PASS QUESTION

QUESTION & ANSWER

HIGHER QUALITY, BETTER SERVICE

Provide One Year Free Update!

https://www.passquestion.com

Exam : **AZ-303**

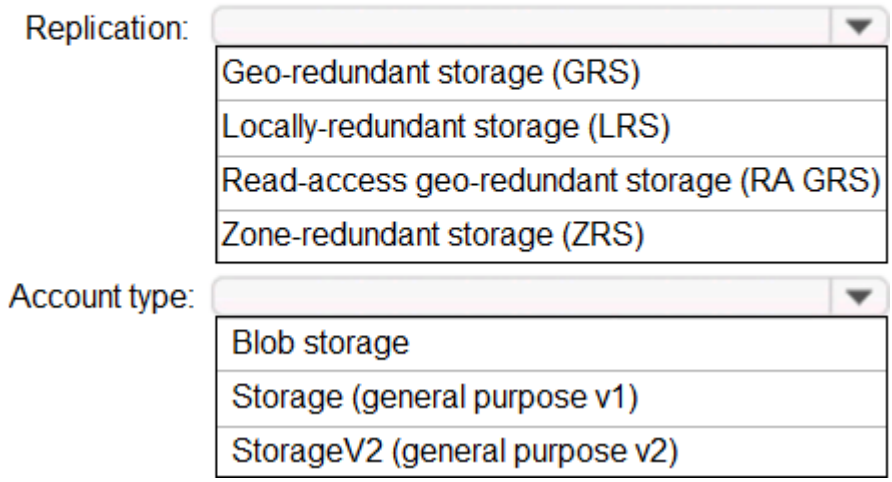
Title : Microsoft Azure Architect Technologies

Version : V8.02

1. Question Set 1

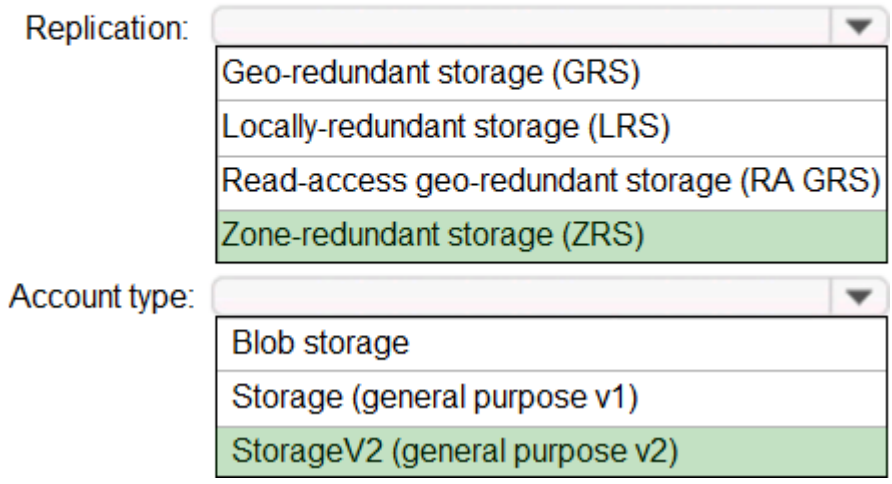
You have an Azure subscription that contains 10 virtual machines on a virtual network. You need to create a graph visualization to display the traffic flow between the virtual machines.
What should you do from Azure Monitor?
A. From Activity log, use quick insights.
B. From Metrics, create a chart.
C. From Logs, create a new query.
D. From Workbooks, create a workbook.
Answer: C
Explanation:
Navigate to Azure Monitor and select Logs to begin querying the data
Reference:
https://azure.microsoft.com/en-us/blog/analysis-of-network-connection-data-with-azure-monitor-for-virtual machines/

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



Answer:

Answer Area



Explanation:

Box 1: Zone-redundant storage (ZRS)

Zone-redundant storage (ZRS) replicates your data synchronously across three storage clusters in a single region.

LRS would not remain available if a data center in the region fails

GRS and RA GRS use asynchronous replication.

Box 2: StorageV2 (general purpose V2)

ZRS only support GPv2.

Reference:

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

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

3.HOTSPOT

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

You need to complete the template.

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

NOTE: Each correct selection is worth one point.

Answer Area

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

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

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

Answer:

Answer Area

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

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

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

Explanation:

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

Box 1: 'Microsoft.Network/networkInterfaces'

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

Microsoft.Storage/storageAccounts

Microsoft.Network/networkInterfaces

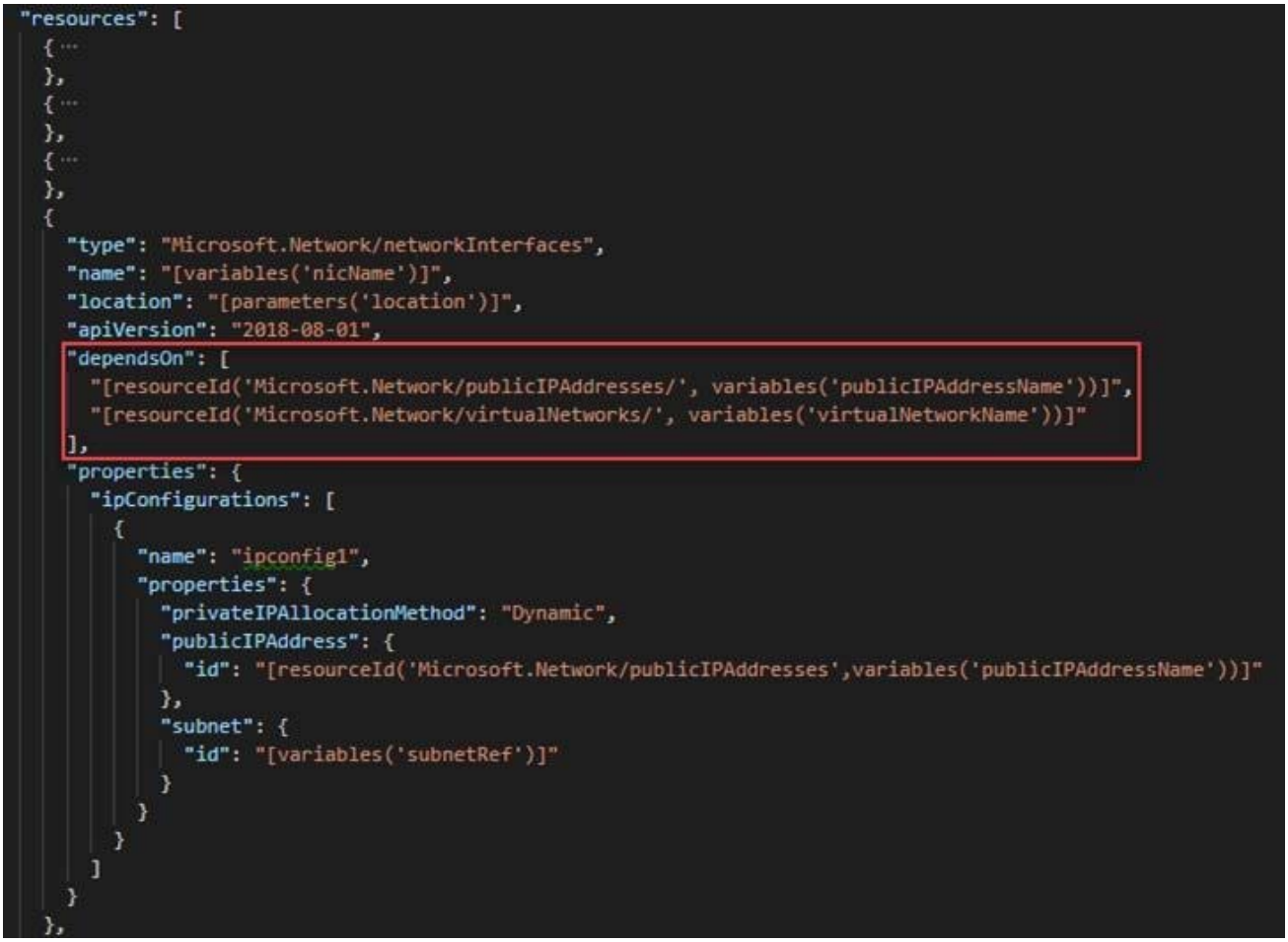
Box 2: 'Microsoft.Network/virtualNetworks/'

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

The resource depends on two other resources:

Microsoft.Network/publicIPAddresses

Microsoft.Network/virtualNetworks



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

4.HOTSPOT

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

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

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

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

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

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

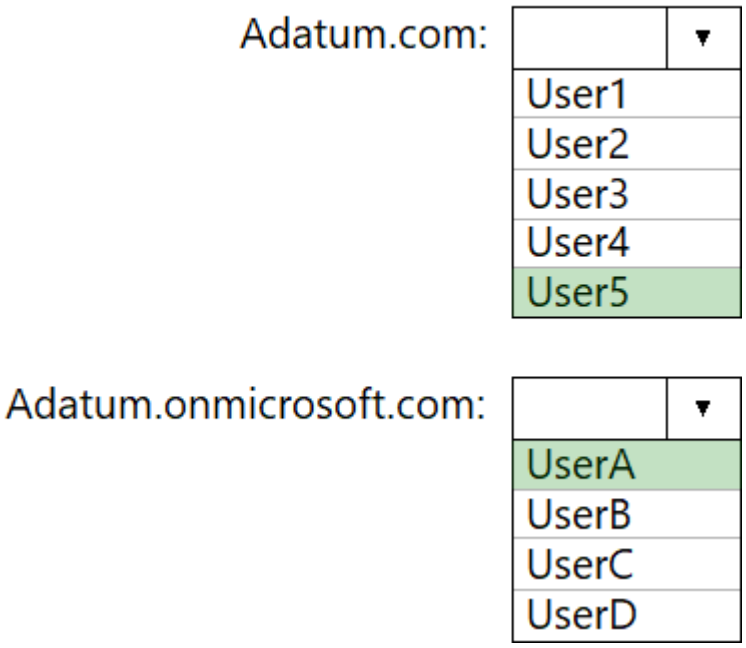
Answer Area

Adatum.com: ▼
- User1
- User2
- User3
- User4
- User5

Adatum.onmicrosoft.com: ▼
- UserA
- UserB
- UserC
- UserD

Answer:

