provides access to view, edit, and update a logic app.

**Reference:**

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

**Quick Preview:**

Question 12: Skipped

***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.***

You have an Azure 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?

- ○ Yes
- ○ No (Correct)

**Explanation**

Logic App Operator role doesn't include the necessary permissions to create Azure Logic Apps, you would need the Logic App Contributor role.

**Reference:**

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

**Quick Preview:**

Question 13: Skipped

***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.***

You have an Azure 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 Dev, you assign the Contributor role to the Developers group.

Does this meet the goal?

- ○ Yes (Correct)
- ○ No

**Explanation**
Contributor role will allow users in Developer group to create Azure Logic Apps.

**Reference:**

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

**Quick Preview:**

Question 14: Skipped
You have an Azure subscription that is used by four departments in your company. The subscription contains 10 resource groups. Each department uses resources in several resource groups. You need to send a report to the finance department. The report must detail the costs for each department.

Which three actions should you perform in sequence?

1 - Assign a tag to each resource group

2 - Assign a tag to each resource

3 - Download the usage report

4 - From the Cost analysis blade, filter the view by tag

5 - Open the **Resource costs** blade of each resource group

- ○

2 - 4 - 3
(Correct)

- ○
  1 - 4 - 3
- ○
  5 - 4 - 3
- ○
  4 - 5 - 3

**Explanation**
***Assign a tag to each resource:***

You apply tags to your Azure resources giving metadata to logically organize them into a taxonomy. After you apply tags, you can retrieve all the resources in your subscription with that tag name and value. Each resource or resource group can have a maximum of 50 tag name/value pairs. Tags applied to the resource group are not inherited by the resources in that resource group.

***From the Cost analysis blade, filter the view by tag***

After you get your services running, regularly check how much they're costing you. You can see the current spend and burn rate in Azure portal.

1. Visit the Subscriptions blade in Azure portal and select a subscription. You should see the cost breakdown and burn rate in the popup blade.

2. Click Cost analysis in the list to the left to see the cost breakdown by resource. Wait 24 hours after you add a service for the data to populate.

3. You can filter by different properties like tags, resource group, and timespan. Click Apply to confirm the filters and Download if you want to export the view to a Comma-Separated Values (.csv) file.

***Download the usage report***

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources

https://docs.microsoft.com/en-us/azure/cost-management-billing/cost-management-billing-overview

**Quick Preview:**

Question 15: Skipped
You have an Azure subscription named Subscription1 that contains an Azure Log Analytics workspace named Workspace1. You need to view the error from a table named Event.

Which query should you run in Workspace1?

- ○
  Get-Event Event | where {$_. EventType == "error"}
- ○
  Event | search "error"
  (Correct)
- ○
  search in (Event)* | where EventType –eq "error"
- ○
  Get-Event Event | where {$_.EventTye –eq "error"}

**Explanation**
The same query can be written in two forms Event | search "error" Or search in (Event) "error"

**Further Learning:**

https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview

**Quick Preview:**

Question 16: Skipped
You need to create an Azure Storage account that meets the following requirements:

- Minimizes costs

- Supports hot, cool, and archive blob tiers

- Provides fault tolerance if a disaster affects the Azure region where the account resides

How should you complete the below command?

az storage account create -g RG1 -n storageaccount1 --kind `(1)` --sku `(2)`

- □
  (1) BlobStorage
- □

(1) Storage

- □
  (1) Storage V2
  (Correct)
- □
  (2) Standard_GRS
  (Correct)
- □
  (2) Standard_LRS
- □
  (2) Standard_RAGRS
- □
  (2) Premium_LRS

**Explanation**
You may only tier your object storage data to hot, cool, or archive in Blob storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts do not support tiering. General-purpose v2 accounts deliver the lowest per-gigabyte capacity prices for Azure Storage, as well as industry-competitive transaction prices.

Geo-redundant storage (GRS): Cross-regional replication to protect against region-wide unavailability.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers?tabs=azure-portal

https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

**Quick Preview:**

Question 17: Skipped
You have an Azure subscription that contains the resources in the following table:
Larger image

Store1 contains a file share named data. Data contains 5,000 files. You need to synchronize the files in the file share named ***data*** to an on-premises server named ***Server1***.

Which three actions should you perform?

- □
  Create a container instance

- □ Register Server1 (Correct)
- □ Install the Azure File Sync agent on Server1 (Correct)
- □ Download an automation script
- □ Create a sync group (Correct)

**Explanation**
***Step 1: Install the Azure File Sync agent on Server1***

The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share.

***Step 2: Register Server1*** **-** Register Windows Server with Storage Sync Service

Registering your Windows Server with a Storage Sync Service establishes a trust relationship between your server (or cluster) and the Storage Sync Service.

***Step 3: Create a sync group and a cloud endpoint***

A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints. A server endpoint represents a path on registered server.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide?tabs=azure-portal%2Cproactive-portal

**Quick Preview:**

Question 18: Skipped
You have an Azure subscription that contains the resources shown in the following table:
Larger image

The status of VM1 is Running.

You assign an Azure policy as shown in the exhibit below:

Larger image

You assign the policy by using the following parameters:

***- Microsoft.ClassicNetwork/virtualNetworks***

***- Microsoft.Network/virtualNetworks***

***- Microsoft.Compute/virtualMachines***

`True` or `False`.

An administrator can move VNET1 to RG2.

- ○ True
- ○ False (Correct)

**Explanation**

***Not Allowed resource types*** policy is preventing the resource types selected in the assignment from being **deployed**.

You can delete previous existing resources of these types and you can also make modifications not requiring a **deployment**.

In fact until May 2021, you could move a vNet to a resource group with a Not Allowed resource type policy, including the *Microsoft.Network/virtualNetworks* type.

But a recent change deployed in Azure by the end of May 2021, is not allowing to move a vNet to a resource group with this policy applied.

Therefore the statement is false.

**Reference:**

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

**Quick Preview:**

Question 19: Skipped

You have an Azure subscription that contains the resources shown in the following table:
Larger image

The status of VM1 is Running.

You assign an Azure policy as shown in the exhibit below:

Larger image

You assign the policy by using the following parameters:

***- Microsoft.ClassicNetwork/virtualNetworks***

***- Microsoft.Network/virtualNetworks***

***- Microsoft.Compute/virtualMachines***

`True` or `False`.

The state of VM1 changed to deallocated.

- ○ True
- ○ False (Correct)

**Explanation**
Started VM1 stays on after applying the policy. If you test the scenario in Azure Portal, you will be able to stop and start again.

The policy definition denies a user to deploy VNET and virtual machine resources, it will not affect the running state of VM1.

**Reference:**

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

**Quick Preview:**

Question 20: Skipped

You have an Azure subscription that contains the resources shown in the following table:
Larger image

The status of VM1 is Running.

You assign an Azure policy as shown in the exhibit below:

Larger image

You assign the policy by using the following parameters:

***- Microsoft.ClassicNetwork/virtualNetworks***

***- Microsoft.Network/virtualNetworks***

***- Microsoft.Compute/virtualMachines***

`True` or `False`.

An administrator can modify the address space of VNET2.

- ○ True
- ○ False (Correct)

**Explanation**
***Not Allowed resource types*** policy is preventing the resource types selected in the assignment from being **deployed**.

You can delete previous or existing resources of these types and you can also make modifications that don't require a **deployment**.

But modifying the address space requires you to **deploy** again the vNet, and this is not allowed with the ***Not Allowed resource types*** policy applied. This operation requires a **deployment** because the command you need to run, for explample using AZ CLI is the following:

*az network vnet update --address-prefixes 10.1.0.0/16 10.2.0.0/16 --name vnet2 --resource-group RG2,* and the command contains all the address prefixes, and not only the new one you may be adding or deleting.

Additionally, when you create the policy, you are informed that the assignment takes around 30 minutes to take effect:

This time is needed, because the policy applies directly to new resources you want to create(deploy), but over existing resources the evaluation does not work until they are marked as non-compliant.

This means that just after you create the policy you still can modify the vNet address space(Adding new spaces or deleting unused spaces). But once the existing vNets have been marked as non-compliant the modification of Address space cannot be done, and the message you receive is very clear:

**Reference:**

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

**Quick Preview:**

Question 21: Skipped

You have an Azure subscription that contains a storage account. You have an on-premises server named Server1 that runs Windows 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 below actions?

(1) From the Azure portal, update the import job

(2) From the Azure portal, create an import job

(3) Attach an external disk to Server1 and then run waimportexport.exe

(4) Detach the external disks from Server1 and ship the disks to an Azure data center

- ○ 3 - 2 - 1 - 4
- ○ 3 - 2 - 4 - 1 (Correct)

- ○
  2 - 3 - 1 - 4
- ○
  2 - 3 - 4 - 1

**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.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-service

**Quick Preview:**

Question 22: Skipped
You have an Azure subscription that includes the following Azure file shares:
Larger image

You have the following on-premises servers:
Larger image

You create a Storage Sync Service named Sync1 and an Azure File Sync group named Group1. Group1 uses share1 as a cloud endpoint.

You register Server1 and Server2 in Sync1. You add D:\Folder1 on Server1 as a server endpoint of Group1.

Please evaluate if the following statement is `True` or `False`.

Share2 can be added as a cloud endpoint for Group1.

- ○ True
- ○ False (Correct)

**Explanation**

Group1 already has a cloud endpoint named Share1.

A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide?tabs=azure-portal%2Cproactive-portal

**Quick Preview:**

Question 23: Skipped

You have an Azure subscription that includes the following Azure file shares:

Larger image

You have the following on-premises servers:

Larger image

You create a Storage Sync Service named Sync1 and an Azure File Sync group named Group1. Group1 uses share1 as a cloud endpoint.

You register Server1 and Server2 in Sync1. You add D:\Folder1 on Server1 as a server endpoint of Group1.

Please evaluate if the following statement is `True` or `False`.

E:\Folder2 on Server1 can be added as a server endpoint for Group1.

- ○

True

- ○ False (Correct)

**Explanation**

Multiple server endpoints can exist on the same volume if their namespaces are not overlapping (for example, D:\Folder1 and E:\Folder2) and each endpoint is syncing to a unique sync group.

In the question’s scenario, namespaces are not overlapping, but we are asking to sync with the same sync group, and that’s not possible, so correct answer is false.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-server-endpoint

https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide?tabs=azure-portal%2Cproactive-portal

**Quick Preview:**

Question 24: Skipped

You have an Azure subscription that includes the following Azure file shares:

Larger image

You have the following on-premises servers:

Larger image

You create a Storage Sync Service named Sync1 and an Azure File Sync group named Group1. Group1 uses share1 as a cloud endpoint.

You register Server1 and Server2 in Sync1. You add D:\Folder1 on Server1 as a server endpoint of Group1.

Please evaluate if the following statement is `True` or `False`.

D:\Data on Server2 can be added as a server endpoint

- ○
  True
  (Correct)
- ○
  False

**Explanation**
Yes, one or more server endpoints can be added to the sync group.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide?tabs=azure-portal%2Cproactive-portal

**Quick Preview:**

Question 25: Skipped
You create a virtual machine scale set named Scale1. Scale1 is configured as shown in the following exhibit:
Larger image

If Scale1 is utilized at 85% for 6 minutes after it is deployed, Scale1 will be running .......... .

- ○
  2 virtual machines
- ○
  4 virtual machines
- ○
  6 virtual machines
  (Correct)
- ○
  10 virtual machines
- ○
  20 virtual machines

**Explanation**
The Autoscale scale out rule increases the number of VMs by 2 if the CPU threshold is 80% or higher. The initial instance count is 4 VMs and rises to 6 VMS, when the 2 extra instances of VMs are added.

**Further Learning:**

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/overview

**Quick Preview:**

Question 26: Skipped

You create a virtual machine scale set named Scale1. Scale1 is configured as shown in the following exhibit:

Larger image

If Scale1 is first utilized at 25% for 6 minutes after it is deployed, and then utilized at 50% for 6 minutes, Scale1 will be running ........... .

- ○ 2 virtual machines (Correct)
- ○ 4 virtual machines
- ○ 6 virtual machines
- ○ 8 virtual machines
- ○ 10 virtual machines

**Explanation**

The Autoscale scale in rule decreases the number of VMs by 4 if the CPU threshold is 30% or lower. The initial instance count is 4 and thus cannot be reduced to 0 as the minimum instances is set to 2. So the number of instances running is 2 after running for 6 minutes as 25%. Instances are only added when the CPU threshold reaches 80%, so 2 instances remain.

**Further Learning:**

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-autoscale-overview

**Quick Preview:**

Question 27: Skipped

You plan to automate the deployment of a virtual machine scale set that uses the Windows Server 2016 Datacenter image.

You need to ensure that when the scale set virtual machines are provisioned, they have web server components installed.

Which two actions should you perform?

- □
  Upload a configuration script
- □
  Create an automation account
- □
  Create an Azure policy
- □
  Modify the extensionProfile section of the Azure Resource Manager template
  (Correct)
- □
  Create a new virtual scale set in the Azure portal
  (Correct)

**Explanation**
Virtual Machine Scale Sets can be used with the Azure Desired State Configuration (DSC) extension handler. Virtual machine scale sets provide a way to deploy and manage large numbers of virtual machines, and can elastically scale in and out in response to load. DSC is used to configure the VMs as they come online so they are running the production software.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-dsc

**Quick Preview:**

Question 28: Skipped
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? (SELECT TWO)

(1) (2) install-cli

- □
  (1) az
  (Correct)
- □
  (1) docker
- □
  (1) msiexec.exe
- □

(1) Install-Module

- □
  (2) aks
  (Correct)
- □
  (2) /package
- □
  (2) -name
- □
  (2) pull

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

**Reference:**

https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough

**Quick Preview:**

Question 29: Skipped
You onboard 10 Azure virtual machines to Azure Automation State Configuration. You need to use Azure Automation State Configuration to manage the ongoing consistency of the virtual machine configurations.

Which three actions should you perform in sequence?

(1) Assign the node configuration

(2) Check the compliance status of the node

(3) Compile a configuration into a node configuration

(4) Upload a configuration to Azure Automation State Configuration

(5) Create a management group

- ○
  3 - 2 - 4
- ○
  4 - 1 - 3
- ○
  4 - 3 - 1
  (Correct)

- ○
  5 - 3 - 1

**Explanation**

***Step 1:*** Upload a configuration to Azure Automation State Configuration. Import the configuration into the Automation account.

***Step 2:*** Compile a configuration into a node configuration. A DSC configuration defining that state must be compiled into one or more node configurations (MOF document), and placed on the Automation DSC Pull Server.

***Step 3:*** Assign the node configuration

***Step 4:*** Check the compliance status of the node

Each time Azure Automation State Configuration performs a consistency check on a managed node, the node sends a status report back to the pull server. You can view these reports on the page for that node. On the blade for an individual report, you can see the following status information for the corresponding consistency check:

The report status — whether the node is "Compliant", the configuration "Failed", or the node is "Not Compliant"

**Reference:**

https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

**Quick Preview:**

Question 30: Skipped

You have an Azure Resource Manager template named Template1 that is used to deploy an Azure virtual machine.

Template1 contains the following text:

Larger image

The variables section in Template1 contains the following text: "location": "westeurope". The resources section in Template1 contains the following text:
Larger image

You need to deploy the virtual machine to the West US location by using Template1.

What should you do?

- ○ Modify the location in the ***resource section to westus*** (Correct)
- ○ Select West US during the deployment
- ○ Modify the location in the variables section to westus

Question 31: Skipped

You create an App Service plan named Plan1 and an Azure web app named webapp1. You discover that the option to create a staging slot is unavailable. You need to create a staging slot for Plan1.

What should you do first?

- ○ From Plan1, scale up the App Service plan (Correct)
- ○ From webapp1, modify the Application settings
- ○ From webapp1, add a custom domain
- ○ From Plan1, scale out the App Service plan

**Explanation**

The app must be running in the Standard, Premium, or Isolated tier in order for you to enable multiple deployment slots.

If the app isn't already in the Standard, Premium, or Isolated tier, you receive a message that indicates the supported tiers for enabling staged publishing. At this point, you have the option to select Upgrade and go to the Scale tab of your app before continuing.

Scale up: Get more CPU, memory, disk space, and extra features like dedicated virtual machines (VMs), custom domains and certificates, staging slots, autoscaling, and more.

**Reference:**

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

https://docs.microsoft.com/en-us/azure/app-service/manage-scale-up

**Quick Preview:**

Question 32: Skipped
You have an Azure subscription named Subscription1. Subscription1 contains the virtual machines in the following table:
Larger image

Subscription1 contains a virtual network named VNet1 that has the subnets in the following table:
Larger image

VM3 has multiple network adapters, including a network adapter named NIC3. IP forwarding is enabled on NIC3. Routing is enabled on VM3. You create a route table named RT1 that contains the routes in the following table:
Larger image

You apply RT1 to Subnet1 and Subnet2.

Please evaluate the scenario and decide if the following statement is `True` or `False`.

VM3 can establish a network connection to VM1.

- ○ True (Correct)
- ○ False

**Explanation**
Let's cover some context first.

IP forwarding enables the virtual machine to:

- Receive network traffic not destined for one of the IP addresses assigned to any of the IP configurations assigned to the network interface.

- Send network traffic with a different source IP address than the one assigned to one of a network interface's IP configurations.

The setting must be enabled for every network interface that is attached to the virtual machine that receives traffic that the virtual machine needs to forward. A virtual machine can forward traffic whether it has multiple network interfaces or a single network interface attached to it.

The routing table enables connections from VM1 to VM2 and VM2 to VM1, through VM3, as the next-hop. VM3 uses default routing and can connect to VM1, so the statement is True.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

**Quick Preview:**

Question 33: Skipped

You have an Azure subscription named Subscription1. Subscription1 contains the virtual machines in the following table:

Larger image

Subscription1 contains a virtual network named VNet1 that has the subnets in the following table:

Larger image

VM3 has multiple network adapters, including a network adapter named NIC3. IP forwarding is enabled on NIC3. Routing is enabled on VM3. You create a route table named RT1 that contains the routes in the following table:

Larger image

You apply RT1 to Subnet1 and Subnet2.

Please evaluate the scenario and decide if the following statement is `True` or `False`.

If VM3 is turned off, VM2 can establish a network connection to VM1.

- ○ True
- ○ False (Correct)

**Explanation**

Let's cover some context first.

IP forwarding enables the virtual machine to:

- Receive network traffic not destined for one of the IP addresses assigned to any of the IP configurations assigned to the network interface.

- Send network traffic with a different source IP address than the one assigned to one of a network interface's IP configurations.

The setting must be enabled for every network interface that is attached to the virtual machine that receives traffic that the virtual machine needs to forward. A virtual machine can forward traffic whether it has multiple network interfaces or a single network interface attached to it.

Default routing has been modified for Subnet1 and Subnet2 and RT1 has been attached to these two subnets. The next-hop defined is VM3, so traffic will traverse VM3 between the two subnets. If VM3 is turned off, VM2 can't establish a network connection to VM1.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

**Quick Preview:**

Question 34: Skipped

You have an Azure subscription named Subscription1. Subscription1 contains the virtual machines in the following table:

Larger image

Subscription1 contains a virtual network named VNet1 that has the subnets in the following table:

Larger image

VM3 has multiple network adapters, including a network adapter named NIC3. IP forwarding is enabled on NIC3. Routing is enabled on VM3. You create a route table named RT1 that contains the routes in the following table:

Larger image

You apply RT1 to Subnet1 and Subnet2.

Please evaluate the scenario and decide if the following statement is `True` or `False`.

VM1 can establish a network connection to VM2.

- ○ True (Correct)
- ○ False

**Explanation**
Let's cover some context first.

IP forwarding enables the virtual machine to:

- Receive network traffic not destined for one of the IP addresses assigned to any of the IP configurations assigned to the network interface.

- Send network traffic with a different source IP address than the one assigned to one of a network interface's IP configurations.

The setting must be enabled for every network interface that is attached to the virtual machine that receives traffic that the virtual machine needs to forward. A virtual machine can forward traffic whether it has multiple network interfaces or a single network interface attached to it.

The routing table allows connections from VM1 and VM2 to VM3. IP forwarding on VM3 allows VM1 to connect to VM2 via VM3.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

**Quick Preview:**

Question 35: Skipped

Your on-premises network contains an SMB share named Share1. You have an Azure subscription that contains the following resources:

- A web app named webapp1

- A virtual network named VNET1

You need to ensure that webapp1 can connect to Share1. What should you deploy?

- ○ an Azure Application Gateway
- ○ an Azure Active Directory (Azure AD) Application Proxy
- ○ an Azure Virtual Network Gateway (Correct)

**Explanation**

A Site-to-Site VPN gateway connection can be used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel.

This type of connection requires a VPN device, a VPN gateway, located on-premises that has an externally facing public IP address assigned to it.

**Reference:**

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

**Quick Preview:**

Question 36: Skipped

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- ○ the Publish-AzVMDscConfiguration cmdlet
- ○ Azure Application Insights
- ○

Azure Custom Script Extension
(Correct)

- ○
  the New-AzConfigurationAssignement cmdlet

**Explanation**
The Custom Script Extension downloads and executes scripts on Azure virtual machines. This extension is useful for post deployment configuration, software installation, or any other configuration or management tasks. Using a Custom Script Extension you can make sure that NGINX is installed once the VMs are deployed.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/custom-script-windows

**Quick Preview:**

Question 37: Skipped
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:
Larger image

You need to recommend a networking solution to meets the following requirement:

- Ensure that communication between the web servers and the business logic tier spreads equally across the virtual machines

Which Azure resource should you recommend for the above requirement?

- ○
  an application gateway that uses the standard tier
- ○
  an application gateway that uses the WAF tier
- ○
  an internal load balancer
  (Correct)
- ○
  a network security group (NSG)
- ○
  a public load balancer

**Explanation**
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.

**Reference:**

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

**Quick Preview:**

Question 38: Skipped
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:
Larger image

You need to recommend a networking solution to meets the following requirement:

- Protect the web servers from SQL injection attacks.

Which Azure resource should you recommend for the above requirement?

- ○ an application gateway that uses the Standard tier
- ○ an application gateway that uses the WAF tier (Correct)
- ○ an internal load balancer
- ○ a network security group (NSG)
- ○ a public load balancer

**Explanation**
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.

**Reference:**

https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview

**Quick Preview:**

Question 39: Skipped

Your company has three offices. The offices are located in Miami, Los Angeles, and New York. Each office contains datacenter.

You have an Azure subscription that contains resources in the East US and West US Azure regions. Each region contains a virtual network. The virtual networks are peered. You need to connect the datacenters to the subscription. The solution must minimize network latency between the data centers.

What should you create?

- ○ three Azure Application Gateways and one On-premises data gateway
- ○ two virtual hubs and one virtual WAN **(Correct)**
- ○ three virtual WANs and one virtual hub
- ○ three On-premises data gateways and one Azure Application Gateway

**Explanation**

For this scenario, 2 virtual hubs would be needed to cover the two regions (East US and West US) and one virtual Wan.

Then we can create VPN connections from our on premises locations to our Virtual Hubs.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology

https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal

**Quick Preview:**

Question 40: Skipped

You plan to deploy five virtual machines to a virtual network subnet. Each virtual machine will have a public IP address and a private IP address. Each virtual machine requires the same inbound and outbound security rules.