Answer Area



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

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

D. a virtual machine that has network access to the 100 virtual machines
E. an alert action group
Answer: ABE
Explanation:
AE: You can call Azure Automation runbooks by using action groups or by using classic alerts to automate tasks based on alerts.
B: Alerts are one of the key features of Azure Monitor. They allow us to alert on actions within an Azure subscription
Reference:
https://docs.microsoft.com/en-us/azure/automation/automation-create-alert-triggered-runbook
https://techsnips.io/snips/how-to-create-and-test-azure-monitor-alerts/?page=13

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

Name	Location
RG1	West US
RG2	East US

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

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

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

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

What is the result of the deployment? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

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

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

Answer:

Answer Area

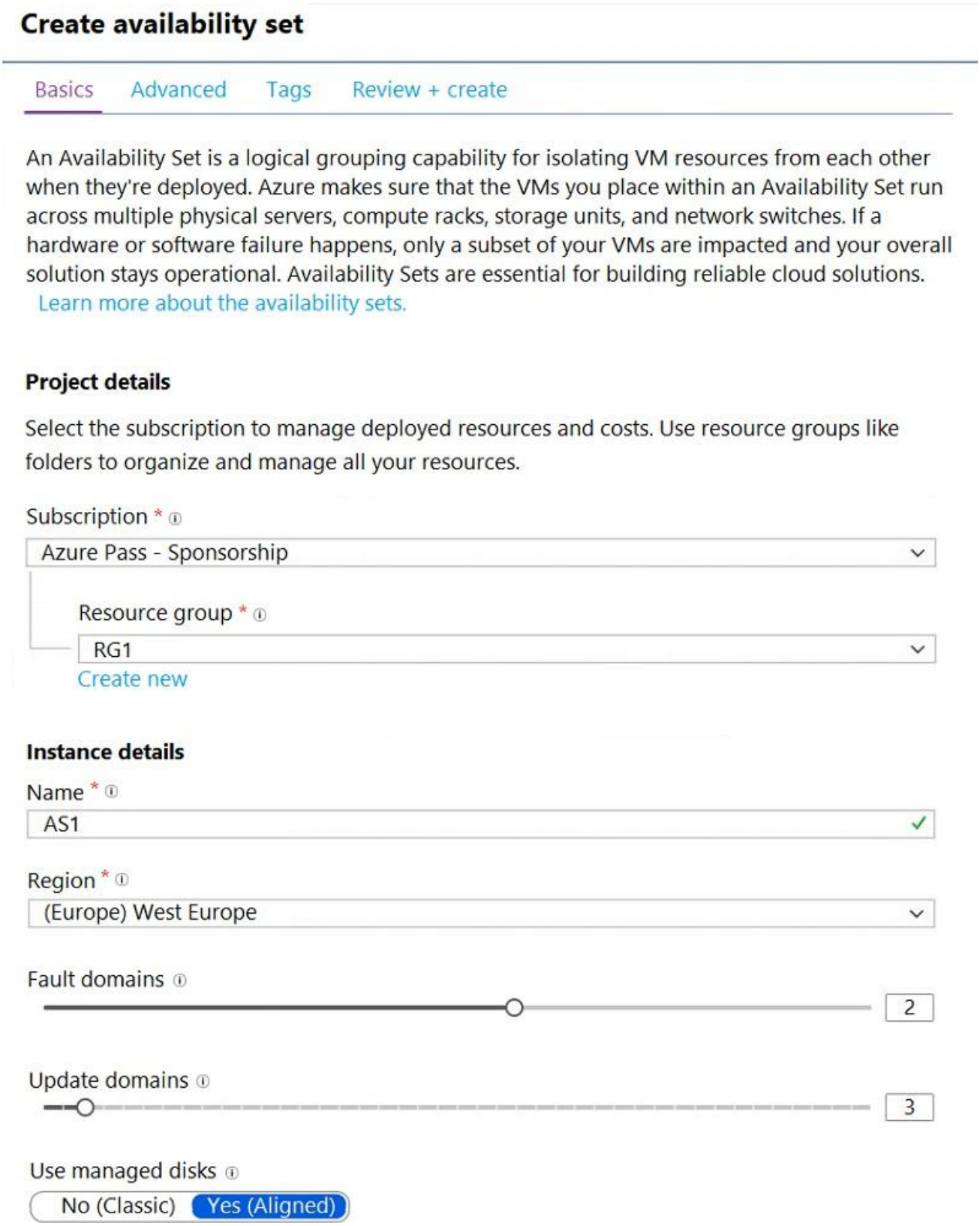
Number of public IP addresses in West US: ▼
1
2
3
4

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

7.HOTSPOT

You have an Azure subscription that contains multiple resource groups.

You create an availability set as shown in the following exhibit.



You deploy 10 virtual machines to AS1.

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

Answer Area

During planned maintenance, at least **[answer choice]** virtual machines will be available.

- 4
- 5
- 6
- 8

To add another virtual machine to AS1, the virtual machine must be added to **[answer choice]**.

- any region and the RG1 resource group
- the West Europe region and any resource group
- the West Europe region and the RG1 resource group

Answer:

Answer Area

During planned maintenance, at least **[answer choice]** virtual machines will be available.

- 4
- 5
- 6
- 8

To add another virtual machine to AS1, the virtual machine must be added to **[answer choice]**.

- any region and the RG1 resource group
- the West Europe region and any resource group
- the West Europe region and the RG1 resource group

Explanation:

Box 1: 6

Two out of three update domains would be available, each with at least 3 VMs.

An update domain is a group of VMs and underlying physical hardware that can be rebooted at the same time.

As you create VMs within an availability set, the Azure platform automatically distributes your VMs across these update domains. This approach ensures that at least one instance of your application always remains running as the Azure platform undergoes periodic maintenance.

Box 2: the West Europe region and the RG1 resource group

Reference: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/regions

8.You have an Azure subscription that contains an Azure Log Analytics workspace.

You have a resource group that contains 100 virtual machines. The virtual machines run Linux.

You need to collect events from the virtual machines to the Log Analytics workspace.

Which type of data source should you configure in the workspace?