What is the minimum number of network interfaces and network security groups that you require? (SELECT TWO)

- □ Minimum number of network interfaces - 5 (Correct)
- □ Minimum number of network interfaces - 10
- □ Minimum number of network interfaces - 15
- □ Minimum number of network interfaces - 20
- □ Minimum number of network security groups - 1 (Correct)
- □ Minimum number of network security groups - 2
- □ Minimum number of network security groups - 5
- □ Minimum number of network security groups - 10

**Explanation**

A public and a private IP address can be assigned to a single network interface, so we would need minimum 5 network interfaces.

You can associate zero, or one, network security group to each virtual network subnet and network interface in a virtual machine. The same network security group can be associated to as many subnets and network interfaces as you choose, so minimum one network security group is needed.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-addresses

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works

**Quick Preview:**

Question 41: Skipped

You have Azure virtual machines that run Windows Server 2019 and are configured as shown in the following table:

Larger image

You create a private Azure DNS zone named adatum.com. You configure the adatum.com zone to allow auto registration from VNET1.

Which A records will be added to the adatum.com zone for each virtual machine? (SELECT TWO)

- □ A records for VM1 - None
- □ A records for VM1 - Private IP address only (Correct)
- □ A records for VM1 - Public IP address only
- □ A records for VM1 - Private IP address and public IP address
- □ A records for VM2 - None
- □ A records for VM2 - Private IP address only (Correct)
- □ A records for VM2 - Public IP address only
- □ A records for VM2 - Private IP address and public IP address

**Explanation**

The virtual machines are registered (added) to a private zone, so the A records will be pointing to their private IP addresses.

**Reference:**

https://docs.microsoft.com/en-us/azure/dns/private-dns-overview

https://docs.microsoft.com/en-us/azure/dns/private-dns-scenarios

**Quick Preview:**

Question 42: Skipped

You have an Azure virtual network named VNet1 that connects to your on-premises network by using a site-to-site VPN. VNet1 contains one subnet named Sunet1.

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? (SELECT TWO)

- □ Resource to create - An Azure Event Grid
- □ Resource to create - An Azure Log Analytics Workspace
- □ Resource to create - An Azure Storage account (Correct)
- □ Resource on which to enable diagnostics - ILB1
- □ Resource on which to enable diagnostics - NSG1 (Correct)
- □ Resource on which to enable diagnostics - The Azure virtual machines

**Explanation**

A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability.

Although you may be tempted to choose iLB1, diagnostic logs for a basic load balancer do not include the IP addresses of inbound connections. Flow logs do, and those get attached to the network security group.

**Reference:**

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal?toc=/azure/virtual-network/toc.json

**Quick Preview:**

Question 43: Skipped

You have the Azure virtual networks shown in the following table:
Larger image

To which virtual networks can you establish a peering connection from VNET1?

- ○ VNET2 and VNET3
- ○ VNET2 only
- ○ VNET3 and VNET4 (Correct)
- ○ VNET2, VNET3 and VNET4

**Explanation**
The address space of VNET2 overlaps with VNET1, therefore a peering can't be established between VNET2 and VNET1. As you can see below, there could be VMs running in both VNETs, with the same IP address, for example 10.11.0.1.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq

**Quick Preview:**

Question 44: Skipped
You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains four subnets named Gateway, Perimeter, NVA, and Production.

The NVA subnet contains two network virtual appliances (NVAs) that will perform network traffic inspection between the Perimeter subnet and the Production subnet.

You need to implement an Azure load balancer for the NVAs. The solution must meet the following requirements:

- The NVAs must run in an active-active configuration that uses automatic failover.

- The NVA must load balance traffic to two services on the Production subnet. The services have different IP addresses.

Which three actions should you perform?

- □ Deploy a basic load balancer

- □ Deploy a standard load balancer (Correct)
- □ Add two load balancing rules that have HA Ports and Floating IP enabled (Correct)
- □ Add two load balancing rules that have HA Ports enabled and Floating IP disabled
- □ Add a frontend IP configuration, a backend pool, and a health probe
- □ Add a frontend IP configuration, two backend pools, and a health probe (Correct)

**Explanation**

HA ports need are not supported by a basic load balancer, so we would need a Standard Load Balancer.  You need a floating IP address for the active-active configuration to switch over quickly and two backend pools are needed for the two different services.

**Reference:**

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-ha-ports-overview

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip-overview

**Quick Preview:**

Question 45: Skipped

You have an Azure subscription named Subscription1 that contains two Azure virtual networks named VNet1 and VNet2. VNet1 contains a VPN gateway named VPNGW1 that uses static routing. There is a site-to-site VPN connection between your on-premises network and VNet1.

On a computer named Client1 that runs Windows 10, you configure a point-to-site VPN connection to VNet1. You configure virtual network peering between VNet1 and VNet2. You verify that you can connect to VNet2 from the on-premises network. Client1 is unable to connect to VNet2.

You need to ensure that you can connect Client1 to VNet2.

What should you do?

- ○ Download and re-install the VPN client configuration package on Client1 (Correct)
- ○ Select Allow gateway transit on VNet1
- ○ Select Allow gateway transit on VNet2
- ○ Enable BGP on VPNGW1

**Explanation**

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

First, the point-to-site VPN was up and running from Client1 to VNet1 and then a change was implemented : the peering was created between VNET1 and VNET2. For this reason, the the VPN client package must be downloaded and installed again in order to gain connectivity to VNET2.

**Reference:**

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing#multipeered

**Quick Preview:**

Question 46: Skipped

You have an on-premises network that you plan to connect to Azure by using a site-to-site VPN.

In Azure, you have an Azure virtual network named VNet1 that uses an address space of 10.0.0.0/16 VNet1 contains a subnet named Subnet1 that uses an address space of 10.0.0.0/24. You need to create a site-to-site VPN to Azure.

Which four actions should you perform in sequence?

(1) Create a local gateway

(2) Create a VPN gateway

(3) Create a gateway subnet

(4) Create a custom DNS server

(5) Create a VPN connection

(6) Create an Azure Content Delivery Network (CDN) profile

- ○ 3 - 2 - 1 - 5 (Correct)
- ○ 3 - 1 - 2 - 5
- ○ 2 - 3 - 1 - 5
- ○ 3 - 2 - 5 - 1

**Explanation**
**Reference:**

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

**Quick Preview:**

Question 47: Skipped
You have an Azure subscription that contains the resources in the following table:
Larger image

VM1 and VM2 are deployed from the same template and host line-of-business applications.

You configure the network security group (NSG) as shown in the exhibit below:

Larger image

You need to prevent users of VM1 and VM2 from accessing websites on the Internet over TCP port 80.

What should you do?

- ○ Disassociate the NSG from a network interface
- ○ Change the Port_80 inbound security rule.
- ○

Associate the NSG to Subnet1
(Correct)

- ○
  Change the DenyWebSites outbound security rule

**Explanation**
You can associate or dissociate a network security group from a network interface or subnet. The NSG has the appropriate rule to block users from accessing the Internet. We just need to associate it with Subnet1.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group

**Quick Preview:**

Question 48: Skipped
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?

- ○
  Move VM1 to Subscription2
- ○
  Move VNet1 to Subscription2
- ○
  Modify the IP address space of VNet2
- ○
  Provision virtual network gateways
  (Correct)

**Explanation**
The virtual networks can be in the same or different regions, and from the same or different subscriptions. When connecting VNets from different subscriptions, the subscriptions do not need to be associated with the same Active Directory tenant.

Configuring a VNet-to-VNet connection is a good way to easily connect VNets. Connecting a virtual network to another virtual network using the VNet-to-VNet connection type (VNet2VNet) is similar to creating a Site-to-Site IPsec connection to an on-premises location. Both connectivity types use a VPN gateway to provide a secure tunnel using IPsec/IKE, and both function the same way when communicating.

The local network gateway for each VNet treats the other VNet as a local site. This lets you specify additional address space for the local network gateway in order to route traffic.

**Reference:**

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal

**Quick Preview:**

Question 49: Skipped

You plan to create an Azure virtual machine named VM1 that will be configured as shown in the exhibit below:

Larger image

The planned disk configurations for VM1 are shown in the following exhibit:

Larger image

You need to ensure that VM1 can be created in an Availability Zone.

Which two settings should you modify? Each correct answer presents part of the solution.

- □ Use managed disks (Correct)
- □ OS disk type
- □ Availability options (Correct)
- □ Size
- □ Image

**Explanation**
Your VMs should use managed disks if you want to move them to an Availability Zone by using Site Recovery.

When you create a VM for an Availability Zone, Under Settings > High availability, select one of the numbered zones from the Availability zone dropdown menu:

Also, in order for the VM to be deployed into an Availability zone, ***Availability options*** should be changed to ***Availability Zone,*** so that an Availability Zone could be selected below:

**Reference:**

https://docs.microsoft.com/en-us/azure/site-recovery/move-azure-vms-avset-azone

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/create-portal-availability-zone

**Quick Preview:**

Question 50: Skipped
You manage two Azure subscriptions named Subscription1 and Subscription2. Subscription1 has following virtual networks:
Larger image

The virtual networks contain the following subnets:

Larger image

Subscription2 contains the following virtual network:

- Name: VNETA

- Address space: 10.10.128.0/17

- Location: Canada Central

VNETA contains the following subnets:

Larger image

Please evaluate the following statements and select `True` if the statement is true, otherwise, select `False`:

1. A site-to-site connection can be established between VNET1 and VNET2.

2. VNET1 and VNET2 can be peered.

3. VNET1 and VNETA can be peered.

- ○ 1 - True, 2 - True, 3 - False
- ○ 1 - True, 2 - True, 3 - True (Correct)
- ○ 1 - True, 2 - False, 3 - True
- ○ 1 - False, 2 - True, 3 - True

**Explanation**
Azure virtual networks can be connected together by using either VPNs or virtual network peerings. VPNs represent encrypted communication channels that you establish between remote virtual networks, while vnet peerings are not encryptedm but are still private. Traffic within vNET peerings use the Microsoft backbone infrastructure, so the traffic doesn't go over the public internet.

First thing to check when you need to connect vNETs is if the virtual networks' IP addressing space overlap. You can't connect two virtual networks with overlapping IP address space.

**Statement1 - True - A site-to-site connection can be established between VNET1 and VNET2.**

VNET1 and VNET2 IP addressing space doesn't overlap, and there is no restriction to connect VNETs deployed in different Azure regions.

Additionally in both VNETs we have unused address space that we can use to create the GatewaySubnet.

In VNET1, there is free IP address space range 10.10.10.128/25 to use and in VNET2 there are free IP address space ranges to use as well - 172.16.64.0/18 and 172.16.192.0/18.

**Statement2 - True - VNET1 and VNET2 can be peered.**

The same applies for VNET1 and VNET2 peering. No IP address space overlap, vnet peering can be defined between the two VNETs.

**Statement3 - True - VNET1 and VNETA can be peered.**

This one may be a bit tricky, if you don't have some experience already with IPv4 addressing subnetting.

VNET1 address space is 10.10.10.0/24:

and we can see the useable IP addresses in the 4th column.

VNET2 address space is 10.10.128.0/17:

and we can see the useable IP addresses in the 4th column.

In order for the two vNETs to be eligible for vNET peering, there has to be no overlap between the two, so the range of addresses - 3rd column or useable IPs - 4th column, must not overlap. As you can see in the two tables, so two IP address ranges do not overlap, so the two vNETs can be peered together.

**Reference:**

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

**Quick Preview:**

Question 51: Skipped

You have an Azure subscription. You plan to deploy an Azure Kubernetes Service (AKS) cluster to support an app named App1. On-premises clients connect to App1 by using the IP address of the pod.

For the AKS cluster, you need to choose a network type that will support App1.

What should you choose?

- ○ kubenet
- ○ Azure Container Networking Interface (CNI) (Correct)
- ○ Hybrid Connection endpoints
- ○ Azure Private Link

**Explanation**
AKS only supports kubenet networking and Azure Container Networking Interface (CNI) networking, so options C and D are incorrect.

The ***kubenet*** networking option is the default configuration for AKS cluster creation. With *kubenet*, nodes get an IP address from the Azure virtual network subnet. Pods receive an IP address from a logically different address space to the Azure virtual network subnet of the nodes.

With ***Azure CNI***, every pod gets an IP address from the subnet and can be accessed directly. As the question states that the on-premises clients connect to App1 by using the IP address of the pod, Azure CNI is the correct option for this scenario.

**Reference:**

https://docs.microsoft.com/en-us/azure/aks/concepts-network

**Quick Preview:**

Question 52: Skipped
***Case study***

***This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.***

***To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.***

***Overview***

Litware, Inc. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The Montreal office has 2,000 employees. The Seattle office has 1,000 employees. The New York office has 200 employees.

All the resources used by Litware are hosted on-premises. Litware creates a new Azure subscription. The Azure Active Directory (Azure AD) tenant uses a domain named litware.onmicrosoft.com. The tenant uses the P1 pricing tier.

***Existing Environment***

The network contains an Active Directory forest named litware.com. All domain controllers are configured as DNS servers and host the litware.com DNS zone.

Litware has finance, human resources, sales, research, and information technology departments. Each department has an organizational unit (OU) that contains all the accounts of that respective department. All the user accounts have the department attribute set to their respective department. New users are added frequently.

Litware.com contains a user named User1.

All the offices connect by using private connections.

Litware has data centers in the Montreal and Seattle offices. Each office has a firewall that can be configured as a VPN device.

All infrastructure servers are virtualized. The virtualization environment contains the servers in the following table:

Larger image

Litware uses two web applications named App1 and App2. Each instance on each web application requires 1 GB of memory.

The Azure subscription contains the resources in the following table:

Larger image

The network security team implements several network security groups (NSGs).

**Requirements**

**Planned Changes**

Litware plans to implement the following changes:

- Deploy Azure ExpressRoute to the Montreal office.

- Migrate the virtual machines hosted on Server1 and Server2 to Azure.

- Synchronize on-premises Active Directory to Azure Active Directory (Azure AD).

- Migrate App1 and App2 to two Azure web apps named WebApp1 and WebApp2.

***Technical Requirements***

Litware must meet the following technical requirements:

- Ensure that WebApp1 can adjust the number of instances automatically based on the load and can scale up to five instances.

- Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.

- Ensure that routing information is exchanged automatically between Azure and the routers in the Montreal office.

- Enable Azure Multi-Factor Authentication (MFA) for the users in the finance department only.

- Ensure that webapp2.azurewebsites.net can be accessed by using the name app2.litware.com.

- Connect the New York office to VNet1 over the Internet by using an encrypted connection.

- Create a workflow to send an email message when the settings of VM4 are modified.

- Create a custom Azure role named Role1 that is based on the Reader role.

- Minimize costs whenever possible.

QUESTION 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?

- ○ Diagram in VNet1
- ○ Diagnostic settings in Azure Monitor
- ○ Diagnose and solve problems in Traffic Manager profiles
- ○ The security recommendations in Azure Advisor
- ○ IP flow verify in Azure Network Watcher (Correct)

**Explanation**
**From the 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.

**Reference:**

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

Question 1: Skipped
You have an Azure subscription named Subscription1. Subscription1 contains the resource groups in the following table:
Larger image

RG1 has a web app named WebApp1. WebApp1 is located in West Europe. You move WebApp1 to RG2.

What is the effect of the move?

- ○ The App Service plan for WebApp1 remains in West Europe. Policy2 applies to WebApp1
  (Correct)
- ○ The App Service plan for WebApp1 moves to North Europe. Policy2 applies to WebApp1
- ○ The App Service plan for WebApp1 remains in West Europe. Policy1 applies to WebApp1
- ○ The App Service plan for WebApp1 moves to North Europe. Policy1 applies to WebApp1

**Explanation**

You can move an app to another App Service plan, as long as the source plan and the target plan are in the same resource group and geographical region.

The region in which your app runs is the region of the App Service plan it's in. However, you cannot change an App Service plan's region.

**Reference:**

https://docs.microsoft.com/en-us/azure/app-service/app-service-plan-manage

**Quick Preview:**

Question 2: Skipped

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 resources within the resource groups

What should you specify in the assignable scopes and the permission elements of the definition of CR1? (SELECT TWO)

Larger image

- ☐
  assignableScopes - 1
- ☐
  assignableScopes - 2
  (Correct)
- ☐
  assignableScopes - 3
- ☐
  permission elements - 1
  (Correct)
- ☐
  permission elements - 2
- ☐
  permission elements - 3

**Explanation**

For the assignable scopes, there is not an option for **/ResourceGroups**. You can specify this option with a specific Resource Group name, like **/ResourceGroups/RG1** or with an * to match all resource groups, like **/ResourceGroups/*** .

So for assignable scopes the subscription and subscription ID must be selected.

**Microsoft.Authorization/*** resource provider permissions need to be selected, in the notActions section, in order to meet the requirements.

With this selection, you have "**actions**" **: ["*"]** , allowing you to do everything.

And "**notActions**" **: ["Microsoft.Authorization/*"]** , preventing you the access to manage permissions in your subscription, in all your resource groups.

**Reference:**

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#microsoftauthorization

**Quick Preview:**

Question 3: Skipped

You have an Azure subscription. Users access the resources in the subscription from either home or from customer sites. From home, users must establish a point-to-site VPN to access the Azure resources. The users on the customer sites access the Azure resources by using site-to-site VPNs.

You have a line-of-business-app named App1 that runs on several Azure virtual machine. The virtual machines run Windows Server 2016. You need to ensure that the connections to App1 are spread across all the virtual machines.

What are two possible Azure services that you can use?

- □
  an internal load balancer
  (Correct)
- □
  a public load balancer
- □
  an Azure Content Delivery Network (CDN)
- □
  Traffic Manager
- □
  an Azure Application Gateway
  (Correct)

**Explanation**
Users are not accessing application over the internet, they first connect to Azure resources through either point-to-site or site-to-site VPN. For this reason an internal load balancer can be used.

The only option left that makes sense in this context is Azure Application Gateway, to be deployed in front of VMs.

**Further Learning:**

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

https://docs.microsoft.com/en-us/azure/application-gateway/overview

**Quick Preview:**

Question 4: Skipped
You have an Azure subscription. You have 100 Azure virtual machines. You need to quickly identify underutilized virtual machines that can have their service tier changed to a less expensive offering.

Which blade should you use from Azure Portal?

- ○

Monitor

- ○ Advisor (Correct)
- ○ Metrics
- ○ Customer Insights

**Explanation**
Advisor helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources. You can get cost recommendations from the Cost tab on the Advisor dashboard.

**Reference:**

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

**Quick Preview:**

Question 5: Skipped
You have an Azure Active Directory (Azure AD) tenant. You need to create a conditional access policy that requires all users to use multi-factor authentication when they access the Azure portal.

Which three settings should you configure?

Larger image

- □ 1. (Correct)
- □ 2. (Correct)
- □ 3.
- □ 4. (Correct)
- □ 5.

**Explanation**

In order to create a basic Conditional Access policy to prompt for MFA when a user signs in to the Azure portal, we need first to select the users or groups where we enforce the policy:

Next, we select Cloud Apps and Microsoft Azure Management, so the policy applies to sign-in events to the Azure portal.

And last we enforce the policy by selecting Grant - Require multi-factor authentication.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

**Quick Preview:**

Question 6: Skipped

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The User administrator role is assigned to a user named Admin1.

An external partner has a Microsoft account that uses the user1@outlook.com sign in. Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: “Unable to invite user user1@outlook.com – Generic authorization exception.”

You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.

What should you do?

- ○ From the Users blade, modify the External collaboration settings (Correct)
- ○ From the Custom domain names blade, add a custom domain
- ○ From the Organizational relationships blade, add an identity provider
- ○ From the Roles and administrators blade, assign the Security administrator role to Admin1

**Explanation**

In order to accomplish the task, the External collaboration settings would need to be modified.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/b2b/delegate-invitations

**Quick Preview:**

Question 7: Skipped

You have an Azure subscription named Subscription1. You create an Azure Storage account named ***contosostorage***, and then you create a file share named ***data***.

Which UNC path should you include in a script that references files from the data file share?

\\ .......... . .......... \ ..........

Please select the correct order that forms the path, from the below options:

(1) blob

(2) contosostorage

(3) file

(4) portal.azure.com

(5) blob.core.windows.net

(6) data

(7) file.core.windows.net

(8) subscription1

- ○ 2 - 5 - 6
- ○ 2 - 7 - 6 (Correct)
- ○ 2 - 4 - 6
- ○ 6 - 5 - 1

**Explanation**

UNC path format is :

**\\ <storageAccountName>.file.core.windows.net \ <fileShareName>**

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows

**Quick Preview:**

Question 8: Skipped

You have an Azure subscription that contains an Azure Storage account. You plan to copy an on-premises virtual machine image to a container named ***vmimages***. You need to create the container for the planned image.

Which command should you run?

az copy .......... https://mystorageaccount. .......... .core.windows.net/vmimages

- □ az copy - make (Correct)
- □ az copy - sync
- □ az copy - copy
- □ https link option - blob (Correct)
- □ https link option - dfs
- □ https link option - queue
- □ https link option - table
- □ https link option - images
- □ https link option - file

**Explanation**

az copy ***make*** option is used to create container, and because it's a container, the ***blob*** option needs to be chosen in the full URL

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-ref-azcopy-make

**Quick Preview:**

Question 9: Skipped

You have an Azure File sync group that has the endpoints shown in the following table:

Larger image

Cloud tiering is enabled for Endpoint2. Using SMB protocol, you add a file named File1 to Endpoint1 and a file named File2 to Endpoint2.

On which endpoints will File1 and File2 be available within 24 hours of adding the files? (SELECT TWO)

- □ File 1 - Endpoint 1 only
- □ File 1 - Endpoint 3 only
- □ File 1 - Endpoint 2 and Endpoint 3 only
- □ File 1 - Endpoint 1, Endpoint 2 and Endpoint 3 (Correct)
- □ File 2 - Endpoint 2
- □ File 2 - Endpoint 3
- □ File 2 - Endpoint 2 and Endpoint 3
- □ File 2 - Endpoint 1, Endpoint 2 and Endpoint 3 (Correct)

**Explanation**

Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints. For this scenario, Endpoint1 is the cloud endpoint and two server endpoints are part of this sync group - Endpoint2 and Endpoint3.

A cloud endpoint is a pointer to an Azure file share. All server endpoints will sync with a cloud endpoint, making the cloud endpoint the hub. The entirety of the Azure file share will be synced.

Synchronization occurs in different ways in each direction.

From Server endpoint to cloud endpoint, synchronization is happening very fast, because the Azure File Sync agent you install in the server, is continuously detecting changes and synchronizing.

But in the cloud endpoint, there is not an agent running to detect changes and starting the synchronization. So there are two important points to understand:

◉ Synchronisation is based on a *change detection job* that is automatically executed once every 24 hours.

◉ This *Change detection job* is based on the SMB last update time info. But this information is only updated when you add or modify the file using SMB Protocol. So if you use REST protocol(AzCopy, Storage Explorer,...) to add or update the file in Azure File Share, the SMB last update time info is not updated, and the file is not synced.

**Therefore, using SMB protocol when adding the files, and after 24 hours, both files will be available in all endpoints.**

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide

https://docs.microsoft.com/en-us/azure/storage/files/storage-files-faq#azure-file-sync

**Quick Preview:**

Question 10: Skipped
You have several Azure virtual machines on a virtual network named vNET2. You configure an Azure Storage account as shown in the following exhibit:
Larger image

Please select the option that is true for the following statement:

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

- ○ always
- ○ during a backup
- ○ never (Correct)

**Explanation**
Subnet 10.2.9.0/24 hasn't been enabled under vNET2, only VMs in 10.2.0.0/24 will have access to file shares in this storage account.