A. Syslog

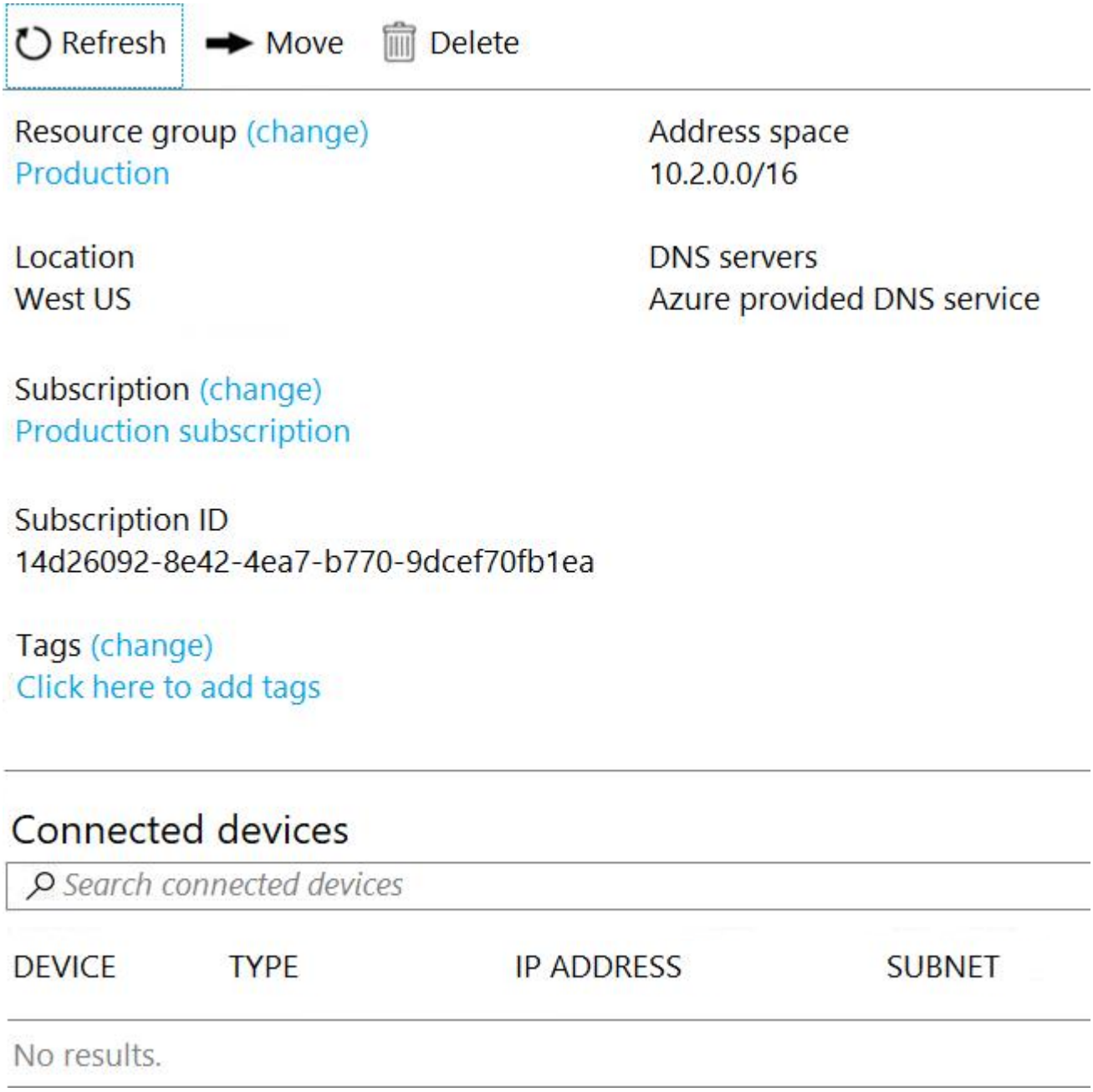
B. Linux performance counters

C. custom fields

Answer: A

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

9.You have a virtual network named VNet1 as shown in the exhibit. (Click the Exhibit tab.)



No devices are connected to VNet1.
You plan to peer VNet1 to another virtual network named VNet2. VNet2 has an address space of 10.2.0.0/16.
You need to create the peering.

What should you do first?
A. Configure a service endpoint on VNet2.
B. Add a gateway subnet to VNet1.
C. Create a subnet on VNEt1 and VNet2.
D. Modify the address space of VNet1.
Answer: D
Explanation:
The virtual networks you peer must have non-overlapping IP address spaces. The exhibit indicates that VNet1 has an address space of 10.2.0.0/16, which is the same as VNet2, and thus overlaps. We need to change the address space for VNet1.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-anddconstraints

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

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

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

Answer Area

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

Answer:

Answer Area

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

Explanation:

Box 1: Yes

The Resource group is not specified.

Box 2: No

The default value for the operating system is Windows 2016 Datacenter.

Box 3: Yes

Location is no default value.

Reference:

https://docs.microsoft.com/bs-latn-ba/azure/virtual-machines/windows/ps-template

11.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?

A. Metrics

B. Customer sights

C. Monitor
D. Advisor
Answer: D
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

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

Name	Member of
User1	Group1
User2	Group2

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

Name	Member of
Computer1	GroupA
Computer2	GroupA
Computer3	GroupB

You enable Enterprise State Roaming in contoso.com for Group1 and Group A.
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:

Answer Area

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

Explanation:

Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.

Box 1: Yes

Box 2: No

Box 3: Yes

Reference:

https://docs.microsoft.com/en-us/azure//////active-directory/devices/enterprise-state-roaming-overview

13.HOTSPOT

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

ARM Template

template1

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

    ]
  }

```

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

Answer Area

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

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

Template1 deploys **[answer choice]**.

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

Answer:

Answer Area

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

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

Template1 deploys **[answer choice]**.

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

Explanation:

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

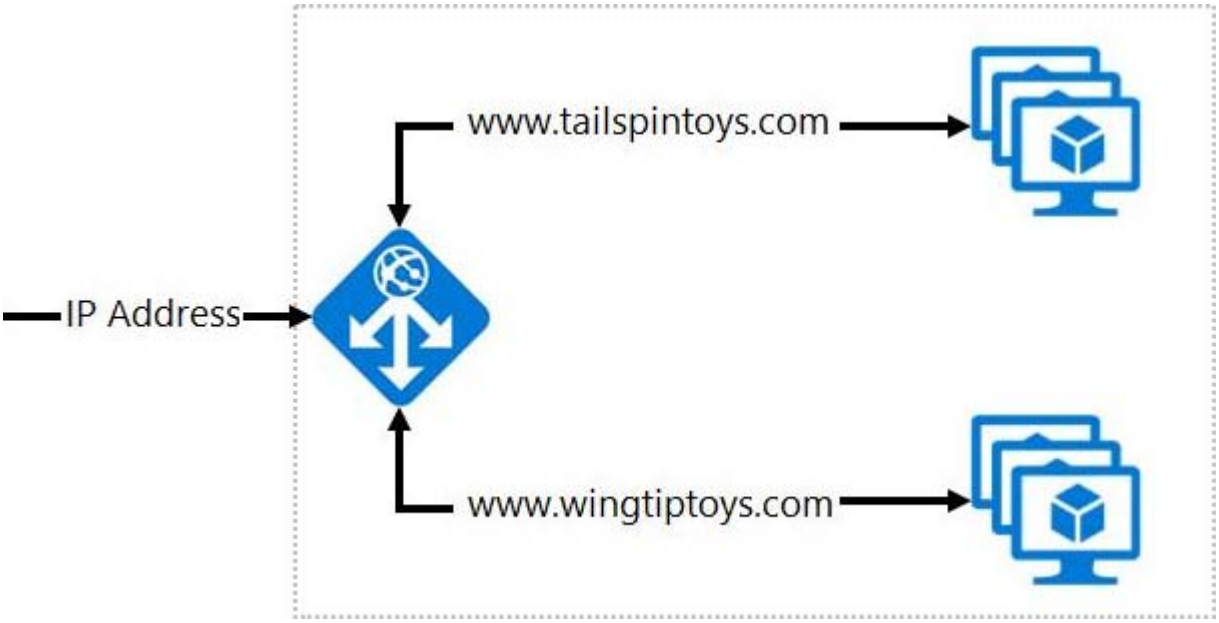
14.HOTSPOT

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

All network communications must be secured by using end to end Secure Socket Layer (SSL) encryption.

User sessions must be routed to the same server by using cookie-based session affinity.

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



Use the drop-down menus to select the answer choice that answers each question. NOTE: Each correct selection is worth one point.

Answer Area

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

Azure VPN Gateway
Azure Application Gateway
Azure ExpressRoute
Azure Network Watcher

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

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

Answer:

Answer Area

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

Azure VPN Gateway
Azure Application Gateway
Azure ExpressRoute
Azure Network Watcher

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

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

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

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

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

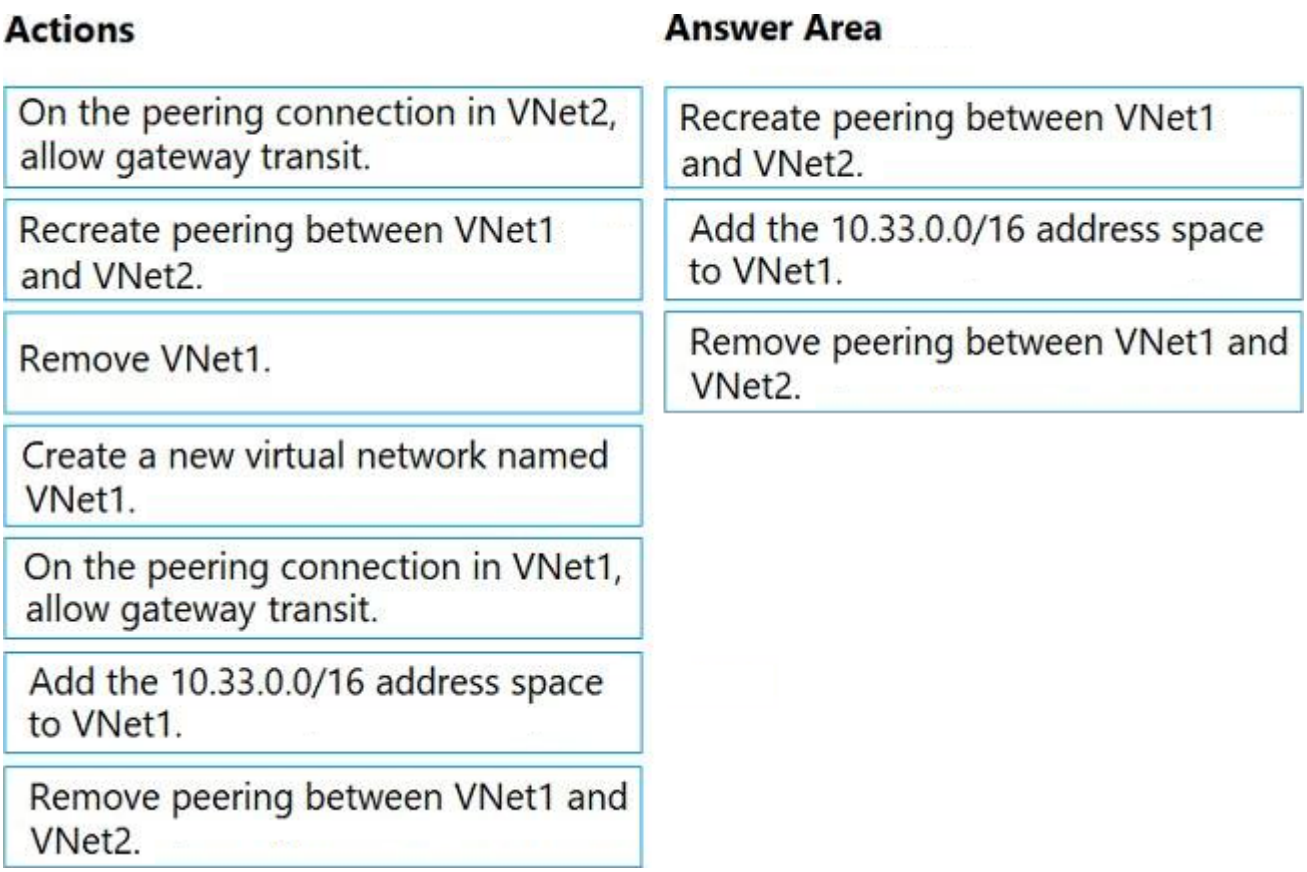
You need to add the address space of 10.33.0.0/16 to VNet1. The solution must ensure that the hosts on VNet1 and VNet2 can communicate.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

- On the peering connection in VNet2, allow gateway transit.
- Recreate peering between VNet1 and VNet2.
- Remove VNet1.
- Create a new virtual network named VNet1.
- On the peering connection in VNet1, allow gateway transit.
- Add the 10.33.0.0/16 address space to VNet1.
- Remove peering between VNet1 and VNet2.

Answer Area

Answer:



Explanation:

Step 1: Remove peering between Vnet1 and VNet2.

You can't add address ranges to, or delete address ranges from a virtual network's address space once a virtual network is peered with another virtual network. To add or remove address ranges, delete the peering, add or remove the address ranges, then re-create the peering.

Step 2: Add the 10.44.0.0/16 address space to VNet1.

Step 3: Recreate peering between VNet1 and VNet2

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

16.You have an Azure App Service app.

You need to implement tracing for the app.

The tracing information must include the following:

- Usage trends
- AJAX call responses
- Page load speed by browser
- Server and browser exceptions

What should you do?

A. Configure IIS logging in Azure Log Analytics.

B. Configure a connection monitor in Azure Network Watcher.

C. Configure custom logs in Azure Log Analytics.

D. Enable the Azure Application Insights site extension.

Answer: D

Explanation:

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

17.HOTSPOT
You have an Azure subscription named Subscription1.
Supscription1 contains the resources in the following table.

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

VNet1 is in RG1. VNet2 is in RG2. There is no connectivity between VNet1 and VNet2. An administrator named Admin1 creates an Azure virtual machine 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? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

First action:

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

Second action:

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

Answer:

Answer Area

First action:

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

Second action:

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

Explanation:

We cannot just move a virtual machine between networks.

What we need to do is identify the disk used by the VM, delete the VM itself while retaining the disk, and recreate the VM in the target virtual network and then attach the original disk to it.

Reference:

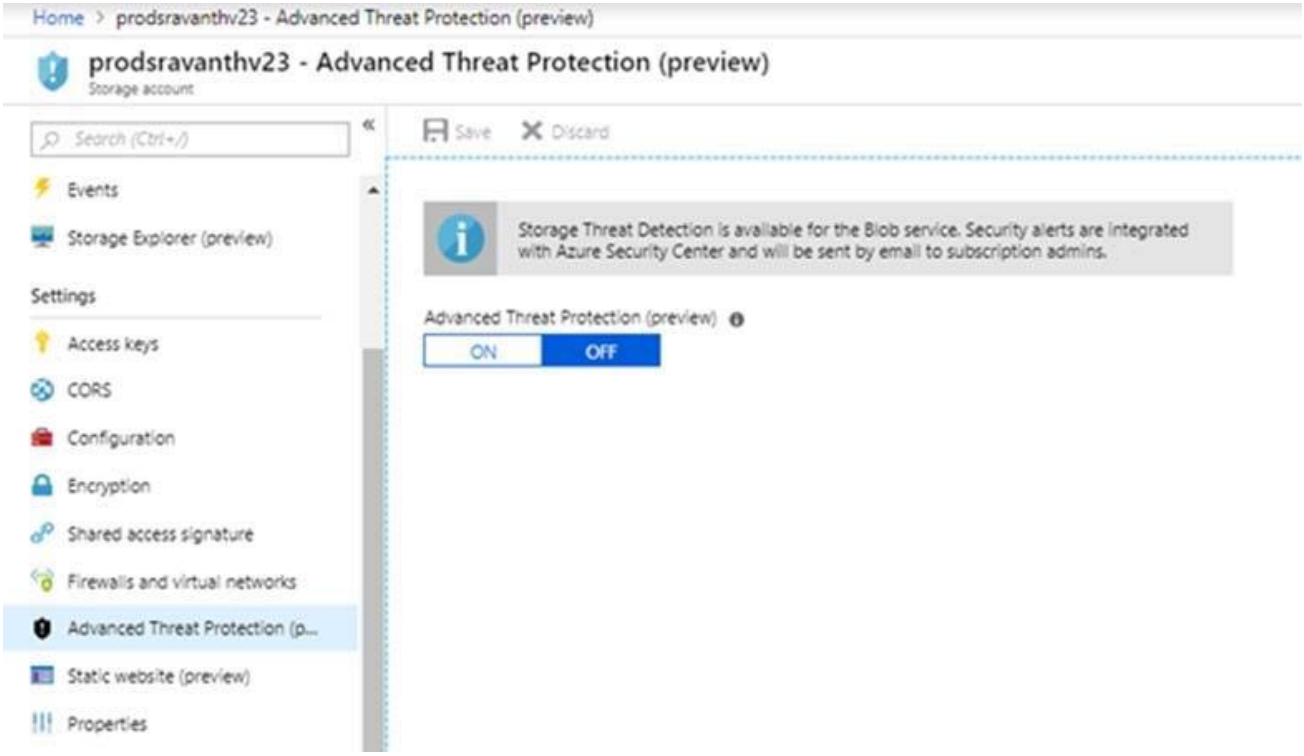
https://blogs.technet.microsoft.com/canitpro/2014/06/16/step-by-step-move-a-vm-to-a-different-vnet-on-azure/

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

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

Name	Contains
storagecontoso1	A blob service and a table service
storagecontoso2	A blob service and a file service
storagecontoso3	A queue service
storagecontoso4	A file service and a queue service
storagecontoso5	A table service

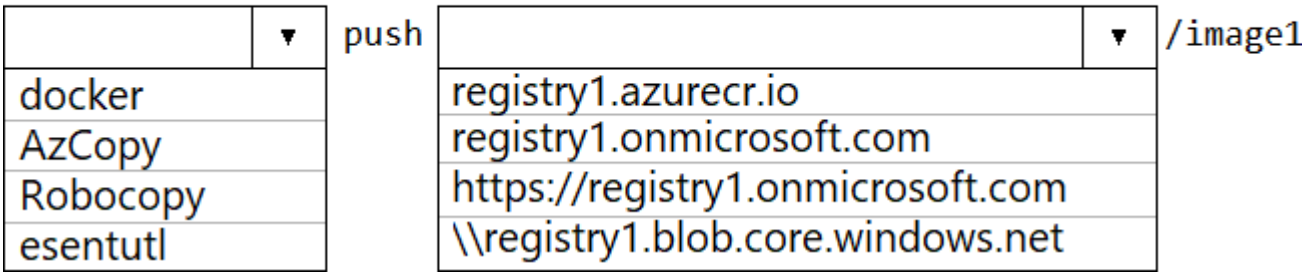
You enable Storage Advanced Threat Protection (ATP) for all the storage accounts. You need to identify which storage accounts will generate Storage ATP alerts.
Which two storage accounts should you identify? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. storagecontoso1
B. storagecontoso2
C. storagecontoso3
D. storagecontoso4
E. storagecontoso5
Answer: AB
Explanation:
Storage Threat Detection is available for the Blob Service.



Reference:
https://azure.microsoft.com/en-us/blog/advanced-threat-protection-for-azure-storage-now-in-public-preview/

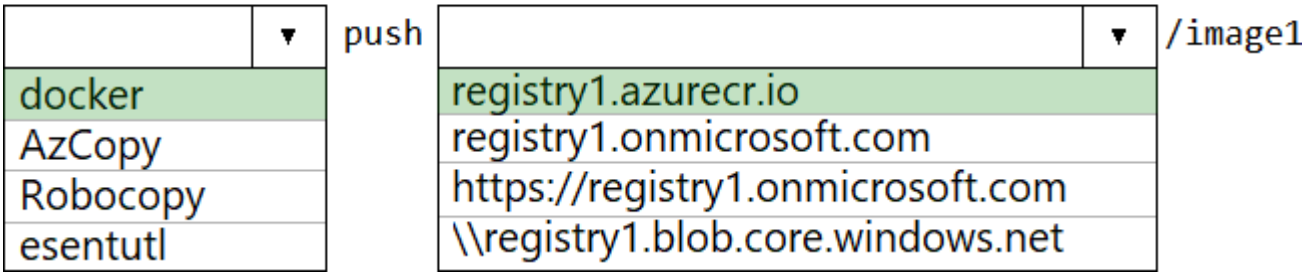
19.HOTSPOT
You company has an Azure Container Registry named Registry1. You have an Azure virtual machine named Server1 that runs Windows Server 2019. From Server1, you create a container image named image1. You need to add image1 to Registry1.
Which command should you run on Server1? To answer, select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

Answer Area



Answer:

Answer Area



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

20.HOTSPOT
You are developing an Azure Web App. You configure TLS mutual authentication for the web app. You need to validate the client certificate in the web app.
To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:

Answer Area

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

21.DRAG DROP

You are designing a solution to secure a company's Azure resources. The environment hosts 10 teams.

Each team manages a project and has a project manager, a virtual machine (VM) operator, developers, and contractors.
Project managers must be able to manage everything except access and authentication for users. VM operators must be able to manage VMs, but not the virtual network or storage account to which they are connected. Developers and contractors must be able to manage storage accounts.
You need to recommend roles for each member.
What should you recommend? To answer, drag the appropriate roles to the correct employee types. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.

Roles

- Owner
- Contributor
- Reader
- Virtual Machine Contributor
- Storage Account Contributor

Answer Area

Employee type	Role
Project manager	Role
VM operators	Role
Developers	Role
Contractors	Role