**Reference:**

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

**Quick Preview:**

Question 11: Skipped
You have several Azure virtual machines on a virtual network named vNET2. You configure an Azure Storage account as shown in the following exhibit:
Larger image

Please select the option that is true for the following statement:

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account.

- ○ always
- ○ during a backup
- ○ never (Correct)

**Explanation**

After you configure firewall and virtual network settings for your storage account, select ***Allow trusted Microsoft services to access this storage account*** as an exception to enable Azure Backup service to access the network restricted storage account.

In this scenario, the option is not enabled and access is denied.

**Reference:**
https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

**Quick Preview:**

Question 12: Skipped
You have a sync group named Sync1 that has a cloud endpoint. The cloud endpoint includes a file named File1.txt.

Your on-premises network contains servers that run Windows Server 2016. The servers are configured as shown in the following table:

Larger image

You add Share1 as an endpoint for Sync1. One hour later, you add Share2 as an endpoint for Sync1.

`True` or `False`.

On the cloud endpoint, File1.txt is overwritten by File1.txt from Share1.

- ○ True
- ○ False (Correct)

**Explanation**
Best is to test it in your Azure subscription. Here's what happens:

File1 in Cloud is renamed as File1-Cloud.txt automatically. File1 from server 1 is copied over to Cloud. File1-Cloud.txt is copied over to Server1.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-planning

**Quick Preview:**

Question 13: Skipped

You have a sync group named Sync1 that has a cloud endpoint. The cloud endpoint includes a file named File1.txt.

Your on-premises network contains servers that run Windows Server 2016. The servers are configured as shown in the following table:

Larger image

You add Share1 as an endpoint for Sync1. One hour later, you add Share2 as an endpoint for Sync1.

`True` or `False`.

On Server1, File1.txt is overwritten by File1.txt from the cloud endpoint.

- ○ True
- ○ False (Correct)

**Explanation**

The statement is false. The scenario is similar to the previous one, bot on the server side.

Question 14: Skipped

You have a sync group named Sync1 that has a cloud endpoint. The cloud endpoint includes a file named File1.txt.

Your on-premises network contains servers that run Windows Server 2016. The servers are configured as shown in the following table:

Larger image

You add Share1 as an endpoint for Sync1. One hour later, you add Share2 as an endpoint for Sync1.

`True` or `False`.

File1.txt from Share1 replicates to Share2.

- ○ True (Correct)

- ○ False

**Explanation**
They all are part of the same group, so the data will be synced.

Question 15: Skipped
You have an Azure subscription that contains the storage accounts shown in the following table:
Larger image

You need to identify which storage account can be converted to zone-redundant storage (ZRS) replication by requesting a live migration from Azure support.

What should you identify?

- ○ Storage1
- ○ Storage2 (Correct)
- ○ Storage3
- ○ Storage4

**Explanation**
ZRS supports general-purpose v2 accounts only, so make sure to upgrade your storage account before you submit a request for a live migration to ZRS Live migration is supported only for storage accounts that use LRS or GRS replication. If your account uses RA-GRS, then you need to first change your account's replication type to either LRS or GRS before proceeding

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/redundancy-migration?tabs=portal#request-a-live-migration-to-zrs

**Quick Preview:**

Question 16: Skipped
You have an Azure subscription that contains a storage account named account1. You plan to upload the disk files of a virtual machine to account1 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.

- ☐
  From the Firewalls and virtual networks blade of account1, select ***Selected networks***
  (Correct)
- ☐
  From the Firewalls and virtual networks blade of account1, select ***Allow trusted Microsoft services to***
  ***access this storage account***
- ☐
  From the Firewalls and virtual networks blade of account1, add the 131.107.1.0/24 IP address range
  (Correct)
- ☐
  From the Firewalls and virtual networks blade of account1, add VNet1
- ☐
  From the Service endpoints blade of VNet1, add a service endpoint

**Explanation**

In order to be granted access to upload files to ***account1*** storage account, you would need to add the public IP address range of the on-premises location to the trusted ip ranges, under ***Firewall***.

With this configuration we ensure requirements:
- Ensure that you can upload the disk files to account1.
- Prevent all other access to account1.

But what about requirement **Ensure that you can attach the disks to VM1**?

Well, if you have a look at the second link provided, you will see that Virtual machine disk traffic (including mount and unmount operations, and disk IO) is not affected by network rules:

So you can use the uploaded VHD files, without any additional configuration, because the mount, unmount and disk I/O operations are not affected by network rules.

**Reference:**

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

https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security#scenarios

**Quick Preview:**

Question 17: Skipped

You plan to move a distributed on-premises app named App1 to an Azure subscription. After the planned move, App1 will be hosted on several Azure virtual machines.

You need to ensure that App1 always runs on at least eight virtual machines during planned Azure maintenance.

What should you create?

- ○ one virtual machine scale set that has 10 virtual machines instances
- ○ one Availability Set that has three fault domains and one update domain
- ○ one Availability Set that has 10 update domains and 2 fault domains (Correct)
- ○ one virtual machine scale set that has 12 virtual machines instances

**Explanation**

Update domains can help during Azure planned maintenance windows, because VMs in different update domaine are not restarted at the same time.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/manage-availability

**Quick Preview:**

Question 18: Skipped

***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.***

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?

- ○ Yes
- ○ No (Correct)

**Explanation**

You would need to redeploy the VM.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/redeploy-to-new-node-windows

**Quick Preview:**

Question 19: Skipped

***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.***

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 Redeploy blade, you click **Redeploy**.

Does this meet the goal?

- ○ Yes (Correct)
- ○ No

**Explanation**
When you redeploy a VM, it moves the VM to a new node within the Azure infrastructure and then powers it back on, retaining all your configuration options and associated resources.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/redeploy-to-new-node-windows

**Quick Preview:**

Question 20: Skipped
***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.***

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?

- ○ Yes
- ○ No (Correct)

**Explanation**
You would need to redeploy the VM.

When you redeploy a VM, it moves the VM to a new node within the Azure infrastructure and then powers it back on, retaining all your configuration options and associated resources.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/redeploy-to-new-node-windows

**Quick Preview:**

Question 21: Skipped

You have an Azure subscription that contains a web app named webapp1.

You need to add a custom domain named www.x-a-a-s.com to webapp1.

What should you do first?

- ○ Create a DNS record **(Correct)**
- ○ Add a connection string
- ○ Upload a certificate
- ○ Stop webapp1

**Explanation**

You can use either a CNAME record or an A record to map a custom DNS name to App Service.

**Reference:**

https://docs.microsoft.com/en-us/Azure/app-service/app-service-web-tutorial-custom-domain

**Quick Preview:**

Question 22: Skipped

***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.***

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

Larger image

VM1 connects to VNET1. You need to connect VM1 to VNET2.

***Solution***: You move VM1 to RG2, and then you add a new network interface to VM1.

Does this meet the goal?

- ○ Yes
- ○ No (Correct)

**Explanation**
Instead you should delete VM1. You recreate VM1, and then you add the network interface for VM1.

When you create an Azure virtual machine (VM), you must create a virtual network (vNET) or use an existing vNET. You can change the subnet a VM is connected to after it's created, but you cannot change the vNET.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/network-overview

**Quick Preview:**

Question 23: Skipped
***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.***

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

Larger image

VM1 connects to VNET1. You need to connect VM1 to VNET2.

***Solution:*** You delete VM1. You recreate VM1, and then you create a new network interface for VM1 and connect it to VNET2.

Does this meet the goal?

- ○ Yes (Correct)
- ○ No

**Explanation**

The solution meets the goal. You should delete VM1. You recreate VM1, and then you add the network interface for VM1.

When you create an Azure virtual machine (VM), you must create a virtual network (vNET) or use an existing vNET. You can change the subnet a VM is connected to after it's created, but you cannot change the vNET.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/network-overview

**Quick Preview:**

Question 24: Skipped

***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.***

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

Larger image

VM1 connects to VNET1. You need to connect VM1 to VNET2.

***Solution:*** You turn off VM1, and then you add a new network interface to VM1.

Does this meet the goal?

- ○ Yes

- ○ No (Correct)

**Explanation**
Instead you should delete VM1. You recreate VM1, and then you add the network interface for VM1.

When you create an Azure virtual machine (VM), you must create a virtual network (vNET) or use an existing vNET. You can change the subnet a VM is connected to after it's created, but you cannot change the vNET.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/network-overview

**Quick Preview:**

Question 25: Skipped

***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.***

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

Larger image

VM1 connects to VNET1. You need to connect VM1 to VNET2.

***Solution:*** You create a new network interface, and then you add the network interface to VM1.

Does this meet the goal?

- ○ Yes
- ○ No (Correct)

**Explanation**
Instead you should delete VM1. You recreate VM1, and then you add the network interface for VM1.

When you create an Azure virtual machine (VM), you must create a virtual network (vNET) or use an existing vNET. You can change the subnet a VM is connected to after it's created, but you cannot change the vNET.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/network-overview

**Quick Preview:**

Question 26: Skipped
You have an Azure subscription named Subscription1 that contains the quotas shown in the following table:
Larger image

You deploy virtual machine to Subscription1 as shown in the following table:
Larger image

You plan to deploy the virtual machines shown in the following table:
Larger image

`True` or `False`.

You can deploy VM3 to West US.

- ○ True (Correct)
- ○ False

**Explanation**
Quota is calculated based on the total number of cores in use, both allocated and deallocated. This means that with VM1 and VM20 deployed, currently 2+16=18 vCPUs are already used, out of 20 vCPUs total - the quota.

As VM3 size is 1 vCPU, VM3 can be deployed to West US, reaching 19 vCPUs out of maxim 20 vCPUs.

**Reference:**

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

**Quick Preview:**

Question 27: Skipped
You have an Azure subscription named Subscription1 that contains the quotas shown in the following table:
Larger image

You deploy virtual machine to Subscription1 as shown in the following table:
Larger image

You plan to deploy the virtual machines shown in the following table:
Larger image

`True` or `False`.

You can deploy VM4 to West US.

- ○ True
- ○ False (Correct)

**Explanation**
Quota is calculated based on the total number of cores in use, both allocated and deallocated. This means that with VM1 and VM20 deployed, currently 2+16=18 vCPUs are already used, out of 20 vCPUs total - the quota.

As VM4 size is 4 vCPU, VM4 can't be deployed to West US, because it will be over the quota, reaching 18+4=22 vCPUs out of maxim 20 vCPUs.

**Reference:**

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

**Quick Preview:**

Question 28: Skipped
You have an Azure subscription named Subscription1 that contains the quotas shown in the following table:
Larger image

You deploy virtual machine to Subscription1 as shown in the following table:

Larger image

You plan to deploy the virtual machines shown in the following table:

Larger image

`True` or `False`.

You can deploy VM5 to West US.

- ○ True
- ○ False (Correct)

**Explanation**
Quota is calculated based on the total number of cores in use, both allocated and deallocated. This means that with VM1 and VM20 deployed, currently 2+16=18 vCPUs are already used, out of 20 vCPUs total - the quota.

As VM5 size is 16 vCPU, VM5 can't be deployed to West US, because it will be over the quota, reaching 18+16=34 vCPUs out of maxim 20 vCPUs.

**Reference:**

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

**Quick Preview:**

Question 29: Skipped
You have an Azure subscription that contains an Azure Availability Set named WEBPROD-AS-USE2 as shown in the following exhibit:
Larger image

You add 14 virtual machines to WEBPROD-AS-USE2.

When Microsoft performs planned maintenance in EastUS2, the maximum number of unavailable virtual machines will be .......... .

- ○ 2 (Correct)
- ○ 7
- ○ 10
- ○ 14

**Explanation**

You can protect your apps against planned maintenance windows using update domains. Deploying your VMs in different update domains can help a lot, because VMs deployed in different update domains are not restarted/rebooted at the same time.

For this scenario, we have 14 VMs and 10 update domains. The first 10 VMs are split into the 10 update domains, and the rest of 4 VMs will be split through 4 of the update domains. In the end, there will be 4 update domains with 2 VMs each, and 6 update domains with 1 VM each.

This leads to having maximum 2 VMs unavailable when an update domain is restarted.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/manage-availability

**Quick Preview:**

Question 30: Skipped

You have an Azure subscription that contains an Azure Availability Set named WEBPROD-AS-USE2 as shown in the following exhibit:

Larger image

You add 14 virtual machines to WEBPROD-AS-USE2.

If the server rack in the Azure data center that hosts WEBPROD-AS-USE2 experiences a power failure, the maximum number of unavailable virtual machines will be .......... .

- ○
  2
- ○
  7
  (Correct)
- ○
  10
- ○
  14

**Explanation**

You can protect your apps against unplanned maintenance windows using fault domains. Deploying your VMs in different fault domains can help a lot, because VMs deployed in different fault domains are actually deployed on different servers in an Azure data center.

For this scenario, we have 14 VMs and 2 fault domains, and because VMs are equally split between fault domains, each fault domain will have 7 VMs.

This leads to having maximum 7 VMs unavailable when an unexpected power failure occurs, as one failure affects one fault domain.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/manage-availability

**Quick Preview:**

Question 31: Skipped

You deploy an Azure Kubernetes Service (AKS) cluster named Cluster1 that uses the IP addresses shown in the following table:

Larger image

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 Cluster1?

- ○
  131.107.2.1
  (Correct)
- ○
  10.0.10.11

- ○
  172.17.7.1
- ○
  192.168.10.2

**Explanation**
Users connect to the Load Balancer front end IP address in order to access the application. For this reason, a DNS mapping needs to be configured using the Load Balancer frontend IP.

Reference:

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

Quick Preview:

Question 32: Skipped
You have a deployment template named Template1 that is used to deploy 10 Azure web apps. You need to identify what to deploy before you deploy Template1. The solution must minimize Azure costs.

What should you identify

- ○
  five Azure Application Gateways
- ○
  one App Service plan
  **(Correct)**
- ○
  10 App Service plans
- ○
  one Azure Traffic Manager
- ○
  one Azure Application Gateway

**Explanation**
You can deploy multiple Azure web apps in a single App Service plan.

**Reference:**

https://docs.microsoft.com/en-us/azure/app-service/overview-hosting-plans

**Quick Preview:**

Question 33: Skipped
You plan to deploy an Azure container instance by using the following Azure Resource Manager template:
Larger image

Internet users .......... .

- ○
  can connect to the container from any device.
  (Correct)
- ○
  cannot connect to the container.
- ○
  can only connect to the container from devices that run Windows.

**Explanation**
Taking a closer look at the ARM template, Internet users can connect to the container because of this ARM line: "type": "Public", so the container is publicly accessible. Users can connect from any OS, the ***osType : Windows*** defined in the template represents the OS running on the container.

**Further Learning:**

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-overview

**Quick Preview:**

Question 34: Skipped
You plan to deploy an Azure container instance by using the following Azure Resource Manager template:
Larger image

If Internet Information Services (IIS) in the container fails ..........

- ○
  the container will restart automatically.
  (Correct)
- ○
  the container will only restart manually.
- ○
  the container must be redeployed.

**Explanation**

The container restart policy configured in the ARM template is OnFailure, which ensures that containers are restarted automatically if the application fails - IIS.

**Reference:**

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-restart-policy

**Quick Preview:**

Question 35: Skipped

You have an Azure subscription that contains a virtual machine named VM1. VM1 hosts a line-of-business application that is available 24 hours a day. VM1 has one network interface and one managed disk. VM1 uses the D4s v3 size.

You plan to make the following changes to VM1:

- Change the size to D8s v3.

- Add a 500-GB managed disk.

- Add the Puppet Agent extension.

- Enable Desired State Configuration Management.

Which change will cause downtime for VM1?

- ○ Enable Desired State Configuration Management.
- ○ Add the Puppet Agent extension.
- ○ Add a 500-GB managed disk.
- ○ Change the size to D8s v3. (Correct)

**Explanation**

As per official documentation, resizing the VM will lead to VM restart.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/resize-vm

**Quick Preview:**

Question 36: Skipped

You have an Azure subscription. The subscription contains virtual machines that run Windows Server 2016 and are configured as shown in the following table:

Larger image

You create a public Azure DNS zone named adatum.com and a private Azure DNS zone named az104exam.com.

You create a virtual network link for az104exam.com as shown in the following exhibit:

Larger image

`True` or `False`.

When VM1 starts, a record for VM1 is added to the az104exam.com DNS zone.

- ○ True (Correct)
- ○ False

**Explanation**

A virtual network link was created for az104exam.com and auto registration is enabled, so a record is added for VM1, once it starts.

**Reference:**

https://docs.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links

**Quick Preview:**

Question 37: Skipped

You have an Azure subscription. The subscription contains virtual machines that run Windows Server 2016 and are configured as shown in the following table:

Larger image

You create a public Azure DNS zone named adatum.com and a private Azure DNS zone named az104exam.com.

You create a virtual network link for az104exam.com as shown in the following exhibit:

Larger image

`True` or `False`.

When VM2 starts, a record for VM2 is added to the az104exam.com DNS zone.

- ○ True (Correct)
- ○ False

**Explanation**
A virtual network link was created for az104exam.com and auto registration is enabled, so a record is added for VM2, once it starts.

**Reference:**

https://docs.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links

**Quick Preview:**

Question 38: Skipped
You have an Azure subscription. The subscription contains virtual machines that run Windows Server 2016 and are configured as shown in the following table:
Larger image

You create a public Azure DNS zone named adatum.com and a private Azure DNS zone named az104exam.com.

You create a virtual network link for az104exam.com as shown in the following exhibit:

Larger image

`True` or `False`.

When VM3 starts, a record for VM3 is added to the adatum.com DNS zone.

- ○
  True
- ○
  False
  (Correct)

**Explanation**
A virtual network link was created for az104exam.com and ***not*** adatum.com. When VM3 starts, a record for VM3 is ***NOT*** added to the adatum.com DNS zone.

**Reference:**

https://docs.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links

**Quick Preview:**

Question 39: Skipped
You have an Azure subscription that contains the resources in the following table:
Larger image

To which subnets can you apply NSG1?

- ○
  the subnets on VNet1 only
- ○
  the subnets on VNet2 and VNet3 only
- ○
  the subnets on VNet2 only
- ○
  the subnets on VNet3 only
  (Correct)
- ○
  the subnets on VNet1, VNet2, and VNet3

**Explanation**
NSGs can only be associated to resources within the same region as the NSG. For this reason, you can apply NSG1 only to VNET3.

**Further Learning:**

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

**Quick Preview:**

Question 40: Skipped

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2. Virtual machines connect to the virtual networks.

The virtual networks have the address spaces and the subnets configured as shown in the following table:

Larger image

You need to add the address space of 10.33.0.0/16 to VNet1. The solution must ensure that the hosts on VNet1 and VNet2 can communicate.

Which three actions should you perform in sequence?

(1) Remove VNet1

(2) Add 10.33.0.0/16 address space to VNet1

(3) Create a new virtual network name VNet1

(4) On the peering connection in VNet2, allow gateway transit

(5) Recreate peering between VNet1 and VNet2

(6) On the peering connection in VNet1, allow gateway transit

(7) Remove peering between VNet1 and VNet2

- ○ 1 - 2- 5
- ○ 1 - 2 - 3
- ○ 7 - 2 - 5 (Correct)
- ○ 7 - 1 - 2

**Explanation**

***Step 1:*** You can't add address ranges to, or delete address ranges from a virtual network's address space once a virtual network is peered with another virtual network. To add or remove address ranges, delete the peering, add or remove the address ranges, then re-create the peering.

***Step 2:*** Add 10.33.0.0/16 to VNet1

***Step 3:*** Recreate peering between VNet1 and VNet2.

**Further Learning:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering

**Quick Preview:**

Question 41: Skipped

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

Larger image

RG1 contains the resources shown in the following table:

Larger image

VM1 is running and connects to NIC1 and Disk1. NIC1 connects to VNET1. RG2 contains a public IP address named IP2 that is in the East US location. IP2 is not assigned to a virtual machine.

`True` or `False`

You can move storage1 to RG2.

- ○ True (Correct)
- ○ False

**Explanation**

You are allowed to move to RG2, in East US, the following resources:

- Storage1 storage account

- Disk1 disk

- NIC1 network interface card

Please note that region for these resources doesn't change, just the resource group itself, from RG1 to RG2.

**Further Learning:**

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/move-vm

**Quick Preview:**

Question 42: Skipped

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

Larger image

RG1 contains the resources shown in the following table:

Larger image

VM1 is running and connects to NIC1 and Disk1. NIC1 connects to VNET1. RG2 contains a public IP address named IP2 that is in the East US location. IP2 is not assigned to a virtual machine.

`True` or `False`

You can move NIC1 to RG2.

- ○ True (Correct)
- ○ False

**Explanation**

You are allowed to move to RG2, in East US, the following resources:

- Storage1 storage account

- Disk1 disk

- NIC1 network interface card

Please note that region for these resources doesn't change, just the resource group itself, from RG1 to RG2.

**Further Learning:**

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/move-vm

**Quick Preview:**

Question 43: Skipped

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

Larger image

RG1 contains the resources shown in the following table:

Larger image

VM1 is running and connects to NIC1 and Disk1. NIC1 connects to VNET1. RG2 contains a public IP address named IP2 that is in the East US location. IP2 is not assigned to a virtual machine.

`True` or `False`

If you move IP2 to RG1, the location of IP2 will change.

- ○ True
- ○ False (Correct)

**Explanation**

If you move IP2 (deployed in RG2 - East US) to RG1 - West US, the location doesn't change, only the resource group itself.

**Further Learning:**

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/move-vm

**Quick Preview:**

Question 44: Skipped

You have an Azure web app named webapp1. You have a virtual network named VNET1 and an Azure virtual machine named VM1 that hosts a MySQL database. VM1 connects to VNET1.

You need to ensure that webapp1 can access the data hosted on VM1.

What should you do?

- ○ Deploy an internal load balancer
- ○ Peer VNET1 to another virtual network
- ○ Connect webapp1 to VNET1 (Correct)
- ○ Deploy an Azure Application Gateway

**Explanation**

In order for webapp1 to access the data hosted on VM1, webbapp1 needs to be connected to VNET1, where VM1 is deployed.

This basically means integrating the app with the Azure vNET - VNET1.

**Reference:**

https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet

**Quick Preview:**

Question 45: Skipped

Your company has a main office in London that contains 100 client computers. Three years ago, you migrated to Azure Active Directory (Azure AD). The company's security policy states that all personal devices and corporate-owned devices must be registered or joined to Azure AD.

A remote user named User1 is unable to join a personal device to Azure AD from a home network. You verify that User1 was able to join devices to Azure AD in the past. You need to ensure that User1 can join the device to Azure AD.

What should you do?

- ○ Assign the User administrator role to User1
- ○ From the Device settings blade, modify the ***Maximum number of devices per user*** setting (Correct)
- ○ Create a point-to-site VPN from the home network of User1 to Azure

- ○
  From the Device settings blade, modify the Users may join devices to Azure AD setting

**Explanation**

The Maximum number of devices setting enables you to select the maximum number of devices that a user can have in Azure AD. If a user reaches this quota, they will not be able to add additional devices until one or more of the existing devices are removed.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

**Quick Preview:**

Question 46: Skipped

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

Larger image

VMSS1 is set to VM (virtual machines) orchestration mode.

You need to deploy a new Azure virtual machine named VM1, and then add VM1 to VMSS1.