Answer:

Roles

- Owner
- Contributor
- Reader
- Virtual Machine Contributor
- Storage Account Contributor

Answer Area

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

22.You have an Azure virtual machine named VM1 and an Azure Active Directory (Azure AD) tenant

named adatum.com.
VM1 has the following settings:
- IP address: 10.10.0.10
- System-assigned managed identity: On
You need to create a script that will run from within VM1 to retrieve the authentication token of VM1.
Which address should you use in the script?
A. vm1.adatum.com.onmicrosoft.com
B. 169.254.169.254
C. 10.10.0.10
D. vm1.adatum.com
Answer: B
Explanation:
Your code that's running on the VM can request a token from the Azure Instance Metadata Service identity endpoint, accessible only from within the VM:
http://169.254.169.254/metadata/identity/oauth2/token
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

23.HOTSPOT
Your company has a virtualization environment that contains the virtualization hosts shown in the following table.

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

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

Name	Generation	Memory	Operating system (OS)	OS disk	Data disk
VM1	*Not applicable*	4 GB	Windows Server 2016	200 GB	800 GB
VM2	*Not applicable*	12 GB	Red Hat Enterprise Linux 7.2	3 TB	200 GB
VM3	*Not applicable*	32 GB	Windows Server 2012 R2	200 GB	1 TB
VMA	1	8 GB	Windows Server 2012	100 GB	2 TB
VMB	1	16 GB	Red Hat Enterprise Linux 7.2	150 GB	3 TB
VMC	2	24 GB	Windows Server 2016	500 GB	6 TB

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

Answer Area

The virtual machines that can be migrated from Server1:

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

The virtual machines that can be migrated from Server2:

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

Answer:

Answer Area

The virtual machines that can be migrated from Server1:

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

The virtual machines that can be migrated from Server2:

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

Explanation:

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

24.You are designing an Azure solution.
The solution must meet the following requirements:
- Distribute traffic to different pools of dedicated virtual machines (VMs) based on rules.
- Provide SSL offloading capabilities.
You need to recommend a solution to distribute network traffic.
Which technology should you recommend?
A. Azure Application Gateway
B. Azure Load Balancer
C. Azure Traffic Manager
D. server-level firewall rules
Answer: A
Explanation:
If you require "SSL offloading", application layer treatment, or wish to delegate certificate management to Azure, you should use Azure's layer 7 load balancer Application Gateway instead of the Load Balanacer.
Incorrect Answers:
D: Because Load Balancer is agnostic to the TCP payload and TLS offload ("SSL") is not provided.
Reference: https://docs.microsoft.com/en-us/azure/application-gateway/overview

25. Testlet 2

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.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

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 severs 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.
- 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.

HOTSPOT

You need to identify the storage requirements for Contoso.

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

Answer Area

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

Answer:

Answer Area

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

Explanation:

Box 1: Yes

Scenario: Move the existing product blueprint files to Azure Blob storage.

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

Page blobs are optimized for writes at random locations within a blob. They also support Unmanaged Disks.

Scenario:

SQL Server Data Files in Microsoft Azure enables native support for SQL Server database files stored as blobs. It allows you to create a database in SQL Server running in on-premises or in a virtual machine in Microsoft Azure with a dedicated storage location for your data in Microsoft Azure Blob storage.

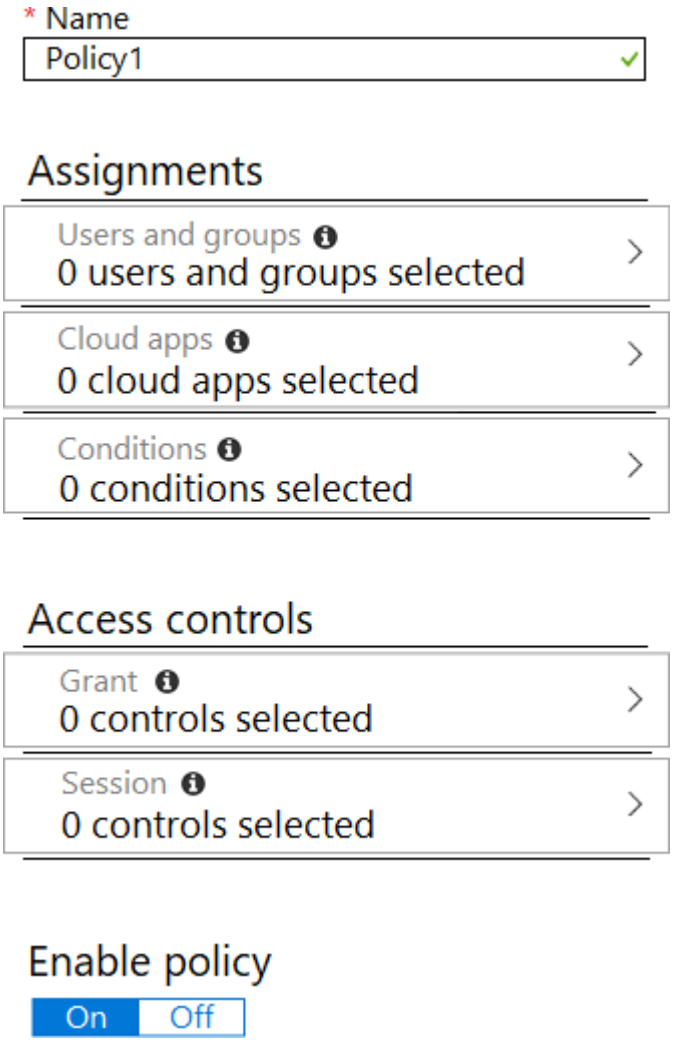
Box 2: No

Box 3: No

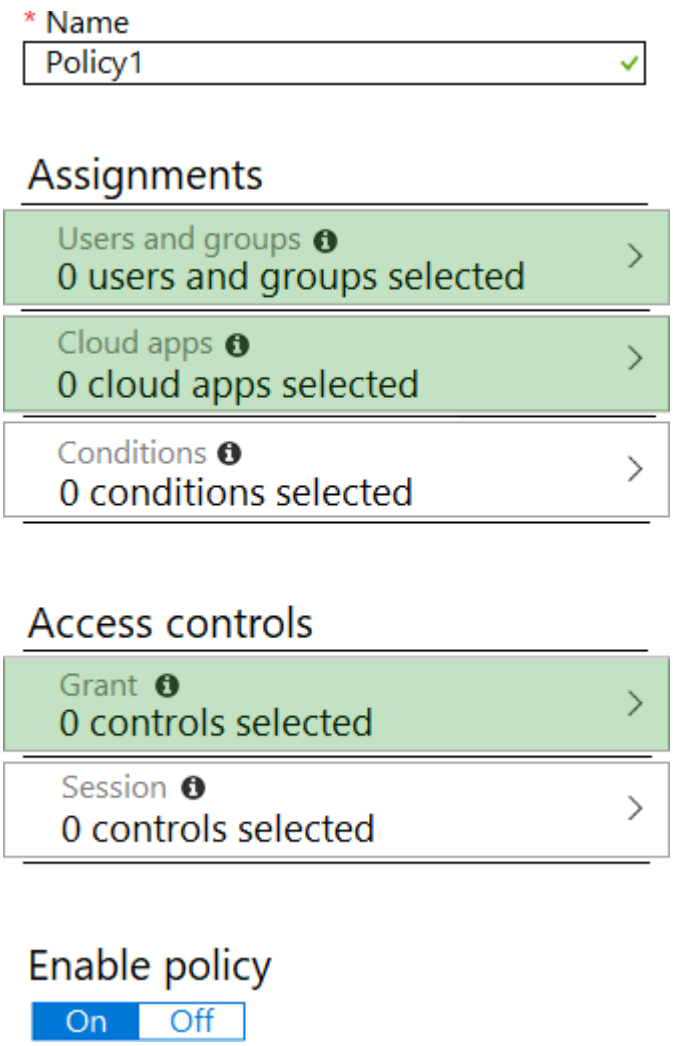
Reference:
https://docs.microsoft.com/en-us/sql/relational-databases/databases/sql-server-data-files-in-microsoft-azure

26. Question Set 1

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



Answer:



Explanation:

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa

27.You are implementing authentication for applications in your company. You plan to implement self-service password reset (SSPR) and multifactor authentication (MFA) in Azure Active Directory (Azure AD). You need to select authentication mechanisms that can be used for both MFA and SSPR.

Which two authentication methods should you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Authenticator app

B. Email addresses

C. App passwords

D. Short Message Service (SMS) messages

E. Security questions

Answer: AD

Explanation:

The following authentication mechanisms can be used for both MFA and SSPR:

- Short Message Service (SMS) messages
- Azure AD passwords
- Microsoft Authenticator app

- Voice call
- Incorrect Answers:
B, E: The following authentication mechanisms are used for SSPR only:
- Email addresses
- Security questions
E: App passwords authentication mechanisms can be used for MFA only, but only in certain cases.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

28.Your company has the groups shown in the following table.

Group	Number of members
Managers	10
Sales	100
Development	15

The company has an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. An administrator named Admin1 attempts to enable Enterprise State Roaming for all the users in the Managers groups.
Admin1 reports that the options for Enterprise State Roaming are unavailable from Azure AD. You verify that Admin1 is assigned the Global administrator role. You need to ensure that Admin1 can enable Enterprise State Roaming.
What should you do?
A. Assign an Azure AD Privileged Identity Management (PIM) role to Admin1.
B. Purchase an Azure Rights Management (Azure RMS) license for each user in the Managers group.
C. Enforce Azure Multi-Factor Authentication (MFA) for Admin1.
D. Purchase an Azure AD Premium P1 license for each user in the Managers group.
Answer: D
Explanation:
Enterprise State Roaming is available to any organization with an Azure AD Premium or Enterprise Mobility + Security (EMS) license.
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/devices/enterprise-state-roaming-enable

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

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

You enable self-service password reset (SSPR) for Group1.
You configure the Notifications settings as shown in the following exhibit.

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

Answer Area

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

Answer:

Answer Area

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

Explanation:
Box 1: Yes
Notify all admins when other admins reset their passwords: Yes.

Box 2: No
Notify users on password resets: No.
Box 3: No
- Notify users on password resets