Which resource group and location should you use to deploy VM1? (SELECT TWO)

- □
  Resource group - RG1 only
- □
  Resource group - RG2 only
- □
  Resource group - RG1 or RG2 only
- □
  Resource group - RG1, RG2 or RG3
  **(Correct)**
- □
  Location - West US only
  **(Correct)**
- □
  Location - Central US only

- □ Location - Central US or West US
- □ Location - East US, Central US or West US

**Explanation**

The resource group stores metadata about the resources. When you specify a location for the resource group, you're specifying where that metadata is stored.

Virtual machine scale sets will support 2 distinct orchestration modes:

ScaleSetVM – Virtual machine instances added to the scale set are based on the scale set configuration model. The virtual machine instance lifecycle - creation, update, deletion - is managed by the scale set.

VM (virtual machines) – Virtual machines created outside of the scale set can be explicitly added to the scale set.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/orchestration-modes

**Quick Preview:**

Question 47: Skipped

Peering for VNET2 is configured as shown in the following exhibit:

Larger image

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

Larger image

Where can packets from VNET1 be routed to?

- ○ VNET2 only
- ○ VNET3 only
- ○ VNET2 and VNET3 (Correct)

**Explanation**

VNET1 is peered with both VNET2 and VNET3, so communication from VNET1 to either VNET2 or VNET3 is working.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

**Quick Preview:**

Question 48: Skipped

Peering for VNET2 is configured as shown in the following exhibit:

Larger image

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

Larger image

Where can packets from VNET2 be routed to?

- ○ VNET1 (Correct)
- ○ VNET3
- ○ VNET1 and VNET3

**Explanation**

VNET1 is peered with both VNET2 and VNET3, so communication from VNET1 to either VNET2 or VNET3 is working.

On the other hand VNET2 can communicate to VNET1 only, as a peering is configured. VNET2 can't communicate with VNET3 because ***Gateway transit*** configuration option is not enabled on VNET1.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

**Quick Preview:**

Question 49: Skipped

Peering for VNET2 is configured as shown in the following exhibit:

Larger image

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

Larger image

Where can packets from VNET3 be routed to?

- ○ VNET1 only (Correct)
- ○ VNET2 only
- ○ VNET1 and VNET2

**Explanation**
VNET1 is peered with both VNET2 and VNET3, so communication from VNET1 to either VNET2 or VNET3 is working.

On the other hand VNET3 can communicate to VNET1 only, as a peering is configured. VNET3 can't communicate with VNET2 because ***Gateway transit*** configuration option is not enabled on VNET1.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

**Quick Preview:**

Question 50: Skipped
You have an Azure virtual machine named VM1. Azure collects events from VM1. You are creating an alert rule in Azure Monitor to notify an administrator when an error is logged in the System event log of VM1.

Which target resource should you monitor in the alert rule?

- ○ virtual machine extension
- ○

virtual machine

- ○
  metric alert
- ○
  Azure Log Analytics workspace
  (Correct)

**Explanation**
Azure Monitor maximises the availability and performance of your applications by delivering a comprehensive solution for collecting, analysing, and transmission of events from your Azure cloud and on-premises environments.

The questions states that you are creating an alert rule for monitoring and alerting purposes. When a new error is detected and logged, the alert rule will be triggered and the Administrator will receive an alert, an email for example.

When you define the alert in Azure Portal, as a first step, under the **Create Alert** section, you are going to select your ***Log Analytics workspace*** as the resource, since this is a log based alert signal. For this reason, the target resource that you need to monitor in the alert rule is the ***Azure Log Analytics workspace.***

**Reference:**

https://docs.microsoft.com/en-us/windows-server/storage/storage-spaces/configure-azure-monitor

**Quick Preview:**

Question 51: Skipped
You have an Azure subscription that contains 100 virtual machines. You regularly create and delete virtual machines. You need to identify unattached disks that can be deleted.

What should you do?

- ○
  From Azure Cost Management, view Cost Analysis
- ○
  From Azure Advisor, modify the Advisor configuration
- ○
  From Microsoft Azure Storage Explorer, view the Account Management properties
- ○
  From Azure Cost Management, view Advisor Recommendations
  (Correct)

**Explanation**
Let's analyse each option and we will start with the **first one - From Azure Cost Management, view Cost Analysis**.

This is not a valid option, from the ***Cost Analysis*** blade you can, by default, identify what type of service is generating costs, so in this case ***storage*** represents the Virtual Hard Disk drives:

If you change the ***Service name*** category (top left corner) to ***Resource***, you can see the exact resource, or hard disk drive that is generating the cost, in this case ***vm-az-104-exam_disk1 ... etc ...***

but you can't figure it out if the disk is attached or not to a VM! We need to identify unattached disks that can be deleted, so this answer is not a valid option.

Option 2 - **From Azure Advisor, modify the Advisor configuration** is also wrong. There is no configuration that needs to be modified so that we can identify unattached disks. Actually, Azure Advisor provides these recommendations, will all default configuration.

Option 3 - **From Microsoft Azure Storage Explorer, view the Account Management properties** is partially correct, which makes this option incorrect. If you connect to your Azure subscription using Azure Storage Explorer, and take a look at Account properties, information presented doesn't help to solve the task presented in this scenario. Please take a look below:

The information presented in the Account properties is not related to unattached disks. I mentioned earlier that this option is partially correct. Here's why. You can use Azure Storage Explorer tool to identify unattached disks.

While in Azure Storage Explorer, you can expand your subscription, then expand Disks, and you can check in your resource groups for any ***Unattached*** *Disks*. Here's an example below:

So yes, you can use Azure Storage Explorer to identify unattached disks, but not by taking a look at Account Management properties.

And the last option - **From Azure Cost Management, view Advisor Recommendations**, which is True. Any unattached disks will appear here. Please note that if you will try this in Azure Portal, by deleting an Azure VM, but keeping the Disks, the recommendations will not appear immediately, under ***Advisor Recommendations.*** It will take some time, but the recommendations will eventually be available under Advisor Recommendations.

**Reference:**

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

**Quick Preview:**

Question 52: Skipped

***Case study***

***This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.***

***To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.***

***Overview***

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

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

***Existing Environment***

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

- File servers

- Domain controllers

- Microsoft SQL Server servers

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

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

- A SQL database

- A web front end

- A processing middle tier

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

**Requirements**

**Planned Changes**

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.

- Move the existing product blueprint files to Azure Blob storage.

- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

***Technical Requirements***

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.

- Minimize the number of open ports between the App1 tiers.

- Ensure that all the virtual machines for App1 are protected by backups.

- Copy the blueprint files to Azure over the Internet.

- Ensure that the blueprint files are stored in the archive storage tier.

- Ensure that partner access to the blueprint files is secured and temporary.

- Prevent user passwords or hashes of passwords from being stored in Azure.

- Use unmanaged standard storage for the hard disks of the virtual machines.

- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

- Minimize administrative effort whenever possible.

***User Requirements***

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.

- Designate a new user named Admin1 as the service admin for the Azure subscription.

- Admin1 must receive email alerts regarding service outages.

- Ensure that a new user named User3 can create network objects for the Azure subscription.

**QUESTION 1**

You need to recommend a solution for App1. The solution must meet the technical requirements.

What should you include in the recommendation? (SELECT TWO)

- ☐ Number of virtual network - 1 (Correct)
- ☐ Number of virtual network - 2
- ☐ Number of virtual network - 3
- ☐ Number of subnets per virtual network - 1
- ☐ Number of subnets per virtual network - 2
- ☐ Number of subnets per virtual network - 3 (Correct)

**Explanation**

This reference architecture shows how to deploy VMs and a virtual network configured for an N-tier application, using SQL Server on Windows for the data tier.

**From the Scenario:**

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

- A SQL database

- A web front end

- A processing middle tier

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

Technical requirements include:

- Move all the virtual machines for App1 to Azure.

- Minimize the number of open ports between the App1 tiers.

Question 1: Skipped

You have an Azure Active Directory (Azure AD) tenant. You need to create a conditional access policy that requires all users to use multi-factor authentication when they access the Azure portal.

Which three settings should you configure?  NOTE: Each correct selection is worth one point.

Larger image

- □ 1 (Correct)
- □ 2 (Correct)
- □ 3
- □ 4 (Correct)
- □ 5

**Explanation**

Multi-factor authentication (MFA) is a process where a user is prompted during a sign-in event for additional forms of identification. So, after the user provides username and password, you can request for example the user to enter a code received through an SMS on mobile phone, or maybe a code received in an app installed on the mobile phone. One common option to use is Microsoft Authentication, available for both iOS and Android.

In order to secure access to Azure portal, you can implement Multi-factor authentication through a conditional access policy.

You would first need to configure and select where will the conditional policy apply - so this is **option 1 - Users and Groups**.

In order to enable MFA for Azure portal access, you would need to select **option 2 - Cloud apps or actions** and choose **Microsoft Azure Management,** so the policy applies to sign-in events to the Azure portal.

Last, but not least, you would need to select **option 4 - Grant**, under Access controls, and make sure that **Grant access** radio button is selected, and check the box for **Require multi-factor authentication**.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa

**Quick Preview:**

Question 2: Skipped

You have an Azure Active Directory (Azure AD) tenant named x-a-a-s.onmicrosoft.com.

The User administrator role is assigned to a user named Admin1. An external partner has a Microsoft account that uses the user1@outlook.com sign in.

Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: ***“Unable to invite user user1@outlook.com – Generic authorisation exception.”***

You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.

What should you do?

- ○ From the Users blade, modify the External collaboration settings. **(Correct)**
- ○ From the Custom domain names blade, add a custom domain.
- ○ From the Organizational relationships blade, add an identity provider.
- ○ From the Roles and administrators blade, assign the Security administrator role to Admin1.

**Explanation**

"Generic Authorization error" means that Admin1 doesn't have the necessary permission to invite user1.

In order to solve this issue, Admin1 can navigate to **User settings** and select **Manage external collaboration settings**, right under **External**

Because user1 is an external partner, so it's a Guest user, the relevant part to take a look at is the **Guest invite settings**:

Selecting the **Yes** options here will allow Admin1 to invite user1, and no error will be displayed in this case.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#guest-inviter

**Quick Preview:**

Question 3: Skipped

You have an Azure subscription linked to an Azure Active Directory tenant. The tenant includes a user account named User1.

You need to ensure that User1 can assign a policy to the tenant root management group.

What should you do?

- ○ Assign the Owner role for the Azure Subscription to User1, and then modify the default conditional access policies.
- ○ Assign the Owner role for the Azure subscription to User1, and then instruct User1 to configure access management for Azure resources. (Correct)
- ○ Assign the Global administrator role to User1, and then instruct User1 to configure access management for Azure resources.
- ○ Create a new management group and delegate User1 as the owner of the new management group.

**Explanation**

In Azure, resources are deployed and available in a hierarchy, for easy management and administration purposes. At the top of the hierarchy is the Root management group. The Root management group is a container for your Azure subscriptions, but it can also include management groups that you manually define.

Moving down the hierarchy, Azure subscriptions include resource groups, and resource groups include the Azure resources. Here's a visual representation of Azure hierarchy levels:

The Root management group allows for global policies and Azure role assignments to be applied at the directory level. The Azure AD Global Administrator needs to elevate themselves to the User Access Administrator role of this root group initially. After elevating access, the administrator can assign any Azure role to other directory users or groups to manage the hierarchy. **So, coming back to this question, with the User Access Administrator role assigned, the Administrator can now assign any Azure role to User1, so that User1 can perform its job.**

What role needs to be assigned to User1?

The following chart shows the list of roles and the supported actions on management groups:

As you can see, User1 would need one of the three roles marked in the **Assign Policy** column, to be allowed to assign a policy to the tenant root management group. Taking a look at the available answer options, the only answer that fits is **Answer B - Assign the Owner role for the Azure subscription to User1**.

**Reference:**

https://docs.microsoft.com/en-us/azure/governance/management-groups/overview

**Quick Preview:**

Question 4: Skipped

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains the users shown in the following table:

Larger image

You need to modify the JobTitle and UsageLocation attributes for the users.

For which users can you modify the attributes from Azure AD? (Select TWO)

- □ JobTitle - User1 only
- □ JobTitle - User1 and User2 only
- □

JobTitle - User1 and User3 only
(Correct)

- □
  JobTitle - User1, User2 and User3
- □
  UsageLocation: User1 only
- □
  UsageLocation: User1 and User2 only
- □
  UsageLocation: User1 and User3 only
- □
  UsageLocation: User1, User2 and User3
  (Correct)

**Explanation**

The key information for this question is the last column - **Source.** One thing to note is that users that come from Windows Server Active Directory can be updated **only** from Windows Server Active Directory. This leaves us **only User1 and User3** that you can use Azure Active Directory to update the JobTitle.

The above mentioned restriction applies only for identity, contact info, or job info for users whose source of authority is Windows Server Active Directory. As this limitation doesn't apply for UsageLocation, you can use **Azure AD to update UsageLocation field for all users : User1, User2 and User3.**

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-profile-azure-portal

**Quick Preview:**

Question 5: Skipped

***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.***

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 Network Contributor role at the subscription level to Admin1.`

Does this meet the goal?

- ○ Yes (Correct)
- ○ No

**Explanation**
In order for a user to be allowed to enable Traffic Analytics for an Azure subscription, the user must have one of the following roles assigned at the subscription level: owner, contributor, reader, or network contributor.

Since the proposed solution is to assign the Network Contributor role to Admin1, Admin1 will be allowed to enable Traffic Analytics for the Azure subscription.

**Reference:**

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq

**Quick Preview:**

Question 6: Skipped
***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.***

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?

- ○ Yes (Correct)
- ○ No

**Explanation**

In order for a user to be allowed to enable Traffic Analytics for an Azure subscription, the user must have one of the following roles assigned at the subscription level: owner, contributor, reader, or network contributor.

Since the proposed solution is to assign the Owner role to Admin1, Admin1 will be allowed to enable Traffic Analytics for the Azure subscription.

**Reference:**

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq

**Quick Preview:**

Question 7: Skipped

***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.***

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 Reader role at the subscription level to Admin1.
```

Does this meet the goal?

- ○ Yes (Correct)
- ○ No

**Explanation**

In order for a user to be allowed to enable Traffic Analytics for an Azure subscription, the user must have one of the following roles assigned at the subscription level: owner, contributor, reader, or network contributor.

Since the proposed solution is to assign the Reader role to Admin1, Admin1 will be allowed to enable Traffic Analytics for the Azure subscription.

**Reference:**

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq

**Quick Preview:**

Question 8: Skipped

You have an Azure subscription that contains a user named User1. You need to ensure that User1 can deploy virtual machines and manage virtual networks. The solution must use the principle of least privilege.

Which role-based access control (RBAC) role should you assign to User1?

- ○ Owner
- ○ Virtual Machine Contributor
- ○ Contributor
  (Correct)
- ○ Virtual Machine Administrator Login

**Explanation**

One important aspect is that we need to assign a role to User1, and the proposed solution must use the principle of least privilege. This means that we need to assign a role to User1 that includes the minimum permissions, so that User1 can deploy virtual machines and manage virtual networks, **but no extra permissions !** Simply put, User1 shouldn't be allowed to perform more than deploying virtual machines and managing virtual networks.

Let's take it one by one:

- **Owner** role: Grants full access to manage all resources, including the ability to assign roles in Azure RBAC; this role allows User1 to perform more actions than needed, so this option is incorrect.

- **Virtual Machine Contributor** role: Lets you manage virtual machines, but not access to them, **and not the virtual network** or storage account they're connected to; this role doesn't allow managing virtual networks, so it doesn't fulfil the minimum requirements.

- **Virtual Machine Administrator Login** role: View Virtual Machines in the portal and login as administrator; this role allows User1 to only read virtual machines, so it doesn't fulfil the minimum requirements.

The only one that fits the requirements is the **Contributor** role, which grants full access to manage all resources ( but does not allow you to assign roles in Azure RBAC). This means that User1 will be able to manage virtual machines and associated virtual networks.

**Reference:**

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

**Quick Preview:**

Question 9: Skipped
You plan to use the Azure Import/Export service to copy files to a storage account.

Which two files should you create before you prepare the drives for the import job? Each correct answer presents part of the solution.

- □ an XML manifest file
- □ a dataset CSV file (Correct)
- □ a JSON configuration file
- □ a PowerShell PS1 file
- □ a driveset CSV file (Correct)

**Explanation**
You need to modify the ***dataset.csv*** file in the root folder where the tool resides. Depending on whether you want to import a file or folder or both, add entries in the dataset.csv file.

You need also to modify the ***driveset.csv*** file in the root folder where the tool is. The driveset file has the list of disks and corresponding drive letters so that the tool can correctly pick the list of disks to be prepared.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-data-to-files?tabs=azure-portal

**Quick Preview:**

Question 10: Skipped

You have a Recovery Service vault that you use to test backups. The test backups contain two protected virtual machines. You need to delete the Recovery Services vault.

What should you do first?

- ○ From the Recovery Service vault, delete the backup data
- ○ Modify the disaster recovery properties of each virtual machine
- ○ Modify the locks of each virtual machine
- ○ From the Recovery Service vault, stop the backup of each backup item (Correct)

**Explanation**

You can't delete a Recovery Services Vault that contains protected data sources, for example IaaS virtual machines (VMs), or backup data. If you try to perform such an action, you will receive an error and the action will fail.

In order to delete a vault, there are several steps that need to be performed first, as follows:

- Disable the soft delete feature; soft delete still keeps the deleted data available for some time, before complete removal

- **Stop any ongoing backups**

- Ensure all registered storage accounts are deleted

- And last, delete the actual vault

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault

**Quick Preview:**

Question 11: Skipped

You have an Azure subscription named Subscription1 that contains the resources shown in the following table:

Larger image

In Storage1, you create a blob container named blob1 and a file share named share1.

Which resources can be backed up to Vault1 and Vault2? (Select two)

- □
  Can use Vault1 for backups - VM1 only
  (Correct)
- □
  Can use Vault1 for backups - VM1 and share1 only
- □
  Can use Vault1 for backups - VM1 and SQL1
- □
  Can use Vault1 for backups - VM1, Storage1 and SQL1 only
- □
  Can use Vault1 for backups - VM1, blob1, share1 and SQL1
- □
  Can use Vault2 for backups - Storage1 only
- □
  Can use Vault2 for backups - share1 only
  (Correct)
- □
  Can use Vault2 for backups - VM1 and share1 only
- □
  Can use Vault2 for backups - blob1 and share1 only
- □
  Can use Vault2 for backups - storage1 and SQL1 only

**Explanation**

The key information for such scenarios is the following: **To create a vault to protect any data source, the vault *must* be in the same region as the data source.**

So now, it's really easy to find the correct answers, let's start with Vault1. Vault1 is deployed in Central US and the only resource deployed in Central US is VM1. This clarifies the first correct answer:

**Can use Vault1 for backups - VM1 only**

Vault2 has been deployed in West US and the only resource deployed in West US is Storage1. Storage1 storage account includes a blob container named blob1 and a file share named share1. At this moment, there are two answers left to evaluate:

**Can use Vault2 for backups - share1 only**

and

**Can use Vault2 for backups - blob1 and share1 only**

As blobs can't be backed up using Recovery Services vaults, and only Azure file shares, this clarifies the second correct answer for this question: **Can use Vault2 for backups - share1 only**

**Reference:**

https://docs.microsoft.com/bs-cyrl-ba/azure/backup/backup-create-rs-vault

https://docs.microsoft.com/en-us/azure/backup/backup-afs

**Quick Preview:**

Question 12: Skipped

You have an Azure subscription named Subscription1. You have 5 TB of data that you need to transfer to Subscription1 and you plan to use an Azure Import/Export job.

What can you use as the destination of the imported data?

- ○ a virtual machine
- ○ an Azure Cosmos DB database
- ○ Azure File Storage (Correct)
- ○ the Azure File Sync Storage Sync Service

**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. Also, please note that the maximum size of an Azure Files Resource of a file share is 5 TB.

Again, although not available as an option in this question, a valid destination could also be a blob container, inside an Azure storage account.

**Reference:**

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

**Quick Preview:**

Question 13: Skipped
You have an Azure subscription. You create the Azure Storage account shown in the following exhibit:
Larger image

Please select the answer choice that completes the following statement based on the information presented in the graphic.

The minimum number of copies of the storage account will be .......... .

- ○ 1
- ○ 2
- ○ 3 (Correct)
- ○ 4

**Explanation**
Taking a look at ***az104practicetests*** storage account configuration, we can see that the storage account replication chosen in this case is **Locally redundant storage (LRS).**

**LRS copies your data synchronously three times** within a single physical location, in the primary region. LRS is the least expensive replication option, but is not recommended for applications requiring high availability.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

**Quick Preview:**

Question 14: Skipped
You have an Azure subscription. You create the Azure Storage account shown in the following exhibit:
Larger image

Please select the answer choice that completes the following statement based on the information presented in the graphic.

To reduce the cost of infrequently accessed data in the storage account, you must modify the .......... setting.

- ○ Access tier (default)
  **(Correct)**
- ○ Performance
- ○ Account kind
- ○ Replication

**Explanation**

Azure storage offers different access tiers, allowing you to store blob object data in the most cost-effective manner. Currently, there are three access tiers available, as follows:

**Hot** - Optimized for storing data that is accessed frequently.

**Cool** - Optimized for storing data that is infrequently accessed and stored for at least 30 days.

**Archive** - Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements, on the order of hours.

As the question refers to infrequently accessed data, you would need to modify the current access tier (Hot) to Cool access tier. Also, please note that the cheapest storage tier is the Archive tier, which should be used for rarely accessed data.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers

**Quick Preview:**

Question 15: Skipped

You have an Azure subscription that contains an Azure file share. You have an on-premises server named Server1 that runs Windows Server 2016. You plan to set up Azure File Sync between Server1 and the Azure file share.

You need to prepare the subscription for the planned Azure File Sync.

Which two actions should you perform in the Azure Subscription to configure Azure File Sync? (Select two)

- □ First Action - Create a Storage Sync Service (Correct)
- □ First Action - Install Azure File Sync Agent
- □ First Action - Create a sync group
- □ First Action - Run Server Registration
- □ Second Action - Create a Storage Sync Service
- □ Second Action - Install Azure File Sync Agent
- □ Second Action - Create a sync group (Correct)
- □ Second Action - Run Server Registration

**Explanation**
In the provided link, you can see the steps followed in the step by step process are the following:

◉ Prepare Windows Server to use with Azure File Sync

◉ Deploy the Storage Sync Service

◉ Install the Azure File Sync agent

◉ Register Windows Server with Storage Sync Service

◉ Create a sync group and a cloud endpoint

◉ Create a server endpoint

◉ Configure firewall and virtual network settings

But in the same link, you can find Onboarding with Azure File Sync section, with the following steps:

As you can see global recommended order is not followed by the example in the same page, as the Sync group is created after installing Azure File Sync Agent and registering with Storage Sync Service.

But the question is asking specifically for actions to perform in Azure Subscription, so taking in order the actions to perform in the Azure Subscription from the provided answers, the correct answers are:

◉ First Action - Create a Storage Sync Service.

◉ Second Action - Create a sync group.

The other two actions are later in the process, according to the recommended order and additionally are not performed in the Azure subscription.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide?tabs=azure-portal%2Cproactive-portal

**Quick Preview:**

Question 16: Skipped

You have an Azure subscription that contains a web app named webapp1. You need to add a custom domain named www.x-a-a-s.com to webapp1.

What should you do first?

- ○ Create a DNS record
  **(Correct)**
- ○ Add a connection string
- ○ Upload a certificate
- ○ Stop webapp1

**Explanation**

There are two options to map a custom domain, like www.x-a-a-s.com, to your webapp deployed in Azure. You can either use a CNAME record or an A DNS record.

Defining an A DNS record means mapping a public IP address to your custom domain. The result is that when users  initiate an http or https connection to your domain (https://x-a-a-s.com), the connection will be redirected to the public IP address that you defined in the A DNS record, so they will be able to access your website.

Moving one step further, you also have the option to define a CNAME DNS record. A CNAME DNS record maps a domain to another domain. An example would be mapping https://aaaa.com to https://bbbb.com. What's a common use case for this?

Let's consider that company AAAA has been acquired by company BBBB. You would naturally want customers connecting to https://aaaa.com (AAAA's company website) to be redirected to the new BBBB's website (https://bbbb.com). In order to accomplish this, you can define a CNAME record, so that when users try to connect to https://aaaa.com, their https connection gets redirected to https://bbbb.com.

**Reference:**

https://docs.microsoft.com/en-us/Azure/app-service/app-service-web-tutorial-custom-domain#map-an-a-record

**Quick preview:**

Question 17: Skipped
You have Azure subscriptions named Subscription1 and Subscription2. Subscription1 has following resource groups:
Larger image

RG1 includes a web app named App1 in the West Europe location. Subscription2 contains the following resource groups:
Larger image

Please evaluate the following statements if they are `True` or `False`:

1. App1 can be moved to RG2

2. App1 can be moved to RG3

3. App1 can be moved to RG4

- ○
  1 - False, 2 - True, 3 - True
  (Correct)
- ○
  1 - True, 2 - True, 3 - False
- ○
  1 - False, 2 - True, 3 - False
- ○

1 - False, 2 - False, 3 - True

**Explanation**
If needed, resources in Azure can be moved:

- in the same region, to a different resource group

- in a different Azure region, but same Azure subscription

- in a different Azure subscription, same or different Azure region, as compared to current one

**Statement 1:** App1 can be moved to RG2 **- False**

This operation was possible until end of May 2021, but now when you try to move a resource to a Resource Group with a Read-only lock, you get a very explicit error during the validation not allowing you to perform the move operation.

You cannot move any resource to a Resource Group with a Read-Only lock, here's how the error received from the portal Moving Web App looks like:

And error received from the portal Moving App Service plan:

Similar errors are received using AZ CLI:

**Statement 2** and **Statement 3**: App1 can be moved to RG3 / RG4 **- True**

There are some requirements that need to be met when considering moving App Service resources (web apps) to a new subscription, but this is definitely possible. Taking a look at the lock types applied on RG3 and RG4, we see that only RG3 has a lock applied - Delete lock - which means that resources inside RG3 can't be deleted, but new resources can be added to RG3.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json#considerations-before-applying-locks

https://docs.microsoft.com/en-us/azure/app-service/manage-move-across-regions

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-limitations/app-service-move-limitations

**Quick Preview:**

Question 18: Skipped

You have an Azure subscription named Subscription1 that contains the following resource group:

- Name: RG1

- Region: West US

- Tag: “tag1”: “value1”

You assign an Azure policy named Policy1 to Subscription1 by using the following configurations:

- Exclusions: None

- Policy definition: Append a tag and its value to resources

- Assignment name: Policy1

Parameters:

- Tag name: tag2

- Tag value: value2

After Policy1 is assigned, you create a storage account that has the following configuration:

- Name: storage1

- Location: West US

- Resource group: RG1

- Tags: “tag3”: “value3”

You need to identify which tags are assigned to RG1 resource.

- ○ "tag1" : "value1" only (Correct)
- ○ "tag2" : "value2" only
- ○ "tag1" : "value1" and "tag2" : "value2"

**Explanation**

Before even starting to evaluate what are the correct answers, we need to clarify one important aspect. Tags applied to the resource group or subscription aren't inherited by the resources deployed in the respective resource groups or subscriptions.

If this is something you need to achieve, you can apply tags from a subscription or resource group to the resources, using Azure Policies. One thing to note about Azure Policies is that once the Azure Policy is applied, it produces the effect only for new resources deployed.

In this question, Policy1 has the following policy definition: **Append a tag and its value to resources**. The end result is that any new resources deployed in your Azure subscription will get "tag2" : "value2" attached automatically, but Policy1 has no effects on exiting resources, already deployed in your Azure subscription.

As RG1 has been previously defined, before Policy1 has been configured, no other tags will be applied to RG1.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources

**Quick Preview:**

Question 19: Skipped

You have an Azure subscription named Subscription1 that contains the following resource group:

- Name: RG1

- Region: West US

- Tag: “tag1”: “value1”

You assign an Azure policy named Policy1 to Subscription1 by using the following configurations:

- Exclusions: None

- Policy definition: Append a tag and its value to resources

- Assignment name: Policy1

Parameters:

- Tag name: tag2

- Tag value: value2

After Policy1 is assigned, you create a storage account that has the following configuration:

- Name: storage1

- Location: West US

- Resource group: RG1

- Tags: “tag3”: “value3”

You need to identify which tags are assigned to storage1 resource.

- ○
  "tag3" : "value3" only
- ○
  "tag1" : "value1" and "tag3" : "value3" only
- ○
  "tag2" : "value2" and "tag3" : "value3" only
  (Correct)
- ○
  "tag1" : "value1", "tag2" : "value2" and "tag3" : "value3"

**Explanation**
Before even starting to evaluate what are the correct answers, we need to clarify one important aspect. Tags applied to the resource group or subscription aren't inherited by the resources deployed in the respective resource groups or subscriptions.

If this is something you need to achieve, you can apply tags from a subscription or resource group to the resources, using Azure Policies. One thing to note about Azure Policies is that once the Azure Policy is applied, it produces the effect only for new resources deployed.

In this question, Policy1 has the following policy definition: **Append a tag and its value to resources**. The end result is that any new resources deployed in your Azure subscription will get "tag2" : "value2" attached automatically, but Policy1 has no effects on exiting resources, already deployed in your Azure subscription.

Taking a look at the question, we can see that storage1 is deployed with one tag attached-> “tag3”: “value3”, and because storage1 is deployed after Policy1 is configured and applied, it will also inherit “tag2”: “value2” from Policy1. The end result is that storage1 will have ***"tag2" : "value2"*** and ***"tag3" : "value3" attached.***

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources

**Quick Preview:**

Question 20: Skipped

You have an Azure subscription named Subscription1. In Subscription1, you create an alert rule named Alert1.

The Alert1 action group is configured to send emails to all users part of the Admins_Group.  Alert1 alert criteria is triggered every minute.

The number of email messages that Alert1 will send in an hour is .......... .

- ○ 0
- ○ 4
- ○ 6
- ○ 12
- ○ 60 (Correct)

**Explanation**

Because Alert1 alert criteria is triggered every minute, this results in one email sent every minute, so 60 emails in an hour.

Please note that rate limiting is implemented by Azure, which means that there is a maximum limit of notifications to be sent, in a particular time interval. The rate limit thresholds are:

**SMS**: No more than 1 SMS every 5 minutes.

**Voice**: No more than 1 Voice call every 5 minutes.

**Email**: No more than 100 emails in an hour.

As the email limit is 100 emails in an hour, than the correct answer for this question remains **60 emails in an hour.**

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-rate-limiting

**Quick Preview:**

Question 21: Skipped

You have an Azure subscription named Subscription1. In Subscription1, you create an alert rule named Alert1.

The Alert1 action group is configured to send SMS messages to all users part of the Admins_Group.  Alert1 alert criteria is triggered every minute.

The number of SMS messages that Alert1 will send in an hour is ........... .

- ○ 0
- ○ 4
- ○ 6
- ○ 12 (Correct)
- ○ 60

**Explanation**

Because Alert1 alert criteria is triggered every minute, this results in potentially one SMS sent every minute, so 60 SMS in an hour.

Please note that rate limiting is implemented by Azure, which means that there is a maximum limit of notifications to be sent, in a particular time interval. The rate limit thresholds are:

**SMS**: No more than 1 SMS every 5 minutes.

**Voice**: No more than 1 Voice call every 5 minutes.

**Email**: No more than 100 emails in an hour.

As the SMS limit is 1 SMS every 5 minutes, then the correct answer for this question is **12 SMS messages in an hour.**

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-rate-limiting

**Quick Preview:**

Question 22: Skipped

You have an Azure subscription named Subscription1 that contains the resources shown in the following table:

Larger image

You create virtual machines in Subscription1 as per the following table:

Larger image

You plan to use Vault1 for the backup of as many virtual machines as possible.

Which virtual machines can be backed up to Vault1?

- ○ VM1 only
- ○ VM3 and VMC only
- ○ VM1, VM2, VM3, VMA, VMB, and VMC
- ○ VM1, VM3, VMA, and VMC only (Correct)
- ○ VM1 and VM3 only

**Explanation**

To create a vault to protect virtual machines, the vault must be in the same region as the virtual machines. If you have virtual machines in several regions, create a Recovery Services vault in each region.

Taking a look at the question, we can see that Vault1 is deployed in West Europe Azure region, so this means that Vault1 can be used for virtual machines deployed in West Europe only. The only virtual machines deployed in West Europe region are **VM1, VM3, VMA, and VMC**.

**Reference:**

https://docs.microsoft.com/bs-cyrl-ba/azure/backup/backup-create-rs-vault

**Quick Preview:**

Question 23: Skipped
You have an Azure Kubernetes Service (AKS) cluster named AKS1. You need to configure cluster autoscaler for AKS1.

Which two tools should you use?

- □
  the `kubectl` command
- □
  the `az aks` command
  (Correct)
- □
  the `Set-AzVm` cmdlet
- □
  the Azure portal
  (Correct)
- □
  the `Set-AzAks` cmdlet

**Explanation**
Let’s review each possible answer in order to discover if it’s a correct option or not:
**the kubectl command.**
kubetcl command is mainly used to horizontally scale pods. Kubernetes as deployed some integrations with main cloud providers, to autoscale nodes, based in a yaml configuration file.

In the first link provided you have detailed information about this process.
This option is deployed by kubernetes, and not supported by Microsoft, so if we have two better options we will discard this one.

**the az aks command.**
This option is correct and represents the way to autoscale a AKS Cluster using Az CLI commands. You can find all the information in the second link provided.
To setup AKS cluster autoscaler when creating it use az aks create command:

To setup an existing AKS cluster to autoscale, use az aks update command:

**the Set-AzVm cmdlet.**
This Az Powershell cmdlet is not the appropriate to aks cluster autoscaler. The correspondent Az PowerShell cmdlet is Set-AzAksCluster.

**the Azure portal.**
Currently, June 2021, it is not possible to enable autoscale when creating an AKS

Cluster, but once created you can enable autoscale. To do that, go to your AKS cluster, and from the left side menu go to agent pools. Select the agent pool you want to scale:

In the overview screen click on the Disabled link next to autoscale:

And finally in the scale screen, slect Autoscale and setup min and max node count:

**the Set-AzAks cmdlet.**

This Az Powershell cmdlet is not the appropriate to aks cluster autoscaler. The correspondent Az PowerShell cmdlet is Set-AzAksCluster.

**Reference:**

https://github.com/kubernetes/autoscaler/tree/master/cluster-autoscaler/cloudprovider/azure

https://docs.microsoft.com/en-us/azure/aks/cluster-autoscaler

**Quick Preview:**

Question 24: Skipped

You create the following resources in an Azure subscription:

- An Azure Container Registry instance named Registry1

- An Azure Kubernetes Service (AKS) cluster named Cluster1

You create a container image named App1 on your administrative workstation. You need to deploy App1 to Cluster1.

What should you do first?

- ○ Run the `docker push` command.
- ○ Create an App Service plan.
- ○ Run the `az acr build` command (Correct)
- ○ Run the `az aks create` command

**Explanation**

Azure Container Registry (ACR) is a managed, private Docker registry service based on the open-source Docker Registry 2.0. You can create and maintain Azure container registries to store and manage your private Docker container images and related artifacts.

So, once you have a registry configured and available in Azure, you can build a container image and store it in Azure ACR.  In order to do this, you can run the `az acr build` command to build and push the container image.

Here's an example:

`az acr build` ***--registry*** $ACR_NAME ***--image*** helloworld

**Reference:**

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-tutorial-quick-task

**Quick Preview:**

Question 25: Skipped

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

Larger image

You need to configure a proximity placement group for VMSS1.

Which proximity placement groups should you use?

- ○ Proximity2 only
- ○ Proximity1, Proximity2, and Proximity3
- ○ Proximity1 only (Correct)
- ○ Proximity1 and Proximity3 only

**Explanation**

A proximity placement group is a logical grouping used to make sure that Azure compute resources are physically located close to each other. When would you use Azure proximity placement groups? Proximity placement groups are useful for workloads or applications where low latency is a requirement.

So the solution to get VMs as close as possible and achieve the lowest possible latency, you should deploy them within a proximity placement group.

Also, because VMs will be deployed in the same location, so the same Azure region, we first need to take a look at VMSS1 location, which is West US. Now, taking a look at the different locations for available proximity placement groups 1, 2 and 3, we can see that only Proximity1 proximity placement group is available in the same Azure region as VMSS1 - West US.

**Reference:**

https://azure.microsoft.com/en-us/blog/announcing-the-general-availability-of-proximity-placement-groups/

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/proximity-placement-groups-portal

**Quick Preview:**

Question 26: Skipped

You plan to deploy several Azure virtual machines that will run Windows Server 2019 in a virtual machine scale set by using an Azure Resource Manager template. You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

- ○ Deployment Center in Azure App Service
- ○ A Desired State Configuration (DSC) extension (Correct)
- ○ the `New-AzConfigurationAssignment` cmdlet
- ○ a Microsoft Intune device configuration profile

**Explanation**

Azure virtual machine extensions are small packages that run post-deployment configuration and automation on Azure virtual machines. For this specific scenario, you would need to add NGINX web server package in your custom script that needs to run.

Here's an example:

***az vm extension set*** \

```
--resource-group myResourceGroup \

--vm-name myVM --name customScript \

--publisher Microsoft.Azure.Extensions \

--settings '{"commandToExecute": "apt-get install -y nginx"}
```

In the above example, Azure Command Line Interface (CLI) is used to deploy a custom script extension to an existing virtual machine, which installs a NGINX web server.

Please note that you could also use ***Azure Custom Script Extension*** to accomplish the same goal, similar to ***Desired State Configuration (DSC) extension.***

**Reference:**

https://docs.microsoft.com/en-us/azure/architecture/framework/devops/automation-configuration

**Quick Preview:**

Question 27: Skipped

You deploy an Azure Kubernetes Service (AKS) cluster that has the network profile shown in the following exhibit:

Larger image

Containers will be assigned an IP address in the .......... subnet.

- ○ 10.244.0.0/16 (Correct)
- ○ 10.0.0.0/16
- ○ 172.17.0.1/16

**Explanation**

By default, when you deploy an AKS cluster, an Azure virtual network and subnet are created for you. With *kubenet*, nodes get an IP address from the Azure virtual network subnet. Pods receive an IP address from a logically different address space to the Azure virtual network subnet of the nodes.

Taking a look at the exhibit presented in the question, there are two fields we need to pay attention to: Pod CIDR and Service CIDR.

The ***Pod CIDR*** should be a large address space that isn't in use elsewhere in your network environment. This range includes any on-premises network ranges if you connect, or plan to connect, your Azure virtual networks using Express Route or a Site-to-Site VPN connection.

This address range must be large enough to accommodate the number of nodes that you expect to scale up to. Also, please note that you can't change this address range once the cluster is deployed if you need more addresses for additional nodes.

The ***Service CIDR*** is used to assign internal services in the AKS cluster an IP address. Similar to Pod CIDR, this IP address range should be an address space that isn't in use elsewhere in your network environment, including any on-premises network ranges if you connect, or plan to connect, your Azure virtual networks using Express Route or a Site-to-Site VPN connection.

Now that we have a better understanding on these topics, we can conclude that :

Containers will be assigned an IP address in the ***10.244.0.0/16 subnet***, which is the ***Pod CIDR.***

**Reference:**

https://docs.microsoft.com/en-us/azure/aks/configure-kubenet

**Quick Preview:**

Question 28: Skipped
You deploy an Azure Kubernetes Service (AKS) cluster that has the network profile shown in the following exhibit:
Larger image

Services in the AKS cluster will be assigned an IP address in the .......... subnet.

- ○ 10.244.0.0/16
- ○ 10.0.0.0/16 (Correct)
- ○ 172.17.0.1/16

**Explanation**
By default, when you deploy an AKS cluster, an Azure virtual network and subnet are created for you. With *kubenet*, nodes get an IP address from the Azure virtual

network subnet. Pods receive an IP address from a logically different address space to the Azure virtual network subnet of the nodes.

Taking a look at the exhibit presented in the question, there are two fields we need to pay attention to: Pod CIDR and Service CIDR.

The ***Pod CIDR*** should be a large address space that isn't in use elsewhere in your network environment. This range includes any on-premises network ranges if you connect, or plan to connect, your Azure virtual networks using Express Route or a Site-to-Site VPN connection.

This address range must be large enough to accommodate the number of nodes that you expect to scale up to. Also, please note that you can't change this address range once the cluster is deployed if you need more addresses for additional nodes.

The ***Service CIDR*** is used to assign internal services in the AKS cluster an IP address. Similar to Pod CIDR, this IP address range should be an address space that isn't in use elsewhere in your network environment, including any on-premises network ranges if you connect, or plan to connect, your Azure virtual networks using Express Route or a Site-to-Site VPN connection.

Now that we have a better understanding on these topics, we can conclude that :

Services in the AKS cluster will be assigned an IP address in the ***10.0.0.0/16 subnet***, which is the ***Service CIDR.***

**Reference:**

https://docs.microsoft.com/en-us/azure/aks/configure-kubenet

**Quick Preview:**

Question 29: Skipped
You have the App Service plan shown in the following exhibit:
Larger image

The scale-in settings for the App Service plan are configured as shown in the following exhibit:

Larger image

The scale out rule is configured with the same duration and cool down timer, as the scale in rule.

Please evaluate the above information and choose the correct option for the following statement:

If after deployment CPU usage is 70 percent for one hour and then reaches 90 percent for five minutes, at that time the total number of instances will be .......... .

- ○ 1
- ○ 2 (Correct)
- ○ 3
- ○ 4
- ○ 5

**Explanation**
After the deployment is complete, there will be one single instance running, because the minimum instance limit is configured as 1. The question states that after deployment is complete, CPU usage is 70% for one hour. During this time, no instances will be added or removed, because conditions for auto-scaling are set to CPU usage greater than 85% - for adding instances, and lower than 30% - for removing instances.

The CPU usage reaches 90% for five minutes, which will trigger the scale out rule and 1 instance will be added. As the condition is evaluated every 5 minutes, there is only one check for the CPU usage in this scenario.

The total number of instances in this case is 2 instances, one from the beginning and one instance added when CPU reaches 90%.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-monitor/autoscale/tutorial-autoscale-performance-schedule

**Quick Preview:**

Question 30: Skipped
You have the App Service plan shown in the following exhibit:
Larger image

The scale-in settings for the App Service plan are configured as shown in the following exhibit:

Larger image

The scale out rule is configured with the same duration and cool down timer, as the scale in rule.

Please evaluate the above information and choose the correct option for the following statement:

If after deployment the CPU maintains constant usage of 90% for one hour, and then the average CPU usage is below 25% for nine minutes, at that point the number of instances will be .......... .

- ○ 1
- ○ 2
- ○ 3
- ○ 4 (Correct)
- ○ 5

**Explanation**
After the deployment is complete, there will be one single instance running, because the minimum instance limit is configured as 1. The question states that after deployment is complete, the CPU maintains constant usage of 90% for one hour. From the exhibits presented in the question, we can see that the CPU usage is verified every 5 minutes (duration), then a 5 minutes cool down timer follows. During the cool down period, CPU usage is monitored and no decision is taken.

So this means that after first 5 minutes, there will be one more instance added, with a total of 2 instances. Once the first cool down timer expires (minute 10), the CPU usage is again examined and since is 90%, over the 85% threshold, another instance is added. Then another cool down timer, for 5 minutes. So every 10 minutes a new instance is added. ***The end result is that after one hour***, (6 x 10 minutes) ... ***we will have 5 instances running***. Please note that the configuration presented in the exhibits shows that, at maximum, 5 instances can run at any given moment.

Let's move on to the second part of the question. The statement mentions that after one hour, the average CPU usage is below 25% for nine minutes. Taking a look at the ***scale in*** configuration, we can see that if the average CPU usage is below 30%, one instance will be removed. So, after 5 minutes (out of 9 minutes with average CPU at 25%) one instance will be removed. ***We now have 4 instances running.***

Before any other decision is taken, the cool down timer needs to expire, and the cool down timer is configured at 5 minutes, for both scale in and scale out rules. This means that no other actions will be taken for the other 4 minutes left (out of total 9 minutes with 25% average CPU utilisation). ***The end result is 4 instances running***.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-monitor/autoscale/tutorial-autoscale-performance-schedule

**Quick Preview:**

Question 31: Skipped

You create an Azure VM named VM1 that runs Windows Server 2019. VM1 is configured as shown in the exhibit:

Larger image

You need to enable Desired State Configuration for VM1.

What should you do first?

- ○ Connect to VM1
- ○ Start VM1 (Correct)
- ○ Capture a snapshot of VM1
- ○ Configure a DNS name for VM1

**Explanation**
If we take a closer look at the exhibit, we can see that the virtual machine's status is Stopped (Deallocated). The DSC extension for Windows requires that the target virtual machine is able to communicate with Azure, so you would ***first need to start the VM***.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-windows

**Quick Preview:**

Question 32: Skipped
***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.***

You have an Azure subscription that contains the following resources:

- A virtual network that has a subnet named Subnet1

- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1

- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- Priority: 300

- Source: Any

- Source port range: *

- Destination: *

- Destination port range: 3389

- Protocol: UDP

- Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

`Solution: You add an inbound security rule to NSG-Subnet1 that allows connections from the Any source to the * destination for port range 3389 and uses the TCP protocol. You remove NSG-VM1 from the network interface of VM1.`

Does this meet the goal

- ○ Yes (Correct)
- ○ No

**Explanation**
First of all, it is crucial to understand that inbound traffic is evaluated by both NSGs, if they are applied at subnet and VM network interface card. Also, there is an order in which traffic is processed. Here's how it goes.

Inbound traffic is first evaluated by the NSG applied at the subnet level. If the NSG applied at the subnet level allows the traffic, then the traffic will be evaluated by the NSG applied at the virtual machine (VM) network interface card level. If this NSG allows the traffic as well, then the traffic will reach the intended destination, the VM itself.

Also, please note that you can have 0 or 1 NSG applied at either of the two levels (subnet or VM), so you don't have to apply an NSG at any of the two levels, but you can do it if you want to.

Now, let's clarify what this question is asking. First of all, the NSG applied at subnet level has an initial configuration, which means that RDP connections will not be allowed to the VM. Next, a new inbound rule is added to NSG-Subnet1, and the end configuration looks like in the below exhibit:

RDP works on TCP port 3389, so NSG-Subnet1 will allow the traffic. Next, the traffic may be analysed by the second NSG, applied at the VM network interface card level. Since the proposed solution states that NSG-VM1 is removed, then the traffic will pass directly to the VM, so the RDP connection will work.

**Reference:**

https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/troubleshoot-rdp-connection

**Quick preview:**

Question 33: Skipped

***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.***

You have an Azure subscription that contains the following resources:

- A virtual network that has a subnet named Subnet1

- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1

- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- Priority: 300

- Source: Any

- Source port range: *

- Destination: *

- Destination port range: 3389

- Protocol: UDP

- Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