If this option is set to Yes, then users resetting their password receive an email notifying them that their password has been changed. The email is sent via the SSPR portal to their primary and alternate email addresses that are on file in Azure AD. No one else is notified of the reset event.
- Notify all admins when other admins reset their passwords
If this option is set to Yes, then all administrators receive an email to their primary email address on file in Azure AD. The email notifies them that another administrator has changed their password by using SSPR.
Example: There are four administrators in an environment. Administrator A resets their password by using SSPR. Administrators B, C, and D receive an email alerting them of the password reset.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr

30.Your company has an Azure subscription. You enable multi-factor authentication (MFA) for all users. The company's help desk reports an increase in calls from users who receive MFA requests while they work from the company's main office. You need to prevent the users from receiving MFA requests when they sign in from the main office.
What should you do?
A. From Conditional access in Azure Active Directory (Azure AD), create a named location.
B. From the MFA service settings, create a trusted IP range.
C. From Conditional access in Azure Active Directory (Azure AD), create a custom control.
D. From Azure Active Directory (Azure AD), configure organizational relationships.
Answer: B
Explanation:
The first thing you may want to do, before enabling Multi-Factor Authentication for any users, is to consider configuring some of the available settings. One of the most important features is a trusted IPs list. This will allow you to whitelist a range of IPs for your network. This way, when users are in the office, they will not get prompted with MFA, and when they take their devices elsewhere, they will. Here's how to do it:
Log in to your Azure Portal.
Navigate to Azure AD > Conditional Access > Named locations.
From the top toolbar select Configure MFA trusted IPs.
Reference: https://www.kraftkennedy.com/implementing-azure-multi-factor-authentication/

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

Answer Area

On App1:

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

On Queue1:

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

Answer:

Answer Area

On App1:

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

On Queue1:

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

Explanation:

On App1: Turn on the managed identity

To use Service Bus with managed identities, you need to assign the identity the role and the appropriate scope. The procedure in this section uses a simple application that runs under a managed identity and accesses Service Bus resources.

Once the application is created, follow these steps:

1. Go to Settings and select Identity.

2. Select the Status to be On.
3. Select Save to save the setting.
On Queue1: Configure Access Control (IAM)
Azure Active Directory (Azure AD) authorizes access rights to secured resources through role-based access control (RBAC). Azure Service Bus defines a set of built-in RBAC roles that encompass common sets of permissions used to access Service Bus entities and you can also define custom roles for accessing the data.
Assign RBAC roles using the Azure portal
In the Azure portal, navigate to your Service Bus namespace. Select Access Control (IAM) on the left menu to display access control settings for the namespace. If you need to create a Service Bus namespace.
Select the Role assignments tab to see the list of role assignments. Select the Add button on the toolbar and then select Add role assignment.
Reference:
https://docs.microsoft.com/en-us/azure/service-bus-messaging/authenticate-application
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-managed-service-identity

32.You have an application named App1 that does not support Azure Active Directory (Azure AD) authentication.
You need to ensure that App1 can send messages to an Azure Service Bus queue. The solution must prevent App1 from listening to the queue.
What should you do?
A. Configure Access control (IAM) for the Service Bus.
B. Add a shared access policy to the queue.
C. Modify the locks of the queue.
D. Configure Access control (IAM) for the queue.
Answer: B
Explanation:
There are two ways to authenticate and authorize access to Azure Service Bus resources: Azure Activity Directory (Azure AD) and Shared Access Signatures (SAS). Each Service Bus namespace and each Service Bus entity has a Shared Access Authorization policy made up of rules.
Reference:
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-authentication-and-authorization
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-sas

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

B. Enable Application Insights
C. Operating System
D. Plan type
Answer: D
Explanation:
The Backup and Restore feature requires the App Service plan to be in the Standard, Premium or Isolated tier.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/manage-backup#requirements-and-restrictions

34.HOTSPOT
You have an Azure subscription.
You plan to deploy an app that has a web front end and an application tier.
You need to recommend a load balancing solution that meets the following requirements:
- Internet to web tier:
  -Provides URL-based routing
  -Supports connection draining
  -Prevents SQL injection attacks
- Web tier to application tier:
  - Provides port forwarding
  - Supports HTTPS health probes
  - Supports an availability set as a backend pool

Which load balancing solution should you recommend for each tier? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Internet to web tier:

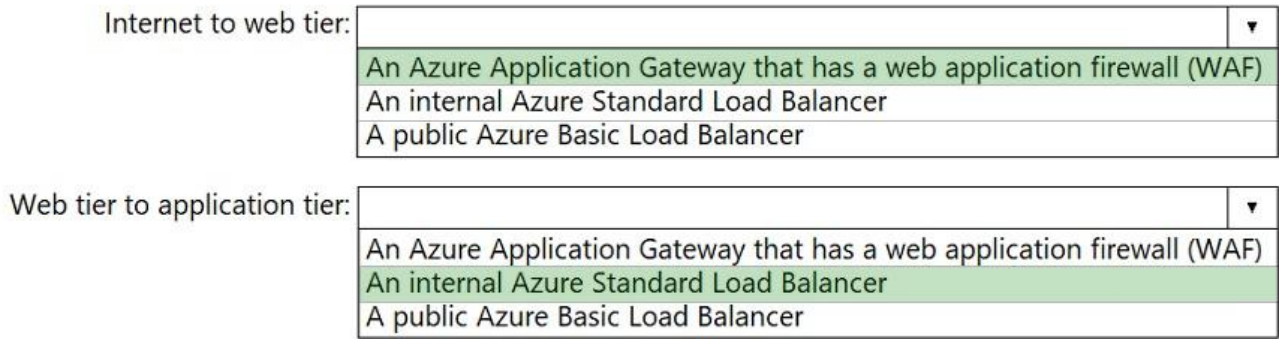
- An Azure Application Gateway that has a web application firewall (WAF)
- An internal Azure Standard Load Balancer
- A public Azure Basic Load Balancer

Web tier to application tier:

- An Azure Application Gateway that has a web application firewall (WAF)
- An internal Azure Standard Load Balancer
- A public Azure Basic Load Balancer

Answer:

Answer Area



Explanation:

Box 1: An Azure Application Gateway that has a web application firewall (WAF)

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

Application Gateway operates as an application delivery controller (ADC). It offers Secure Sockets Layer (SSL) termination, cookie-based session affinity, round-robin load distribution, content-based routing, ability to host multiple websites, and security enhancements.

Box 2: An internal Azure Standard Load Balancer

The internet to web tier is the public interface, while the web tier to application tier should be internal.

Note: When using load-balancing rules with Azure Load Balancer, you need to specify a health probes to allow Load Balancer to detect the backend endpoint status.

Health probes support the TCP, HTTP, HTTPS protocols.

Reference:

https://docs.microsoft.com/en-us/azure/application-gateway/waf-overview

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview

35.You have 10 Azure virtual machines on a subnet named Subnet1. Subnet1 is on a virtual network named VNet1.

You plan to deploy a public Azure Standard Load Balancer named LB1 to the same Azure region as the 10 virtual machines.