```
Solution:  You add an inbound security rule to NSG-Subnet1 that allows
connections from the internet source to the VirtualNetwork destination
for port range 3389 and uses the UDP protocol.
```

Does this meet the goal?

- ○ Yes
- ○ No (Correct)

**Explanation**

First of all, it is crucial to understand that inbound traffic is evaluated by both NSGs, if they are applied at subnet and VM network interface card. Also, there is an order in which traffic is processed. Here's how it goes.

Inbound traffic is first evaluated by the NSG applied at the subnet level. If the NSG applied at the subnet level allows the traffic, then the traffic will be evaluated by the NSG applied at the virtual machine (VM) network interface card level. If this NSG allows the traffic as well, then the traffic will reach the intended destination, the VM itself.

Also, please note that you can have 0 or 1 NSG applied at either of the two levels (subnet or VM), so you don't have to apply an NSG at any of the two levels, but you can do it if you want to.

Now, let's clarify what this question is asking. First of all, the NSG applied at subnet level has an initial configuration, which means that RDP connections will not be allowed to the VM. Next, a new inbound rule is added to NSG-Subnet1, which allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the UDP protocol.

RDP works on TCP port 3389, so NSG-Subnet1 will not allow the traffic, because the new inbound rule allows UDP port 3389 traffic.

**Reference:**

https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/troubleshoot-rdp-connection

**Quick preview:**

Question 34: Skipped

***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.***

You have an Azure subscription that contains the following resources:

- A virtual network that has a subnet named Subnet1

- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1

- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- Priority: 00

- Source: Any

- Source port range: *

- Destination: *

- Destination port range: 3389

- Protocol: UDP

- Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

`Solution: You add an inbound security rule to NSG-Subnet1 and NSG-VM1 that allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the TCP protocol.`

Does this meet the goal?

- ○ Yes

(Correct)

- ○ No

**Explanation**
First of all, it is crucial to understand that inbound traffic is evaluated by both NSGs, if they are applied at subnet and VM network interface card. Also, there is an order in which traffic is processed. Here's how it goes.

Inbound traffic is first evaluated by the NSG applied at the subnet level. If the NSG applied at the subnet level allows the traffic, then the traffic will be evaluated by the NSG applied at the virtual machine (VM) network interface card level. If this NSG allows the traffic as well, then the traffic will reach the intended destination, the VM itself.

Also, please note that you can have 0 or 1 NSG applied at either of the two levels (subnet or VM), so you don't have to apply an NSG at any of the two levels, but you can do it if you want to.

Now, let's clarify what this question is asking. First of all, the NSG applied at subnet level has an initial configuration, which means that RDP connections will not be allowed to the VM. Next, an inbound security rule is added to both NSG-Subnet1 and NSG-VM1 that allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the TCP protocol.

The end result will look similar to the exhibit below:

RDP works on TCP port 3389, so both NSG-Subnet1 and NSG-VM1 will allow the traffic. The traffic is first evaluated by NSG-Subnet1, the traffic is allowed, then the traffic is evaluated by NSG-VM1, which also allows the traffic, so the traffic will reach the end destination - the virtual machine (VM).

**Reference:**

https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/troubleshoot-rdp-connection

**Quick preview:**

Question 35: Skipped
You have an Azure subscription that contains a virtual network named VNET1. VNET1 contains the subnets shown in the following table:
Larger image

Each virtual machine uses a static IP address. You need to create network security groups (NSGs) to meet following requirements:

- Allow web requests from the internet to VM3, VM4, VM5, and VM6.

- Allow all connections between VM1 and VM2.

- Allow Remote Desktop connections to VM1.

- Prevent all other network traffic to VNET1.

What is the minimum number of NSGs you should create?

- ○ 1 (Correct)
- ○ 3
- ○ 4
- ○ 12

**Explanation**

You can use an Azure Network Security Group (NSG) to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains inbound security rules that allow or deny inbound network traffic and outbound security rules that allow or deny outbound traffic from your resources deployed in Azure.

It is absolutely critical to understand that an NSG can include multiple security rules, not just one. Network security group security rules are evaluated by priority using the source, source port, destination, destination port, and protocol of the traffic, to allow or deny the traffic.

So, for this specific scenario, we can create multiple inbound security rules to meet the requirements. The questions states that all virtual machines use a static IP address. Let's consider that the VMs have the following IP addresses allocated:

- VM1 - 1.1.1.1

- VM2 - 2.2.2.2

- VM3 - 3.3.3.3

- VM4 - 4.4.4.4

- VM5 - 5.5.5.5

- VM6 - 6.6.6.6

Next, let's see what inbound security rules we need to define to meet the requirements. Let's take a look at the first one:

***- Allow web requests from the internet to VM3, VM4, VM5, and VM6.***

The inbound security rule would look similar to the following exhibit:

In order to meet the second requirement ...

***- Allow all connections between VM1 and VM2***

... we don't need to add a new inbound rule. Connections between VMs deployed in the same virtual network are allowed by default.

Next, let's take a look at the third requirement:

***- Allow Remote Desktop connections to VM1.***

In order to meet this requirement, we would need to add a new inbound security rule. The end configuration of our new network security group would look like this. Please note that this new security rule is the second one in the NSG, priority 200:

The last requirement to evaluate is the following:

***- Prevent all other network traffic to VNET1.***

By default, traffic that is not explicitly permitted, will be denied. Taking a look at our new network security group presented above, the last requirement is met by the last inbound security rule in the list, ***priority 65500, DenyAllInbound.***

Last, please note that you can apply the same network security group to any subnet or VM that you have available in your Azure subscription. ***The end result is that we need only one network security group to meet all requirements presented in this scenario.***

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#default-security-rules

**Quick Preview:**

Question 36: Skipped

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

Larger image

The `Not allowed resource types` Azure policy 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, and then connect VM2 to VNET1.

What should you do first?

- ○ Remove `Microsoft.Compute/virtualMachines` from the policy (Correct)
- ○ Create an Azure Resource Manager template
- ○ Add a subnet to VNET1
- ○ Remove `Microsoft.Network/virtualNetworks` from the policy

**Explanation**

The `Not allowed resource types` Azure policy denies the deployment of specified resource types. In this specific scenario, the Azure policy denies the deployment of virtual machines - `Microsoft.Compute/virtualMachines` and virtual networks `Microsoft.Network/virtualNetworks` in the Azure subscription.

The question requires that you create a new virtual machine named VM2, and then connect VM2 to VNET1. So you need to be allowed to create a new VM (VM2) in this Azure subscription and then attach it to an existing Azure virtual network - VNET1. As you don't need to create a new virtual network, as you are requested to attach the new VM to your existing virtual network, the only thing that you need to do is to **remove** `Microsoft.Compute/virtualMachines` from the Azure policy.

**Reference:**

https://docs.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies

**Quick Preview:**

Question 37: Skipped

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

Larger image

You install the Web Server server role (IIS) on VM1 and VM2, and then add VM1 and VM2 to LB1.

LB1 is configured as shown in the LB1 exhibit:

Larger image

Rule1 is configured as shown in the Rule1 exhibit below:

Larger image

Please evaluate the following statements and select `Yes` if the statement is true, otherwise select `No`:

VM1 is in the same availability set as VM2.

- ○ Yes (Correct)
- ○ No

**Explanation**

To answer this question, the most relevant piece of information provided in the question is the fact that LB1 is a basic load balancer (Basic SKU). When using an Azure basic load balancer, all virtual machines part of the backend pool are deployed in a single availability set or virtual machine scale set.

For this reason, the statement is ***True*** - ***VM1 is in the same availability set as VM2.***

**Reference:**

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

**Quick Preview:**

Question 38: Skipped
You have an Azure subscription that contains the resources in the following table:
Larger image

You install the Web Server server role (IIS) on VM1 and VM2, and then add VM1 and VM2 to LB1.

LB1 is configured as shown in the LB1 exhibit:

Larger image

Rule1 is configured as shown in the Rule1 exhibit below:
Larger image

Please evaluate the following statements and select `Yes` if the statement is true, otherwise select `No`:

If Probe1.htm is present on VM1 and VM2, LB1 will balance TCP port 80 between VM1 and VM2.

- ○ Yes (Correct)
- ○ No

**Explanation**
When using load-balancing rules with Azure Load Balancer, you need to specify health probes to allow Load Balancer to detect the backend endpoint status. The configuration of the health probe and probe responses determine which backend pool instances will receive new flows.

Simply put, in our case, the load balancer will try to open a connection on Probe1.htm, on TCP port 80. Why TCP port 80? Well, if you take a look at the load balancing rule configuration, you can see that the health probe configuration is HTTP 80, which is the same with TCP 80. So, coming back to our discussion, the load balancer checks the status of both VM1 and VM2, by initiating connections on Probe1.htm. If the connection is successful, then the load balancer knows that both VMs are in a good condition and are eligible to receive traffic.

That is actually the role of the health probe. Just think, it doesn't make any sense for the load balancer to send any traffic to a VM that is not online, that is not in a good condition, because the traffic will be lost.

So now, taking a look again at the statement we need to evaluate,

***If Probe1.htm is present on VM1 and VM2, LB1 will balance TCP port 80 between VM1 and VM2.***

we can conclude that the statement is ***True***. The load balancer receives traffic from the internet, on TCP port 80 and forwards the traffic on TCP port 80 as well ...

To what destination? To virtual machines that are part of the backend pool ...

and only to healthy VMs, so VMs that pass the health check process, defined by the health probes:

**Reference:**

[https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview)

**Quick Preview:**

Question 39: Skipped
You have an Azure subscription that contains the resources in the following table:
Larger image

You install the Web Server server role (IIS) on VM1 and VM2, and then add VM1 and VM2 to LB1.

LB1 is configured as shown in the LB1 exhibit:

Larger image

Rule1 is configured as shown in the Rule1 exhibit below:
Larger image

Please evaluate the following statements and select `Yes` if the statement is true, otherwise select `No`:

If you delete Rule1, LB1 will balance all the requests between VM1 and VM2 for all the ports.

- ○
  Yes

- ○ No (Correct)

**Explanation**

This statement is actually wrong. The load balancing rule is the "glue" that puts all the pieces together. If you have no load balancing rule configured, there will be no load balancing at all, and no traffic will actually reach VM1 or VM2.

The load balancing rule includes the following:

- the public IP address of the load balancer, this is the IP address that the traffic will first connect to

- protocol and port number of traffic to be received and sent to the backend pool

- backend pool

- health probe

- other configurations ...

Again, if no load balancing rules are defined, there will be no load balancing happening at all.

**Reference:**

https://docs.microsoft.com/en-us/azure/load-balancer/components

**Quick Preview:**

Question 40: Skipped

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

Larger image

You need to create a network interface named NIC1. In which location can you create NIC1?

- ○ East US and North Europe only
- ○ East US only (Correct)
- ○ East US, West Europe, and North Europe

- ○ East US and West Europe only

**Explanation**

Before creating a network interface, you must have an existing virtual network in the same location and subscription you create a network interface in. Because VNET1 is deployed in East US, then ***the network interface card can be created only in East US.***

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface

**Quick Preview:**

Question 41: Skipped

You have Azure virtual machines that run Windows Server 2019 and are configured as shown in the following table:

Larger image

You create a public Azure DNS zone named adatum.com and a private Azure DNS zone named contoso.com.

For contoso.com, you create a virtual network link named link1 as shown in the exhibit:

Larger image

You discover that VM1 can resolve names in contoso.com, but cannot resolve names in adatum.com. VM1 can resolve other hosts on the Internet. You need to ensure that VM1 can resolve host names in adatum.com.

What should you do?

- ○ Update the DNS suffix on VM1 to be adatum.com
- ○ Configure the name servers for adatum.com at the domain registrar (Correct)
- ○ Create an SRV record in the contoso.com zone
- ○ Modify the Access control (IAM) settings for link1

**Explanation**

The key point in this scenario is to realise that adatum.com is a public Azure DNS zone.

The link in the exhibit is for contoso.com , a private DNS. And auto registration has not been enabled, so VMs in the vNet will be not auto registered in the DNS Zone.

But the issue reported in the Question is that you cannot resolve names in adatum.com, while you can resolve other hosts on the internet. This means that DNS configuration of VM1 is properly setup, but has not access to the definitions you publish in your public adatum.com zone.

The Internet top level domain DNS servers need to know which DNS servers to direct DNS queries for adatum.com to. This information corresponds to the name servers linked to your domain information.

When you create a public zone in Azure DNS, you have up to 4 Name Servers you have to setup in your domain:

So to solve the problem you need to configure these name servers into your domain in your domain panel at your registrar. This is also called delegate domain.

**Reference:**

https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns#delegate-the-domain

**Quick Preview:**

Question 42: Skipped

You plan to use Azure Network Watcher to perform the following task:

```
Identify a security rule that prevents a network packet from reaching an Azure virtual machine.
```

Which Azure feature should you use for this task?

- ○ IP flow verify (Correct)
- ○ Next hop
- ○ Packet capture

- ○ Security group view
- ○ Traffic Analytics

**Explanation**

`IP flow verify` is one of the several capabilities available in Azure Network Watcher.

You can use `IP flow verify` to test the network communication to an Azure virtual machine. IP flow verify will then inform you if the connection succeeds or fails. If the connection fails, IP flow verify tells you which security rule allowed or denied the communication, so that you can resolve the problem.

The *IP flow verify* capability enables you to specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound).

**Reference:**

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

**Quick Preview:**

Question 43: Skipped

You plan to use Azure Network Watcher to perform the following task:

`Validate outbound connectivity from an Azure virtual machine to an external host.`

Which Azure feature should you use for this task?

- ○ Connection troubleshoot
  (Correct)
- ○ IP flow verify
- ○ Next hop
- ○ NSG flow logs
- ○ Traffic Analytics

**Explanation**

`Connection troubleshoot` is one of the several capabilities available in Azure Network Watcher.

The `connection troubleshoot` capability enables you to test a connection between a VM and the destiantion, such as a VM, an FQDN, a URI, or an IPv4 address. The test returns similar information returned when using the `connection monitor` capability, but tests the connection at a point in time, rather than monitoring it over time, as connection monitor does.

**Reference:**

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

**Quick Preview:**

Question 44: Skipped

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

Larger image

RG1 contains the resources shown in the following table:

Larger image

You need to identify which resources you can move from RG1 to RG2, and once moved to RG2, which resources you can move back from RG2 to RG1.

Which resources should you identify? (Select two)

- □ Resource that you can move from RG1 to RG2: ***None***
- □ Resource that you can move from RG1 to RG2: ***IP2 only***
- □ Resource that you can move from RG1 to RG2: ***IP2 and storage2 only***
- □ Resource that you can move from RG1 to RG2: ***IP2 and VNET2 only***
- □

Resource that you can move from RG1 to RG2: ***IP2, VNET2 and storage2***
(Correct)

- □
  Resource that you can move from RG2 to RG1: ***None***
- □
  Resource that you can move from RG2 to RG1: ***IP2 only***
- □
  Resource that you can move from RG2 to RG1: ***IP2 and storage2***
- □
  Resource that you can move from RG2 to RG1: ***IP2 and VNET2 only***
- □
  Resource that you can move from RG2 to RG1: ***IP2, VNET2 and storage2***
  (Correct)

**Explanation**

Some Azure resources can be moved to different resource groups or subscriptions, while other not. Very important to note here is that Azure Locks don't affect move operations.

Taking a look at the documentation, first link in the resources, we can investigate and check if public IP addresses, virtual networks and storage accounts can be moved to a different resource group ... and the answer is definitely ***Yes***.

Although it doesn't apply to this question, some resources can be moved to a different Azure subscription, information available in the last column (Subscription).

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

**Quick Preview:**

Question 45: Skipped

***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.***

You have an Azure subscription that contains the virtual machines shown in the following table:

Larger image

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?

- ○ Yes
- ○ No (Correct)

**Explanation**
In scenarios with pre-populated backend pools, just like this scenario, we can use IP and virtual network for your backend pool. All backend pool management is done directly on the backend pool object.

Also, there are some limitations that you need to be aware of. The one that applies to this scenario is that you can only use Standard public SKU IP address for your VMs that you want to attach to your Backend Pool.

As VM2 has a Basic SKU public IP address, the deployment will fail. If you try to deploy this scenario in Azure portal, you will even get a message displayed from Azure, highlighted in red in the exhibit below:

***You can only attach virtual machines that have a standard SKU public IP configuration ... or no public IP configuration.***

**Reference:**

https://docs.microsoft.com/en-us/azure/load-balancer/backend-pool-management

**Quick Preview:**

Question 46: Skipped

***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.***

You have an Azure subscription that contains the virtual machines shown in the following table:

Larger image

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 Standard SKU public IP address, associate the address to the network interface of VM1, and then stop VM2.`

Does this meet the goal?

- ○ Yes
- ○ No (Correct)

**Explanation**

In scenarios with pre-populated backend pools, just like this scenario, we can use IP and virtual network for your backend pool. All backend pool management is done directly on the backend pool object.

Also, there are some limitations that you need to be aware of. The one that applies to this scenario is that you can only use  Standard public SKU IP address for your VMs that you want to attach to your Backend Pool.

As VM2 has a Basic SKU public IP address, the deployment will fail. If you try to deploy this scenario in Azure portal, you will even get a message displayed from Azure, highlighted in red in the exhibit below:

***You can only attach virtual machines that have a standard SKU public IP configuration ... or no public IP configuration.***

**Reference:**

https://docs.microsoft.com/en-us/azure/load-balancer/backend-pool-management

**Quick Preview:**

Question 47: Skipped

***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.***

You have an Azure subscription that contains the virtual machines shown in the following table:

Larger image

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 dissociate current Basic public IP from VM2 network interface, 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?

- ○ Yes (Correct)
- ○ No

**Explanation**
In scenarios with pre-populated backend pools, just like this scenario, we can use IP and virtual network for your backend pool. All backend pool management is done directly on the backend pool object.

Also, there are some limitations that you need to be aware of. The one that applies to this scenario is that you can only use  Standard public SKU IP address for your VMs that you want to attach to your Backend Pool.

If you try to deploy this scenario in Azure portal, you will even get a message displayed from Azure, highlighted in red in the exhibit below:

***You can only attach virtual machines that have a standard SKU public IP configuration ... or no public IP configuration.***

***The proposed solution will solve the problem in this case: two Standard SKU Public IP addresses, one for each VM, VM1 and VM2.*** Of course, before attaching a Standard Public IP address to VM2, you would need to first disassociate the current Basic SKU Public IP address and then attach the new Standard SKU Public IP Address.

**Reference:**

https://docs.microsoft.com/en-us/azure/load-balancer/backend-pool-management

**Quick Preview:**

Question 48: Skipped
You have an Azure virtual machine named VM1. The network interface for VM1 is configured as shown in the exhibit:
Larger image

You deploy a web server on VM1, and then create a secure website that is accessible by using the HTTPS protocol. VM1 is used as a web server only.

You need to ensure that users can connect to the website from the Internet.

What should you do?

- ○ Modify the protocol of Rule4
- ○ Delete Rule1
- ○ For Rule5, change the Action to Allow and change the priority to 401 **(Correct)**
- ○ Create a new inbound rule that allows TCP protocol 443 and configure the rule to have a priority of 501

**Explanation**

First of all, HTTPS uses TCP protocol, port 443. So we need to make sure that TCP traffic, on port 443 is allowed.

Before we take a closer look at our existing security rules, let's take note of the following. The security rules' priority is 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. ***Also, very important to keep in mind, once traffic matches a rule, processing stops.*** As a result, no more rules are processed when the first traffic match is found.

Let's now take a look at the security rules presented in the exhibit.

The first rule, priority 300, will be processed first. This rule allows RDP traffic (TCP traffic on port 3389), so it's not related to our traffic.

Second rule, priority 400, denies TCP traffic on port 80, so it denies HTTP traffic.

Third rule, priority 500, denies TCP traffic on port 80 and 443, so it denies HTTP and HTTPS traffic. Well, this is important, so it denies the traffic we are interested in -> HTTPS. As mentioned earlier, when the first match occurs, the evaluation of the security rules stops. Simply put, it doesn't matter if there is another rule with priority number higher than 500, so lower in the list, that allows traffic. HTTPS traffic is denied by this rule, priority 500, and no other rule in the list, below this rule, can change the result.

For this reason, we need to either change the action of this rule to ***Allow***, or have a rule above this rule that accepts HTTPS traffic. This rule should have a lower priority number (lower than 500), which means will have a higher priority and will be evaluated before this rule that denies HTTPS traffic.

Now, coming back to the existing security rules, let's examine the answer options that we have available.

Modifying the protocol for Rule4 will not fix the problem, because Rule4 is after Rule2, that denies HTTPS traffic. It doesn't matter if we make the necessary modifications on Rule4 to allow HTTPS traffic.

Deleting Rule1 will not help, because Rule1 denies HTTP traffic, and not HTTPS.

Next, ***For Rule5, change the Action to Allow and change the priority to 401***, will actually solve the problem. Rule5 matches traffic with port between 50 - 5000, and because HTTPS is TCP port 443, it will match our traffic. Also, modifying the priority to 401 means that Rule 5 will be above Rule2 (which denies HTTPS). The end result is that HTTPS traffic will be allowed.

Here's how the inbound security rules look like, after the change:

**Reference:**

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

**Quick Preview:**

Question 49: Skipped

***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.***

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:

Larger image

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail. 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?

- ○ Yes
- ○ No (Correct)

**Explanation**

The question states that ***"You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443".*** Creating an inbound security rule that denies all traffic from 131.107.100.50 source IP address would block all traffic from this specific IP address, so this is definitely not a solution.

Taking a look at current inbound security rules we see that the first rule - priority 100 - actually allows the traffic to our virtual network, so to App1.

The way inbound security rules are configured in this scenario is actually a best practice:

- first define an inbound rule for the traffic that you want to ***allow***

- ***deny*** any other traffic, as a second step

Technically speaking, the second rule - priority 200 - is not needed to deny traffic that is not permitted by the first rule, because all traffic not allowed by first rule will be denied by the last rule - priority 65500.

**Reference:**

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

**Quick Preview:**

Question 50: Skipped

***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.***

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:

Larger image

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail. You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

```
Solution: You delete the BlockAllOther443 inbound security rule.
```

Does this meet the goal?

- ○ Yes
- ○ No (Correct)

**Explanation**

The question states that "***You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443***". Deleting the second inbound security rule would not help, because the first rule - priority 100 already allows the traffic inbound, so this is definitely not a solution.

Taking a look at current inbound security rules we see that the first rule - priority 100 - actually allows the traffic to our virtual network, so to App1.

The way inbound security rules are configured in this scenario is actually a best practice:

- first define an inbound rule for the traffic that you want to ***allow***

- ***deny*** any other traffic, as a second step

Technically speaking, the second rule - priority 200 - is not needed to deny traffic that is not permitted by the first rule, because all traffic not allowed by first rule will be denied by the last rule - priority 65500.

**Reference:**

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

**Quick Preview:**

**Reference:**

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

**Quick Preview:**

Question 51: Skipped

***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.***

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:

Larger image

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail. You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

`Solution: You modify the load balancing rule configuration to listen for traffic on TCP port 443.`

Does this meet the goal?

- ○ Yes (Correct)
- ○

No

**Explanation**
The question states that ***"You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443".***

Taking a look at current inbound security rules we see that the first rule - priority 100 - actually allows the traffic to our virtual network, so to App1.

The way inbound security rules are configured in this scenario is actually a best practice:

- first define an inbound rule for the traffic that you want to ***allow***

- ***deny*** any other traffic, as a second step

Technically speaking, the second rule - priority 200 - is not needed to deny traffic that is not permitted by the first rule, because all traffic not allowed by first rule will be denied by the last rule - priority 65500.

In order for TCP 443 traffic to arrive at App1, the load balancer needs to be listening and waiting for TCP 443 traffic. The questions states that connections to App1 are managed by using an Azure Load Balancer, so the connection will first hit the load balancer and the load balancer will then share the connections to the backend pool - VM1 and VM2.

Simply put, if the load balancer is not listening for TCP 443 traffic, and is listening maybe for TCP 80 traffic, the TCP 443 traffic will never reach the intended destination - App1.

**Reference:**

https://docs.microsoft.com/en-us/azure/load-balancer/components

**Quick Preview:**

Question 52: Skipped
You purchase a new Azure subscription named Subscription1. You create a virtual machine named VM1 in Subscription1. VM1 is not protected by Azure Backup. You need to protect VM1 by using Azure Backup. Backups must be created at 01:00 and stored for 30 days.

What should you do? Please select two.

- □ Location in which to store the backups - A blob container
- □

Location in which to store the backups - A file share

- □ Location in which to store the backups - A Recovery Services Vault (Correct)
- □ Location in which to store the backups - A storage account
- □ Object to use to configure the protection for VM1 - A backup policy (Correct)
- □ Object to use to configure the protection for VM1 - A batch job
- □ Object to use to configure the protection for VM1 - A batch schedule
- □ Object to use to configure the protection for VM1 - A recovery plan

**Explanation**

***Statement 1:*** Azure VMs can be backed up using Azure Recovery Services vault.

A Recovery Services vault is a storage entity in Azure that stores data. The data is typically copies of data, or configuration information for virtual machines (VMs), workloads, servers, or workstations. You can use Recovery Services vaults to hold backup data for various Azure services such as virtual machines, or simply VMs.

***Statement 2:*** The Azure backup policy defines the settings used to perform the VM backup.

For example, the following backup policy defines the backup frequency - Daily at 1:00AM UTC time, and also defines the retention period for the daily backup point - 30 days.

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/backup-azure-recovery-services-vault-overview

https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-vms-prepare

Question 1: Skipped

You have an Azure Active Directory (Azure AD) tenant named adatum.com. Adatum.com contains the groups in the following table:

Larger image

You create two user accounts that are configured as shown in the following table:
Larger image

To which groups do User1 and User2 belong? (SELECT TWO)

- □
  User 1 - Group1
  (Correct)
- □
  User 1 - Group2
- □
  User 1 - Group3
- □
  User 1 - Group1 and Group2
- □
  User 1 - Group1 and Group3
- □
  User 1 - Group2 and Group3
- □
  User 1 - Group1, Group2 and Group3
- □
  User 2 - Group1
  (Correct)
- □
  User 2 - Group2
- □
  User 2 - Group3
- □
  User 2 - Group1 and Group2
- □
  User 2 - Group1 and Group3
- □
  User 2 - Group2 and Group3
- □
  User 2 - Group1, Group2 and Group3

**Explanation**

User1 - In order for the user to be added to a Microsoft365 group (previously office365 group), a license is needed (it's basically an exchange group + OneDrive, so you need a license to be in it). User1 is part of only Group1, rules apply to dynamically populated groups membership in Azure AD.

User2 - Since the assigned city starts with "M", but the user does not have an office license, it can be part of only Group1.

**Reference:**

https://answers.microsoft.com/en-us/msoffice/forum/msoffice_sharepoint/licensing-requirements-for-office-365-groups/10f294f5-95d8-4603-bd28-209ee050801b

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#rules-with-complex-expressions

Question 2: Skipped
You have a hybrid deployment of Azure Active Directory (Azure AD) that contains the users shown in the following table:
Larger image

You need to modify the JobTitle and UsageLocation attributes for the users. For which users can you modify the attributes from Azure AD? (SELECT TWO)

- □ JobTitle - User1 only
- □ JobTitle - User1 and User2 only
- □ JobTitle - User1 and User3 only (Correct)
- □ JobTitle - User1, User2 and User3
- □ UsageLocation - User1 only
- □ UsageLocation - User1 and User2 only
- □ UsageLocation - User1 and User3 only
- □ UsageLocation - User1, User2 and User3

(Correct)

**Explanation**
You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server Active Directory. For this reason, you can update the JobTitle for User1 and User3 only.

You can update the UsageLocation for all users: User1, User2 and User3.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-profile-azure-portal

**Quick Preview:**

Question 3: Skipped

***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.***

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 Network Contributor role at the subscription level to Admin1.

Does this meet the goal?

- ○ Yes (Correct)
- ○ No

**Explanation**
Your account must meet one of the following to enable traffic analytics:

- Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, reader, or ***network contributor.***

**Reference:**

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq

**Quick Preview:**

Question 4: Skipped

***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.***

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?

- ○ Yes (Correct)
- ○ No

**Explanation**

Your account must meet one of the following to enable traffic analytics:

- Your account must have any one of the following Azure roles at the subscription scope: **owner**, contributor, reader, or *network contributor*.

**Reference:**

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq

**Quick Preview:**

Question 5: Skipped

***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.***

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 Reader role at the subscription level to Admin1.

Does this meet the goal?

- ○

Yes
(Correct)

- ○
  No

**Explanation**
Your account must meet one of the following to enable traffic analytics:

- Your account must have any one of the following Azure roles at the subscription scope: **owner**, contributor, reader, or *network contributor.*

**Reference:**

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq

**Quick Preview:**

Question 6: Skipped
You have an Azure subscription that contains a user named User1. You need to ensure that User1 can deploy virtual machines and manage virtual networks. The solution must use the principle of least privilege.

Which role-based access control (RBAC) role should you assign to User1?

- ○
  Owner
- ○
  Virtual Machine Contributor
- ○
  Contributor
  (Correct)
- ○
  Virtual Machine Administrator Login

**Explanation**
Virtual Machine Contributor: Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.

And because the requirement is to manage Virtual Machines and Virtual Networks, the unique RBAC Role satisfying the requirement is ***Contributor***.

**Reference:**

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

**Quick Preview:**

Question 7: Skipped

You have an on-premises file server named Server1 that runs Windows Server 2016. You have an Azure subscription that contains an Azure file share. You deploy an Azure File Sync Storage Sync Service, and you create a sync group. You need to synchronize files from Server1 to Azure.

Which three actions should you perform in sequence?

(1) Install Azure File Sync agent on Server1

(2) Create an Azure on-premises data gateway

(3) Create a Recovery Services vault

(4) Register Server1

(5) Add a server endpoint

(6) Install the DFS Replication server role on Server1

- ○ 1 - 4 - 5 (Correct)
- ○ 2 - 5 - 6
- ○ 1 - 4 - 2
- ○ 1 - 5 - 4
- ○ 4 - 1 - 3

**Explanation**

***Step 1***: Install the Azure File Sync agent on Server1

The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share

***Step 2:*** Register Server1 - Register Windows Server with Storage Sync Service

Registering your Windows Server with a Storage Sync Service establishes a trust relationship between your server (or cluster) and the Storage Sync Service.

**Step 3:** Add a server endpoint - Create a sync group and a cloud endpoint.

A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints. A server endpoint represents a path on registered server.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide?tabs=azure-portal%2Cproactive-portal

**Quick Preview:**

Question 8: Skipped

You plan to create an Azure Storage account in the Azure region of East US 2. You need to create a storage account that meets the following requirements:

- Replicates synchronously.

- Remains available if a single data center in the region fails.

How should you configure the storage account? (SELECT TWO)

- ☐ Replication - Geo-redundant storage (GRS)
- ☐ Replication - Locally-redundant storage (LRS)
- ☐ Replication - Read-access geo-redundant storage (RA GRS)
- ☐ Replication - Zone-redundant storage (ZRS) **(Correct)**
- ☐ Account Type - Blob storage
- ☐ Account Type - Storage (general purpose v1)
- ☐ Account Type - StorageV2 (general purpose V2) **(Correct)**

**Explanation**

Zone-redundant storage (ZRS) replicates your data synchronously across three storage clusters in a single region AND ZRS only support GPv2 storage account types.

LRS would not remain available if a data center in the region fails

GRS and RA GRS use asynchronous replication.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

**Quick Preview:**

Question 9: Skipped

You plan to use the Azure Import/Export service to copy files to a storage account.

Which two files should you create before you prepare the drives for the import job? Each correct answer presents part of the solution.

- □ an XML manifest file
- □ a dataset CSV file (Correct)
- □ a JSON configuration file
- □ a PowerShell PS1 file
- □ a driveset CSV file (Correct)

**Explanation**

You need to modify the ***dataset.csv*** file in the root folder where the tool resides. Depending on whether you want to import a file or folder or both, add entries in the dataset.csv file.

You need also to modify the ***driveset.csv*** file in the root folder where the tool is. The driveset file has the list of disks and corresponding drive letters so that the tool can correctly pick the list of disks to be prepared.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-data-to-files?tabs=azure-portal

**Quick Preview:**

Question 10: Skipped

You have a Recovery Service vault that you use to test backups. The test backups contain two protected virtual machines.

You need to delete the Recovery Services vault.

What should you do first?

- ○ From the Recovery Service vault, delete the backup data.
- ○ Modify the disaster recovery properties of each virtual machine.
- ○ Modify the locks of each virtual machine
- ○ From the Recovery Service vault, stop the backup of each backup item (Correct)

**Explanation**

You can't delete a Recovery Services vault if it is registered to a server and holds backup data. If you try to delete a vault, but can't, the vault is still configured to receive backup data.

***Remove vault dependencies and delete vault***

In the vault dashboard menu, scroll down to the Protected Items section, and click Backup Items. In this menu, you can stop and delete Azure File Servers, SQL Servers in Azure VM, and Azure virtual machines.

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/backup-azure-delete-vault

**Quick Preview:**

Question 11: Skipped

You have an Azure subscription named Subscription1 that contains the resources shown in the following table:

Larger image

In Storage1, you create a blob container named blob1 and a file share named share1.

Which resources can be backed up to Vault1 ?

- ○
  VM1 only
  (Correct)
- ○
  VM1 and share1 only
- ○
  VM1 and SQL1 only
- ○
  VM1, storage1 and SQL1 only
- ○
  VM1, blob1, share1 and SQL1

**Explanation**
VM1 only can be backed up to Vault1, as VM1 is in the same region as Vault1.

- File1 is not in the same region as Vautl1.

- SQL is not in the same region as Vault1.

- Blobs cannot be backup up to service vaults.

Please note that in order to create a vault to protect virtual machines, the vault must be in the same region as the virtual machines, so VM1 meets the requirements.

**Reference:**

https://docs.microsoft.com/bs-cyrl-ba/azure/backup/backup-create-rs-vault

**Quick Preview:**

Question 12: Skipped
You have an Azure subscription named Subscription1 that contains the resources shown in the following table:
Larger image

In Storage1, you create a blob container named blob1 and a file share named share1.

Which resources can be backed up to Vault2 ?

- ○
  Storage1 only
- ○
  Share1 only
  (Correct)
- ○
  VM1 and Share1
- ○
  Blob1 and Share1
- ○
  Storage1 and SQL1

**Explanation**

Because Storage1 storage account is deployed in West US,  Share1 file share is also in West US, as Vault2.

Note: After you select Backup, the Backup pane opens and prompts you to select a storage account from a list of discovered supported storage accounts. They're either associated with this vault or present in the same region as the vault, but not yet associated to any Recovery Services vault.

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/backup-afs

**Quick Preview:**

Question 13: Skipped

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 virtual machine
- ○
  an Azure Cosmos DB database
- ○
  Azure File Storage
  (Correct)
- ○
  the Azure File Sync Storage Sync Service

**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

**Quick Preview:**

Question 14: Skipped
You have an Azure subscription. You create the Azure Storage account shown in the following exhibit:
Larger image

The minimum number of copies of the storage account will be .......... .

- ○ 1
- ○ 2
- ○ 3 (Correct)
- ○ 4

**Explanation**
Locally Redundant Storage (LRS) provides highly durable and available storage within a single location (sub region). We maintain an equivalent of 3 copies (replicas) of your data within the primary location as described in our SOSP paper; this ensures that we can recover from common failures (disk, node, rack) without impacting your storage account's availability and durability.

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

**Quick Preview:**

Question 15: Skipped
You have an Azure subscription. You create the Azure Storage account shown in the following exhibit:

Larger image

To reduce the cost of infrequently accessed data in the storage account, you must modify the .......... setting.

- ○ access tier (Correct)
- ○ performance
- ○ account kind
- ○ replication

**Explanation**
Changing the access tier from Hot to Cool would reduce the monthly cost.

Note: Azure storage offers different access tiers, which allow you to store blob object data in the most costeffective manner. The available access tiers include:

- Hot - Optimized for storing data that is accessed frequently.

- Cool - Optimized for storing data that is infrequently accessed and stored for at least 30 days.

- Archive - Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency

**Reference:**

https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers?tabs=azure-portal

**Quick Preview:**

Question 16: Skipped
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 Git1.

Webapp1 has the deployment slots shown in the following table:

Larger image

You need to ensure that the App1 update is tested before the update is made available to users.

Which two actions should you perform?

- □ Swap the slots (Correct)
- □ Deploy the App1 update to webapp1-prod, and then test the update
- □ Stop webapp1-prod
- □ Deploy the App1 update to webapp1-test, and then test the update (Correct)
- □ Stop webapp1-test

**Explanation**

Testing the webapp before going live is very important and this usually happens when new features or updates are released. In order to make sure that everything works smoothly, it is recommended that updates are pushed to a testing slot, then run the tests and if everything works as expected, simply swap the Production and Testing slots.

**Reference:**

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

**Quick Preview:**

Question 17: Skipped

You have an Azure subscription named Subscription1 that has the following providers registered:

Authorization, Automation, Resources, Compute, KeyVault, Network, Storage, Billing and Web.

Subscription1 contains an Azure virtual machine named VM1 that has the following configurations:

- Private IP address: 10.0.0.4 (dynamic)

- Network security group (NSG): NSG1

- Public IP address: None

- Availability set: AVSet

- Subnet: 10.0.0.0/24

- Managed disks: No

- Location: East US

You need to record all the successful and failed connection attempts to VM1.

Which three actions should you perform?

- □ Enable Azure Network Watcher in the East US Azure region (Correct)
- □ Add an Azure Network Watcher connection monitor
- □ Register the MicrosoftLogAnalytics provider
- □ Create an Azure Storage account
- □ Register the Microsoft.Insights resource provider (Correct)
- □ Enable Azure Network Watcher flow logs (Correct)

**Explanation**

A storage account is also needed for the whole setup to work, but the storage account already exists. Because the VM is using unmanaged disks, well ... a storage account needs to be created first. This clarifies why we don't need to create a storage account.

Taking a look at the checklist from official documentation, we also need to enable Network Watcher for the region and register a new resource provider - Microsoft.Insights.

Last, we need to enable flow logs.

**Reference:**

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal

**Quick Preview:**

Question 18: Skipped

You need to deploy an Azure virtual machine scale set that contains five instances as quickly as possible.

What should you do?

- ○ Deploy five virtual machines. Modify the Availability Zones settings for each virtual machine
- ○ Deploy five virtual machines. Modify the Size setting for each virtual machine.
- ○ Deploy one virtual machine scale set that is set to VM (virtual machines) orchestration mode
- ○ Deploy one virtual machine scale set that is set to ScaleSetVM orchestration mode (Correct)

**Explanation**

There are two orchestration modes available, as per below screenshot:

Also, by choosing ScaleSetVM, VMs are implicitly created and added to the scale set based on the VM configuration model, while with VM orchestration mode, you need to explicitly add VMs.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/orchestration-modes

**Quick Preview:**

Question 19: Skipped

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

Larger image

What is the minimum number of App Service plans you should create for the web apps?

- ○ 1
- ○ 2 (Correct)

- ○
  3
- ○
  4

**Explanation**
It is possible to add more than one webapp with different runtime stacks to the same App Service Plan, if the runtime stack is supported on the given operating system type.

So for this scenario, knowing if the runtime stack runs on Windows, Linux or both is necessary.

- .NET Core 3.0 -> supported on Windows and Linux

- ASP .NET V4.7 -> Windows only

- PHP -> Windows and Linux

- Ruby 2.6 -> Linux only

Because we have both ***Linux only*** and ***Windows only*** runtime stacks, we would need two App Service Plans, at minimum.

**Reference:**

https://docs.microsoft.com/en-us/azure/app-service/overview

**Quick Preview:**

Question 20: Skipped
You have a pay-as-you-go Azure subscription that contains the virtual machines shown in the following table:
Larger image

You create the budget shown in the following exhibit:

Larger image

The AG1 action group contains a user named user1@contoso.com only.

When the maximum amount in Budget1 is reached .......... .

- ○ VM1 and VM2 are turned off
- ○ VM1 and VM2 continue to run (Correct)
- ○ VM1 is turned off and VM2 continues to run
- ○ VM2 continues to run

**Explanation**

Budgets help you inform others about their spending to proactively manage costs, and to monitor how spending progresses over time. When the budget thresholds you've created are exceeded, only notifications are triggered. None of your resources are affected and your consumption isn't stopped. You can use budgets to compare and track spending as you analyze costs.

**Reference:**

https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/tutorial-acm-create-budgets

**Quick Preview:**

Question 21: Skipped

You have a pay-as-you-go Azure subscription that contains the virtual machines shown in the following table:

Larger image

You create the budget shown in the following exhibit:

Larger image

The AG1 action group contains a user named user1@contoso.com only.

Based on the current usage costs of the virtual machines, ........... .

- ○ no email notifications will be sent each month
- ○ one email notifications will be sent each month

(Correct)

- ○
  two email notifications will be sent each month
- ○
  three email notifications will be sent each month

**Explanation**

Budget1 is applied at RG1 scope, where only VM1 is deployed. VM1 usage is 20 Euros / day, so it will generate around 600 Euros per month. Taking a look at the alert conditions, the email is sent once 50% of the whole budget is reached, so that is 500 Euro.

Because VM1's usage is over the threshold, an email will be sent.

**Reference:**

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/cost-management-budget-scenario

**Quick preview:**

Question 22: Skipped

You have Azure subscriptions named Subscription1 and Subscription2. Subscription1 has following resource groups:

Larger image

RG1 includes a web app named App1 in the West Europe location. Subscription2 contains the following resource groups:

Larger image

`True` or `False`

App1 can be moved to RG2.

- ○
  True
- ○
  False
  (Correct)

**Explanation**

This operation was possible until end of May 2021, but now when you try to move a resource to a Resource Group with a Read-only lock, you get a very explicit error during the validation not allowing you to do the move process.

You cannot move any resource to a Resource Group with a Read-Only lock:

Error received from the portal Moving Web App:

Error received from the portal Moving App Service plan:

Same errors received using AZ CLI:

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json#considerations-before-applying-locks

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-limitations/app-service-move-limitations

**Quick Preview:**

Question 23: Skipped

You have Azure subscriptions named Subscription1 and Subscription2. Subscription1 has following resource groups:

Larger image

RG1 includes a web app named App1 in the West Europe location. Subscription2 contains the following resource groups:

Larger image

`True` or `False`

App1 can be moved to RG3.

- ○ True (Correct)
- ○ False

**Explanation**

App1 can be moved to RG3 as per official documentation.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-limitations/app-service-move-limitations

**Quick Preview:**

Question 24: Skipped

You have Azure subscriptions named Subscription1 and Subscription2.
Subscription1 has following resource groups:

Larger image

RG1 includes a web app named App1 in the West Europe location. Subscription2 contains the following resource groups:

Larger image

`True` or `False`

App1 can be moved to RG4.

- ○ True (Correct)
- ○ False

**Explanation**

App1 can be moved to RG4 as per official documentation.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-limitations/app-service-move-limitations

**Quick Preview:**

Question 25: Skipped

You have an Azure subscription named Subscription1 that contains the following resource group:

- Name: RG1

- Region: West US

- Tag: “tag1”: “value1”

You assign an Azure policy named Policy1 to Subscription1 by using the following configurations:

- Exclusions: None

- Policy definition: Append a tag and its value to resources

- Assignment name: Policy1

- Parameters:

- Tag name: Tag2

- Tag value: Value2

After Policy1 is assigned, you create a storage account that has the following configuration:

- Name: storage1

- Location: West US

- Resource group: RG1

- Tags: “tag3”: “value3”

You need to identify which tags are assigned to each resource. What should you identify? (SELECT TWO)

- □
  Tags assigned to RG1 - tag1 : value1 only
  **(Correct)**
- □
  Tags assigned to RG1 - tag2 : value2 only
- □
  Tags assigned to RG1 - tag1 : value1 only and tag2 : value2 only
- □
  Tags assigned to storage1 - tag3 : value3 only

- □
  Tags assigned to storage1 - tag1 : value1 and tag3 : value3 only
- □
  Tags assigned to storage1 - tag2 : value2 and tag3 : value3 only
  (Correct)
- □
  Tags assigned to storage1 - tag1 : value1, tag2 : value2 and tag3 : value3

**Explanation**
Azure Policy applies to new resources that are created, so it will not apply to RG1. RG1 will have only its tag applied - tag1 - value1.

Storage1 has one tag from the moment it is deployed, and this is tag3 : value3 and will get the second tag from the Azure Policy - tag2 : value2.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies

**Quick Preview:**

Question 26: Skipped
In Subscription1, you create an alert rule named Alert1. The Alert1 action group is configured as shown in the following exhibit:
Larger image

Alert1 alert criteria is triggered every minute.

The number of email messages that Alert1 will send in an hour is .......... .

- ○
  0
- ○
  4
- ○
  6
- ○
  12
- ○

60
(Correct)

**Explanation**
One alert per minute will trigger one email per minute.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-rate-limiting

**Quick Preview:**

Question 27: Skipped
In Subscription1, you create an alert rule named Alert1. The Alert1 action group is configured as shown in the following exhibit:
Larger image

Alert1 alert criteria is triggered every minute.

The number of SMS alerts that Alert1 will send in an hour is .......... .

- ○ 0
- ○ 4
- ○ 6
- ○ 12 (Correct)
- ○ 60

**Explanation**
No more than 1 SMS every 5 minutes can be sent, which equals 12 per hour.

Note: Rate limiting is a suspension of notifications that occurs when too many are sent to a particular phone number, email address or device. Rate limiting ensures that alerts are manageable and actionable.

The rate limit thresholds are:

- SMS: No more than 1 SMS every 5 minutes.

- Voice: No more than 1 Voice call every 5 minutes.

- Email: No more than 100 emails in an hour.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-rate-limiting

**Quick Preview:**

Question 28: Skipped

You create an Azure VM named Windows-Server that runs Windows Server 2019.

Windows-Server VM is configured as shown in the exhibit:

Larger image

You need to enable Desired State Configuration for Windows-Server.

What should you do first?

- ○ Connect to Windows-Server
- ○ Start Windows-Server (Correct)
- ○ Capture a snapshot of Windows-Server
- ○ Configure a DNS name for Windows-Server

**Explanation**

Status is Stopped (Deallocated).

The DSC extension for Windows requires that the target virtual machine is able to communicate with Azure, so you would need to first start the VM.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-windows

**Quick Preview:**

Question 29: Skipped

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines. You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- ○ Floating IP (direct server return) to Disabled
- ○ Idle Time-out (minutes) to 20
- ○ Protocol to UDP
- ○ Session persistence to Client IP (Correct)

**Explanation**

With Sticky Sessions when a client starts a session on one of your web servers, session stays on that specific server. To configure An Azure Load-Balancer For Sticky Sessions set Session persistence to **Client IP** or to **Client IP and protocol**.

**Reference:**

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-distribution-mode

**Quick Preview:**

Question 30: Skipped

***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.***

You have an Azure subscription that contains the following resources:

- A virtual network that has a subnet named Subnet1

- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1

- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- Priority: 100

- Source: Any

- Source port range: *

- Destination: *

- Destination port range: 3389

- Protocol: UDP

- Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

***Solution:*** You add an inbound security rule to NSG-Subnet1 that allows connections from the Any source to the * destination for port range 3389 and uses the TCP protocol. You remove NSG-VM1 from the network interface of VM1.

Does this meet the goal?

- ○ Yes (Correct)
- ○ No

**Explanation**
By default, traffic is evaluated inbound first by NSG applied at subnet level and then by NSG applied at VM NIC card level. The subnet NSG allows the traffic (any source to any destination, TCP 3389) and there is no NSG applied at VM level, so the traffic will be allowed.

**Further Learning:**

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

**Quick Preview:**

Question 31: Skipped

***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.***

You have an Azure subscription that contains the following resources:

- A virtual network that has a subnet named Subnet1

- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1

- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- Priority: 100

- Source: Any

- Source port range: *

- Destination: *

- Destination port range: 3389

- Protocol: UDP

- Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

***Solution:*** You add an inbound security rule to NSG-Subnet1 that allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the UDP protocol.

Does this meet the goal?

- ○ Yes
- ○ No (Correct)

**Explanation**
RDP traffic is TCP port 3389. For this reason, this inbound rule will not help and traffic will not be allowed.

**Further Learning:**

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

**Quick Preview:**

Question 32: Skipped
***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.***

You have an Azure subscription that contains the following resources:

- A virtual network that has a subnet named Subnet1

- Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1

- A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

- Priority: 100

- Source: Any

- Source port range: *

- Destination: *

- Destination port range: 3389

- Protocol: UDP

- Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

***Solution:*** You add an inbound security rule to NSG-Subnet1 and NSG-VM1 that allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the TCP protocol.

Does this meet the goal?

- ○ Yes (Correct)
- ○ No

**Explanation**

By default, traffic is evaluated inbound first by NSG applied at subnet level and then by NSG applied at VM NIC card level. Both subnet NSG and VM NIC card NSG allow the traffic - TCP port 3389, so the traffic will be allowed,

**Further Learning:**

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

**Quick Preview:**

Question 33: Skipped

You have a virtual network named VNet1 that has the configuration shown in the following exhibit:

Larger image

Before a virtual machine on VNet1 can receive an IP address from 192.168.1.0/24, you must first .......... .

- ○ add a network interface
- ○ add a subnet
- ○ add an address space (Correct)
- ○ delete a subnet
- ○ delete an address space

**Explanation**
Your IaaS virtual machines (VMs) and PaaS role instances in a virtual network automatically receive a private IP address from a range that you specify, based on the address space of the subnet they are connected to. We need to add the 192.168.1.0/24 address space, so a new vNET, VNet1 is using 10.2.0.0/16 address space and can allocate an IP address only from this address range.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/private-ip-addresses

**Quick Preview:**

Question 34: Skipped
You have a virtual network named VNet1 that has the configuration shown in the following exhibit:
Larger image

Before a virtual machine on VNet1 can receive an IP address from 10.2.1.0/24, you must first .......... .

- ○ add a network interface
- ○ add a subnet (Correct)
- ○ add an address space
- ○

delete a subnet

- ○
  delete an address space

**Explanation**
Only 10.2.0.0/24 subnet is currently defined, a new subnet covering 10.2.1.0/24 address range needs to be defined so that a virtual machine on VNet1 can receive an IP address from 10.2.1.0/24.

**Reference:**

https://docs.microsoft.com/en-us/azure/virtual-network/private-ip-addresses

**Quick Preview:**

Question 35: Skipped
You have an Azure subscription that contains a virtual network named VNET1.
VNET1 contains the subnets shown in the following table:
Larger image

Each virtual machine uses a static IP address.

You need to create network security groups (NSGs) to meet following requirements:

- Allow web requests from the internet to VM3, VM4, VM5, and VM6.

- Allow all connections between VM1 and VM2.

- Allow Remote Desktop connections to VM1.

- Prevent all other network traffic to VNET1.

What is the minimum number of NSGs you should create?

- ○
  1
  (Correct)
- ○
  3
- ○
  4
- ○
  12

**Explanation**

They key point is in the question itself ... ***What is the minimum*** number of NSGs you should create?

For this reason, you can create one NSG that includes all necessary rules and apply it to all three subnets.

**Reference:**

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

**Quick Preview:**

Question 36: Skipped

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

Larger image

The Not allowed resource types Azure policy 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, and then connect VM2 to VNET1.

What should you do first?

- ○ Remove Microsoft.Compute/virtualMachines from the policy (Correct)
- ○ Create an Azure Resource Manager template
- ○ Add a subnet to VNET1
- ○ Remove Microsoft.Network/virtualNetworks from the policy

**Explanation**

The Not allowed resource types Azure policy prohibits the deployment of specified resource types. You specify an array of the resource types to block.

Virtual Networks and Virtual Machines are currently prohibited, so at least remove Microsoft.Compute/virtualMachines from the policy and then create the VM2. By the way, when you create VM2, you should use an existing vNET, because creating a vNET is prohibited by the policy.

**Reference:**

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

**Quick Preview:**

Question 37: Skipped

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 an Azure DNS zone in Subscription1. The solution must minimize administrative effort.

What should you use?

- ○ Azure CLI **(Correct)**
- ○ Azure PowerShell
- ○ the Azure portal
- ○ the DNS Manager console

**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. This means that adatum.com zone file can be exported only using Azure CLI.

**Reference:**

https://docs.microsoft.com/en-us/azure/dns/dns-import-export

**Quick Preview:**

Question 38: Skipped
You have a public load balancer that balances ports 80 and 443 across three virtual machines. You need to direct all the Remote Desktop Protocol (RDP) connections to VM3 only.

What should you configure?

- ○ an inbound NAT rule
  (Correct)
- ○ a new public load balancer for VM3
- ○ a frontend IP configuration
- ○ a load balancing rule

**Explanation**
An inbound port rule can help in these kind of scenarios, when basic port-forwarding is needed.

**Reference:**

https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-port-forwarding-portal

**Quick Preview:**

Question 39: Skipped
You have an Azure subscription named Subscription1 that contains the virtual networks in the following table:
Larger image

Subscription1 contains the virtual machines in the following table:

Larger image

In Subscription1, you create a load balancer with the following options:

- Name: LB1

- SKU: Basic

- Type: Internal

- Subnet: Subnet11

- Virtual network: VNET1

Please evaluate the following statement and decide if it is `True` or `False`.

LB1 can balance the traffic between VM1 and VM2.

- ○ True (Correct)
- ○ False

**Explanation**
A load balancer is deployed at a VNET level and can load balance traffic for VMs deployed in that respective VNET. In this scenario, as VM1 and VM2 are deployed on Subnet11, which is part of VNET1, LB1 can balance the traffic between VM1 and VM2.

**Reference:**

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

**Quick Preview:**

Question 40: Skipped
You have an Azure subscription named Subscription1 that contains the virtual networks in the following table:
Larger image

Subscription1 contains the virtual machines in the following table:

Larger image

In Subscription1, you create a load balancer with the following options:

- Name: LB1

- SKU: Basic

- Type: Internal

- Subnet: Subnet11

- Virtual network: VNET1

Please evaluate the following statement and decide if it is `True` or `False`.

LB1 can balance the traffic between VM3 and VM4.

- ○ True
- ○ False (Correct)

**Explanation**
VM3 and VM4 are not part of an Availability Set, the basic load balancer will not be able to distribute traffic to these two VMs.

**Reference:**

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

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

**Quick Preview:**

Question 41: Skipped
You have an Azure subscription named Subscription1 that contains the virtual networks in the following table:
Larger image

Subscription1 contains the virtual machines in the following table:

Larger image

In Subscription1, you create a load balancer with the following options:

- Name: LB1

- SKU: Basic

- Type: Internal

- Subnet: Subnet11

- Virtual network: VNET1

Please evaluate the following statement and decide if it is `True` or `False`.

LB1 can balance the traffic between VM5 and VM6.

- ○ True
- ○ False (Correct)

**Explanation**
A load balancer is deployed at a VNET level and can load balance traffic for VMs deployed in that respective VNET. In this scenario, as VM5 and VM6 are deployed on Subnet12, which is ***NOT*** part of VNET1, so LB1 can ***NOT*** balance the traffic between VM5 and VM6.

Additionally, VM5 and VM6 are not part of an Availability Set, the basic load balancer will not be able to distribute traffic to these two VMs.

**Reference:**

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

**Quick Preview:**

Question 42: Skipped
You create a Recovery Services vault backup policy named Policy1 as shown in the following exhibit:

Larger image

The backup that occurs on Sunday, March 1, will be retained for .......... .

- ○ 30 days
- ○ 10 weeks
- ○ 36 months
- ○ 10 years
  (Correct)

**Explanation**
The yearly backup point occurs on 1st of March and its retention period is 10 years.

Question 43: Skipped
You create a Recovery Services vault backup policy named Policy1 as shown in the following exhibit:
Larger image

The backup that occurs on Sunday, November 1, will be retained for .......... .

- ○ 30 days
- ○ 10 weeks
- ○ 36 months
  (Correct)
- ○ 10 years

**Explanation**
The monthly backup point occurs on the 1st of every month and its retention period is 36 months.

Question 44: Skipped
You have an Azure subscription that contains an Azure Storage account named storage1 and the users shown in the following table:
Larger image

You plan to monitor storage1 and to configure email notifications for the signals shown in the following table:
Larger image

You need to identify the minimum number of alert rules and action groups required for the planned monitoring. (SELECT TWO)

- □ Alert rules - 1
- □ Alert rules - 2
- □ Alert rules - 3
- □ Alert rules - 4 (Correct)
- □ Action groups - 1
- □ Action groups - 2
- □ Action groups - 3 (Correct)
- □ Action groups - 4

**Explanation**

Groups to configure - Total=3:

- user1 and user 3 - one group

- user 1 - one group

- user1, user2 and user3 - one group

There are 4 event types that need to be notified, so in this case 4 rules need to be defined.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

**Quick Preview:**

Question 45: Skipped

You have an Azure virtual machine named VM1 and a Recovery Services vault named Vault1. You create a backup policy named Policy1 as shown in the exhibit:

Larger image

You configure the backup of VM1 to use Policy1 on Wednesday December 31 at 5:00PM (17:00).

You need to identify the number of available recovery points for VM1.

How many recovery points are available on January 8 at 2:00PM (14:00) and January 15 at 2:00PM (14:00)?

(Select two)

- □ January 8 at 2:00PM (14:00) - 5
- □ January 8 at 2:00PM (14:00) - 6
- □ January 8 at 2:00PM (14:00) - 8
  (Correct)
- □ January 8 at 2:00PM (14:00) - 10
- □ January 15 at 2:00PM (14:00) - 5
- □ January 15 at 2:00PM (14:00) - 8
- □ January 15 at 2:00PM (14:00) - 15
  (Correct)
- □ January 15 at 2:00PM (14:00) - 18

**Explanation**

First at all we need to understand backup schedule is set to daily. This means that only one backup is generated every day from January 1st, at 2:00AM. That means, we have only one recovery point generated every day.

Instant restore is configured to save the last 5 recovery points. But the same recovery points are stored in the correspondent retention range, so we have to count them only once.

On the other hand, depending on the conditions defined in the backup policy, every backup will be classified in only one of the retention periods, having preference the longer retention.

Therefore in our case and following backup policy definition, the following apply:

- Retention for January 2nd will be monthly one, so 24 months

- Retention for Sundays (4th and 11th in our scenario) will be weekly one, so 20 weeks

- And finally retention for all the other days will be daily, so 30 days

And because all retention are longer than 15 days, and we have only a daily backup, so a new recovery point every day, **we will have 8 recovery points on January 8th at 2:00PM, and 15 recovery points on January 15th at 2:00PM**

Please find bellow a table with retention applied to each backup from January 1 to January 15:

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/guidance-best-practices#retention-considerations

https://docs.microsoft.com/en-us/azure/backup/backup-azure-manage-vms

**Quick Preview:**

Question 46: Skipped

You have an Azure Active Directory (Azure AD) tenant named ***az104exam.onmicrosoft.com*** that contains the users shown in the following table:

Larger image

You enable password reset az104exam.onmicrosoft.com as shown in the Password Reset exhibit below:

Larger image

You configure the authentication methods for password reset as shown in the Authentication Methods exhibit below:

Larger image

Please evaluate if the following statement is `True` or `False`:

After User2 answers three security questions, he can reset his password immediately.

- ○ True
- ○ False (Correct)

**Explanation**

Two methods are required for authentication: security questions and mobile phone.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/authentication/quickstart-sspr

https://docs.microsoft.com/en-us/azure/active-directory/authentication/active-directory-passwords-faq

**Quick Preview:**

Question 47: Skipped

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

Larger image

You enable password reset az104exam.onmicrosoft.com as shown in the Password Reset exhibit below:

Larger image

You configure the authentication methods for password reset as shown in the Authentication Methods exhibit below:

Larger image

Please evaluate if the following statement is `True` or `False`:

After User1 forgets her password, she can reset the password by using the mobile phone app.

- ○ True
- ○ False (Correct)

**Explanation**

Self-service password reset is only enabled for Group2, and User1 is not a member of Group2.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/authentication/quickstart-sspr

https://docs.microsoft.com/en-us/azure/active-directory/authentication/active-directory-passwords-faq

**Quick Preview:**

Question 48: Skipped

You have an Azure Active Directory (Azure AD) tenant named ***az104exam.onmicrosoft.com*** that contains the users shown in the following table:

Larger image

You enable password reset on az104exam.onmicrosoft.com as shown in the Password Reset exhibit below:

Larger image

You configure the authentication methods for password reset as shown in the Authentication Methods exhibit below:

Larger image

Please evaluate if the following statement is `True` or `False`:

User3 can add security questions to the password reset process.

- ○ True
- ○ False (Correct)

**Explanation**
User 3 has User Administrator role assigned, but only users with Global Administrator role can access and setup Azure Active Directory Self Service Password Reset, so the statement is False.

**Reference:**

https://docs.microsoft.com/en-us/azure/active-directory/authentication/quickstart-sspr

https://docs.microsoft.com/en-us/azure/active-directory/authentication/active-directory-passwords-faq

**Quick Preview:**

Question 49: Skipped
***Case study***

***This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.***

***To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.***

***Overview***

Litware, Inc. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The Montreal office has 2,000 employees. The Seattle office has 1,000 employees. The New York office has 200 employees.

All the resources used by Litware are hosted on-premises.

Litware creates a new Azure subscription. The Azure Active Directory (Azure AD) tenant uses a domain named litware.onmicrosoft.com. The tenant uses the P1 pricing tier.

***Existing Environment***

The network contains an Active Directory forest named litware.com. All domain controllers are configured as DNS servers and host the litware.com DNS zone.

Litware has finance, human resources, sales, research, and information technology departments. Each department has an organizational unit (OU) that contains all the accounts of that respective department. All the user accounts have the department attribute set to their respective department. New users are added frequently.

Litware.com contains a user named User1.

All the offices connect by using private connections.

Litware has data centers in the Montreal and Seattle offices. Each office has a firewall that can be configured as a VPN device.

All infrastructure servers are virtualized. The virtualization environment contains the servers in the following table:

Larger image

Litware uses two web applications named App1 and App2. Each instance on each web application requires 1 GB of memory.

The Azure subscription contains the resources in the following table:

Larger image

The network security team implements several network security groups (NSGs)

***Requirements***

***Planned Changes***

Litware plans to implement the following changes:

- Deploy Azure ExpressRoute to the Montreal office.

- Migrate the virtual machines hosted on Server1 and Server2 to Azure.

- Synchronize on-premises Active Directory to Azure Active Directory (Azure AD).

- Migrate App1 and App2 to two Azure web apps named WebApp1 and WebApp2.

***Technical Requirements***

Litware must meet the following technical requirements:

- Ensure that WebApp1 can adjust the number of instances automatically based on the load and can scale up to five instances.

- Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.

- Ensure that routing information is exchanged automatically between Azure and the routers in the Montreal office.

- Enable Azure Multi-Factor Authentication (MFA) for the users in the finance department only.

- Ensure that webapp2.azurewebsites.net can be accessed by using the name app2.litware.com.

- Connect the New York office to VNet1 over the Internet by using an encrypted connection.

- Create a workflow to send an email message when the settings of VM4 are modified.

- Create a custom Azure role named Role1 that is based on the Reader role.

- Minimize costs whenever possible.

**QUESTION 1**

You need to implement Role1.

Which command should you run before you create Role1? Choose from the (1) options and (2) options to complete the following command correctly.

```
(1) -Name "Reader" | (2)
```

(1) Find-RoleCapability

(1) Get-AzureADDirectoryRole

(1) Get-AzRoleDefinition

(1) Get-AzResourceProvider

(2) ConvertFrom-Json

(2) ConvertFrom-String

(2) ConvertTo-Json

(2) ConvertTo-Xml

- □ (1) Find-RoleCapability
- □ (1) Get-AzureADDirectoryRole
- □ (1) Get-AzRoleDefinition (Correct)
- □ (1) Get-AzResourceProvider
- □ (2) ConvertFrom-Json
- □ (2) ConvertFrom-String
- □ (2) ConvertTo-Json (Correct)
- □ (2) ConvertTo-Xml

**Explanation**
**Reference:**

https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-powershell#list-a-custom-role-definition

**Quick Preview:**

Question 50: Skipped
You have an Azure subscription that contains the identities shown in the following table:
Larger image

User1, Principal1, and Group1 are assigned the `Monitoring Reader` role.

An action group named AG1 has the Email Azure Resource Manager Role notification type and is configured to email the Monitoring Reader role.

You create an alert rule named Alert1 that uses AG1. You need to identity who will receive an email notification when Alert1 is triggered.

Who should you identify?

- ○ User1 and Principal1 only
- ○ User1, User2, Principal1, and Principal2
- ○ User1 only
  (Correct)
- ○ User1 and User2 only

**Explanation**
Email will only be sent to Azure AD user members of the Monitoring Reader role. Email will not be sent to Azure AD groups or service principals.

Taking into consideration the above conditions/restrictions, only ***User1*** will receive an email notification when Alert1 is triggered.

**Reference:**

https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups

**Quick Preview:**

Question 51: Skipped
You have an Azure Linux virtual machine that is protected by Azure Backup. One week ago, two files were deleted from the virtual machine. You need to restore the deleted files to an on-premises Windows Server 2016 computer as quickly as possible.

Which four actions should you perform in sequence?

1 - Download and run the script to mount a drive on the local computer

2 - Select a restore point that contains the deleted files

3 - From the Azure portal, click ***Restore VM*** from the vault

4 - From the Azure portal, click ***File Recovery*** from the vault

5 - Mount a VHD

6 - Copy the files by using AzCopy

7 - Copy the files by using File Explorer

- ○
  4 -> 3 -> 2 -> 7
- ○
  4 -> 2 -> 1 -> 7
  (Correct)
- ○
  3 -> 4 -> 1 -> 6
- ○
  3 -> 2 -> 1 -> 6

**Explanation**
Let's run through the step-by-step process.

Azure Backup provides the capability to restore Azure virtual machines (VMs) and disks from Azure VM backups, also known as recovery points.To restore files or folders from the recovery point, you first need to go to the virtual machine, select ***Backup*** and then **STEP1 - File Recovery:**

Once you select ***File Recovery***, the ***File Recovery*** menu opens and you would need to **STEP 2 - Select a Recovery Point.**

A recovery point is a VM backup, so you should select here a date and time, before the accidental delete happened.

Next, in the same ***File Recovery*** menu, you would need to **STEP 3 - Download script**. In this step, a script will be downloaded that you will execute. The script will mount the disks from the selected recovery point as local drives on the machine where it is run.

Once the disk or disks are mounted and available to use, there is one more step to fulfil and access the deleted file, and this is **STEP 4 - Copy the files by using File Explorer**. You can use File Explorer to copy the two files on your local machine, just like you would do, for example, from an USB stick inserted into your laptop or PC.

**Reference:**

https://docs.microsoft.com/en-us/azure/backup/backup-azure-restore-files-from-vm

**Quick Preview:**

Question 52: Skipped

***Case study***

***This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.***

***To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.***

***Overview***

Litware, Inc. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The Montreal office has 2,000 employees. The Seattle office has 1,000 employees. The New York office has 200 employees.

All the resources used by Litware are hosted on-premises.

Litware creates a new Azure subscription. The Azure Active Directory (Azure AD) tenant uses a domain named litware.onmicrosoft.com. The tenant uses the P1 pricing tier.

***Existing Environment***

The network contains an Active Directory forest named litware.com. All domain controllers are configured as DNS servers and host the litware.com DNS zone.

Litware has finance, human resources, sales, research, and information technology departments. Each department has an organizational unit (OU) that contains all the accounts of that respective department. All the user accounts have the department attribute set to their respective department. New users are added frequently.

Litware.com contains a user named User1.

All the offices connect by using private connections.

Litware has data centers in the Montreal and Seattle offices. Each office has a firewall that can be configured as a VPN device.

All infrastructure servers are virtualized. The virtualization environment contains the servers in the following table:

Larger image

Litware uses two web applications named App1 and App2. Each instance on each web application requires 1 GB of memory.

The Azure subscription contains the resources in the following table:

Larger image

The network security team implements several network security groups (NSGs)

***Requirements***

***Planned Changes***

Litware plans to implement the following changes:

- Deploy Azure ExpressRoute to the Montreal office.

- Migrate the virtual machines hosted on Server1 and Server2 to Azure.

- Synchronize on-premises Active Directory to Azure Active Directory (Azure AD).

- Migrate App1 and App2 to two Azure web apps named WebApp1 and WebApp2.

***Technical Requirements***

Litware must meet the following technical requirements:

- Ensure that WebApp1 can adjust the number of instances automatically based on the load and can scale up to five instances.

- Ensure that VM3 can establish outbound connections over TCP port 8080 to the applications servers in the Montreal office.

- Ensure that routing information is exchanged automatically between Azure and the routers in the Montreal office.

- Enable Azure Multi-Factor Authentication (MFA) for the users in the finance department only.

- Ensure that webapp2.azurewebsites.net can be accessed by using the name app2.litware.com.

- Connect the New York office to VNet1 over the Internet by using an encrypted connection.

- Create a workflow to send an email message when the settings of VM4 are modified.

- Create a custom Azure role named Role1 that is based on the Reader role.

- Minimize costs whenever possible.

**QUESTION 2**

You need to recommend a solution to automate the configuration for the finance department users. The solution must meet the technical requirements.

What should you include in the recommendation?

- ○ Azure AD B2C
- ○ dynamic groups and conditional access policies **(Correct)**
- ○ Azure AD Identity Protection
- ○ an Azure logic app and the Microsoft Identity Management (MIM) client

**Explanation**
***From the Scenario:*** Ensure Azure Multi-Factor Authentication (MFA) for the users in the finance department only.

The recommendation is to use conditional access policies that can then be targeted to groups of users, specific applications, or other conditions.