You need to ensure that traffic from all the virtual machines to the internet flows through LB1. The solution must prevent the virtual machines from being accessible on the internet.

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

A. Add health probes to LB1.

B. Add the network interfaces of the virtual machines to the backend pool of LB1.

C. Add an inbound rule to LB1.

D. Add an outbound rule to LB1.

E. Associate a network security group (NSG) to Subnet1.

F. Associate a user-defined route to Subnet1.

Answer: ABD

Explanation:
A: To allow the Load Balancer to monitor the status of your app, you use a health probe. The health probe dynamically adds or removes VMs from the Load Balancer rotation based on their response to health checks.
B: To distribute traffic to the VMs, a backend address pool contains the IP addresses of the virtual (NICs) connected to the Load Balancer.
D: A Load Balancer rule is used to define how traffic is distributed to the VMs. Only outbound traffic is allowed.
Reference:
https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-standard-manage-portal2

36.You have SQL Server on an Azure virtual machine named SQL1.
You need to automate the backup of the databases on SQL1 by using Automated Backup v2 for the virtual machines.
The backups must meet the following requirements:
- Meet a recovery point objective (RPO) of 15 minutes.
- Retain the backups for 30 days.
- Encrypt the backups at rest.
What should you provision as part of the backup solution?
A. Elastic Database jobs
B. Azure Key Vault
C. an Azure Storage account
D. a Recovery Services vault
Answer: C
Explanation:
An Azure storage account is used for storing Automated Backup files in blob storage. A container is created at this location to store all backup files. The backup file naming convention includes the date, time, and database GUID.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/automated-backup

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

Name	Connected to
VM1	VNET1/Subnet1
VM2	VNET1/Subnet2

KeyVault1 has an access policy that provides several users with Create Key permissions.
You need to ensure that the users can only register secrets in KeyVault1 from VM1.
What should you do?
A. Create a network security group (NSG) that is linked to Subnet1.
B. Configure the Firewall and virtual networks settings for KeyVault1.
C. Modify the access policy for KeyVault1.

D. Configure KeyVault1 to use a hardware security module (HSM).

Answer: C

Explanation:

You grant data plane access by setting Key Vault access policies for a key vault.

Note 1: Grant our VM's system-assigned managed identity access to the Key Vault.

1. Select Access policies and click Add new.
2. In Configure from template, select Secret Management.
3. Choose Select Principal, and in the search field enter the name of the VM you created earlier. Select the VM in the result list and click Select.
4. Click OK to finishing adding the new access policy, and OK to finish access policy selection.

Note 2: Access to a key vault is controlled through two interfaces: the management plane and the data plane. The management plane is where you manage Key Vault itself. Operations in this plane include creating and deleting key vaults, retrieving Key Vault properties, and updating access policies. The data plane is where you work with the data stored in a key vault. You can add, delete, and modify keys, secrets, and certificates.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad

https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault2

38.HOTSPOT

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1.

You add the users in the following table.

User	Role
User1	Owner
User2	Security Admin
User3	Network Contributor

Which user can perform each configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Add a subnet to VNet1:

- User1 only
- User3 only
- User1 and User3 only
- User2 and User3 only
- User1, User2, and User3

Assign a user the Reader role to VNet1:

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Answer:

Answer Area

Add a subnet to VNet1:

- **User1 only**
- User3 only
- User1 and User3 only
- User2 and User3 only
- User1, User2, and User3

Assign a user the Reader role to VNet1:

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- **User1, User2, and User3**

Explanation:

Box 1: User1 only.

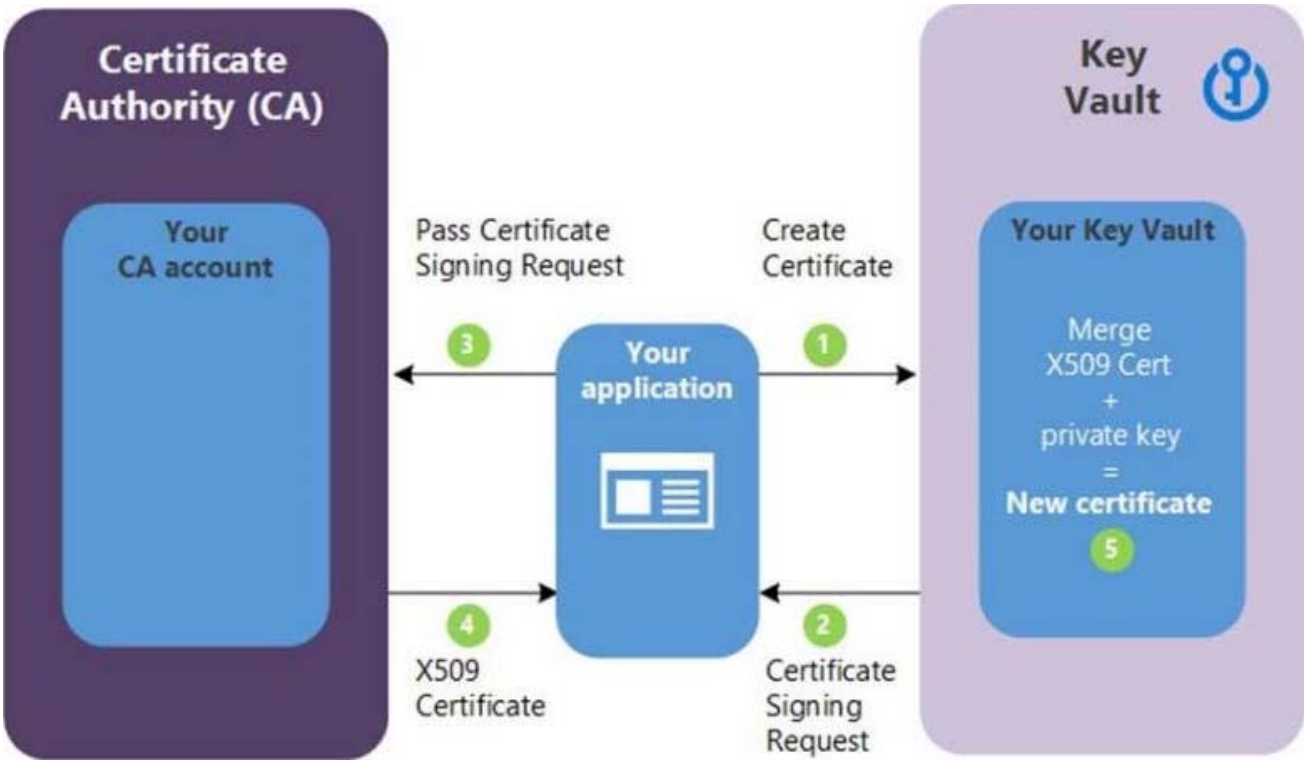
User1: The Owner Role lets you manage everything, including access to resources.

Not User3: The Network Contributor role lets you manage networks, but not access to them.
Box 2: User1 and User2 only
The Security Admin role: In Security Center only: Can view security policies, view security states, edit security policies, view alerts and recommendations, dismiss alerts and recommendations.
Reference: https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

39.You have resources in three Azure regions. Each region contains two virtual machines. Each virtual machine has a public IP address assigned to its network interface and a locally installed application named App1.
You plan to implement Azure Front Door-based load balancing across all the virtual machines.
You need to ensure that App1 on the virtual machines will only accept traffic routed from Azure Front Door.
What should you implement?
A. Azure Private Link
B. service endpoints
C. network security groups (NSGs) with service tags
D. network security groups (NSGs) with application security groups
Answer: C
Explanation:
Configure IP ACLing for your backends to accept traffic from Azure Front Door's backend IP address space and Azure's infrastructure services only.
Refer the IP details below for ACLing your backend:
- Refer AzureFrontDoor.Backend section in Azure IP Ranges and Service Tags for Front Door's IPv4 backend IP address range or you can also use the service tag AzureFrontDoor.Backend in your network security groups.
Reference: https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq

40.You have an Azure key vault named KV1.
You need to ensure that applications can use KV1 to provision certificates automatically from an external certification authority (CA).
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.
A. From KV1, create a certificate issuer resource.
B. Obtain the CA account credentials.
C. Obtain the root CA certificate.
D. From KV1, create a certificate signing request (CSR).
E. From KV1, create a private key,
Answer: CD
Explanation:
C: Obtain the root CA certificate (step 4 in the picture below)
D: From KV1, create a certificate signing request (CSR) (step 2 in the picture below)
Note:
Creating a certificate with a CA not partnered with Key Vault
This method allows working with other CAs than Key Vault's partnered providers, meaning your

organization can work with a CA of its choice.



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

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

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

41.You create the following Azure role definition.

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

You need to create Role1 by using the role definition.

Which two values should you modify before you create Role1? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. AssignableScopes

B. Description

C. DataActions

D. IsCustom

E. Id

Answer: AD

Explanation:

Part of example:

```
"IsCustom": true,
  "AssignableScopes": [
    "/subscriptions/{subscriptionId1}",
    "/subscriptions/{subscriptionId2}",
    "/subscriptions/{subscriptionId3}"
```

The following shows what a custom role looks like as displayed in JSON format. This custom role can be used for monitoring and restarting virtual machines.

```
{
  "Name": "Virtual Machine Operator",
  "Id": "88888888-8888-8888-8888-888888888888",
  "IsCustom": true,
  "Description": "Can monitor and restart virtual machines.",
  "Actions": [
    "Microsoft.Storage/*/read",
    "Microsoft.Network/*/read",
    "Microsoft.Compute/*/read",
```

```
      "Microsoft.Compute/virtualMachines/start/action",
      "Microsoft.Compute/virtualMachines/restart/action",
      "Microsoft.Authorization/*/read",
      "Microsoft.ResourceHealth/availabilityStatuses/read",
      "Microsoft.Resources/subscriptions/resourceGroups/read",
      "Microsoft.Insights/alertRules/*",
      "Microsoft.Insights/diagnosticSettings/*",
      "Microsoft.Support/*"
   ],
   "NotActions": [],
   "DataActions": [],
   "NotDataActions": [],
   "AssignableScopes": [
      "/subscriptions/{subscriptionId1}",
      "/subscriptions/{subscriptionId2}",
      "/subscriptions/{subscriptionId3}"
   ]
}
```

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

42. Testlet 2

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.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

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 severs 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.
- 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.

You need to recommend an identity solution that meets the technical requirements.
What should you recommend?
A. password hash synchronization and single sign-on (SSO)
B. federated single sign-on (SSO) and Active Directory Federation Services (AD FS)
C. Pass-thorough Authentication and single sign-on (SSO)
D. cloud-only user accounts
Answer: C
Explanation:
With Pass-through Authentication the on-premises passwords are never stored in the cloud in any form.
Scenario:
- Prevent user passwords or hashes of passwords from being stored in Azure.
- 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.
Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

43. Question Set 1

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a server named Server1 that runs Windows Server 2019. Server1 is a container host.
You are creating a Dockerfile to build a container image.
You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.
Solution: You add the following line to the Dockerfile.
COPY File1.txt /Folder1/
You then build the container image.
Does this meet the goal?
A. Yes
B. No
Answer: A
Explanation:
Copy is the correct command to copy a file to the container image.
Reference:
https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy
https://docs.docker.com/engine/reference/builder/

44.Note: This question is part of a series of questions that present the same scenario. Each question in

the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a server named Server1 that runs Windows Server 2019. Server1 is a container host.
You are creating a Dockerfile to build a container image.
You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.
Solution: You add the following line to the Dockerfile.
XCOPY File1.txt C:\Folder1\
You then build the container image.
Does this meet the goal?
A. Yes
B. No
Answer: B
Explanation:
Copy is the correct command to copy a file to the container image. Furthermore, the root directory is specified as '/' and not as 'C:/'.
Reference:
https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy
https://docs.docker.com/engine/reference/builder/

45.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a server named Server1 that runs Windows Server 2019. Server1 is a container host.
You are creating a Dockerfile to build a container image.
You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.
Solution: You add the following line to the Dockerfile.
ADD File1.txt C:/Folder1/
You then build the container image.
Does this meet the goal?
A. Yes
B. No
Answer: B
Explanation:
Copy is the correct command to copy a file to the container image. The ADD command can also be used. However, the root directory is specified as '/' and not as 'C:/'.
Reference:
https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy
https://docs.docker.com/engine/reference/builder/

46.Note: This question is part of a series of questions that present the same scenario. Each question in

the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Active Directory (Azure AD) tenant named contoso.com. A user named Admin1 attempts to create an access review from the Azure Active Directory admin center
and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other identity Governance settings are available. Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles. You need to ensure that Admin1 can create access reviews in contoso.com.
Solution: You create an access package.
Does this meet the goal?
A. Yes
B. No
Answer: B
Explanation:
You do not use access packages for Identity Governance. Instead use Azure AD Privileged Identity Management.
Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include: Conduct access reviews to ensure users still need roles
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview

47.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Active Directory (Azure AD) tenant named contoso.com. A user named Admin1 attempts to create an access review from the Azure Active Directory admin center
and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other identity Governance settings are available. Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles. You need to ensure that Admin1 can create access reviews in contoso.com.
Solution: You purchase an Azure Directory Premium P2 license for contoso.com.
Does this meet the goal?
A. Yes
B. No
Answer: B
Explanation:
Instead use Azure AD Privileged Identity Management.
Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about.

Key features of PIM include:
- Conduct access reviews to ensure users still need roles
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

48.Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Active Directory (Azure AD) tenant named contoso.com.
A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other identity Governance settings are available.
Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.
You need to ensure that Admin1 can create access reviews in contoso.com.
Solution: You assign the Global administrator role to Admin1.
Does this meet the goal?
A. Yes
B. No
Answer: B
Explanation:
Instead use Azure AD Privileged Identity Management.
Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include: Conduct access reviews to ensure users still need roles
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

49.Your network contains an on-premises Active Directory domain named contoso.com that contains a member server named Server1.
You have the accounts shown in the following table.

Name	Member of
CONTOSO\User1	Domain Admins
CONTOSO\User2	Domain Users
CONTOSO\User3	Enterprise Admin
SERVER1\User4	Users

You are installing Azure AD Connect on Server1.
You need to specify the account for Azure AD Connect synchronization. The solution must use the principle of least privilege.
Which account should you specify?

A. CONTOSO\User2
B. SERVER1\User4
C. CONTOSO\User1
D. CONTOSO\User3
Answer: A
Explanation:
The default Domain User permissions are sufficient
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

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

Answer Area

Component	Action
Domain	Join the VMs to the existing on-premises domain. Join the VMs to a new domain controller VM in Azure. Join the VMs to Azure Active Directory Domain Services (AD DS).
Connectivity	Set up VPN connectivity. Set up HTTPS connectivity. Set up Azure Relay Service.

Answer:

Answer Area

Component	Action
Domain	Join the VMs to a new domain controller VM in Azure.
Connectivity	Set up VPN connectivity.

Domain options:
- Join the VMs to the existing on-premises domain.
- Join the VMs to a new domain controller VM in Azure.
- Join the VMs to Azure Active Directory Domain Services (AD DS).

Connectivity options:
- Set up VPN connectivity.
- Set up HTTPS connectivity.
- Set up Azure Relay Service.

Explanation:

Box 1: Join the VMs to a new domain controller VM in Azure

Azure provides two solutions for implementing directory and identity services in Azure:

- (Used in this scenario) Extend your existing on-premises Active Directory infrastructure to Azure, by deploying a VM in Azure that runs AD DS as a Domain Controller. This architecture is more common when the on-premises network and the Azure virtual network (VNet) are connected by a VPN or ExpressRoute connection.
- Use Azure AD to create an Active Directory domain in the cloud and connect it to your on-premises Active Directory domain. Azure AD Connect integrates your on-premises directories with Azure AD.

Box 2: Set up VPN connectivity.

This architecture is more common when the on-premises network and the Azure virtual network (VNet) are connected by a VPN or ExpressRoute connection.

Reference: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/identity/

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

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

For which web app can you configure a WebJob?

A. WebApp1

B. WebApp4

C. WebApp2

D. WebApp3

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

52. Testlet 2

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.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

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 severs 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.

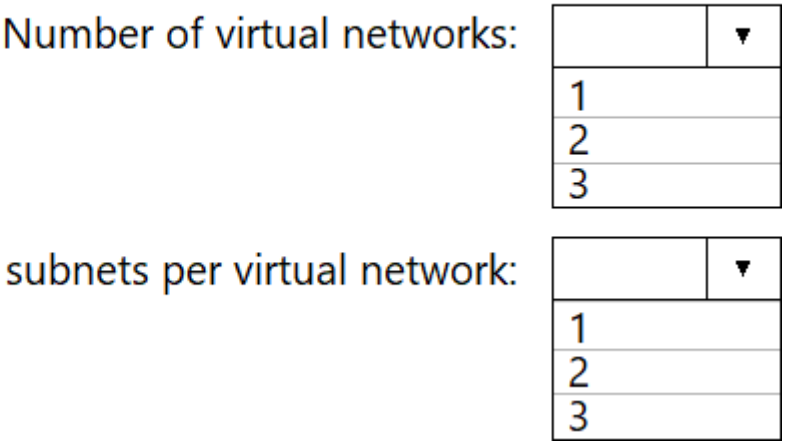
Requirements
Planned Changes
Contoso plans to implement the following changes to the infrastructure:
- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

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.
- 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.

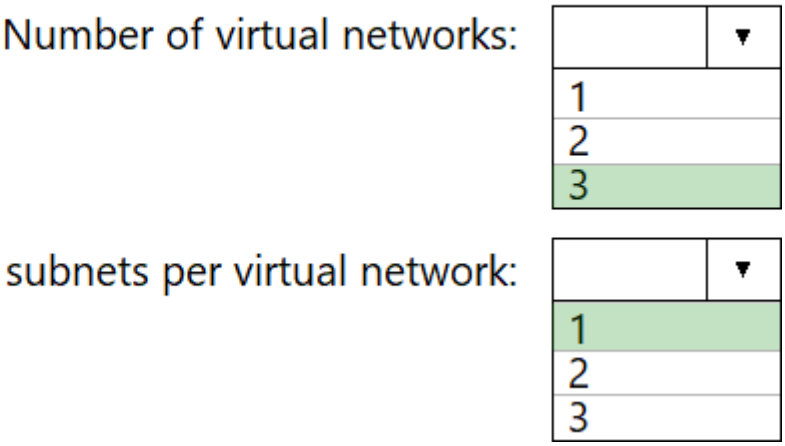
HOTSPOT
You need to recommend a solution for App1. The solution must meet the technical requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

Box 1: 3

One virtual network for every tier

Box 2: 1

Only one subnet for each tier, to minimize the number of open ports.

Scenario: You have a public-facing application named App1.

App1 is comprised of the following three tiers:

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

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

Technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.

53. Question Set 1

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

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

You need to create the Azure Cosmos DB databases to meet the developer request. The solution must minimize costs.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. Create three Azure Cosmos DB accounts, one for the databases that use the Core (SQL) API, one for CosmosDB2, and one for CosmosDB4.
B. Create two Azure Cosmos DB accounts, one for CosmosDB2 and CosmosDB4 and one for CosmosDB1 and CosmosDB3.
C. Create one Azure Cosmos DB account for each database.
D. Create three Azure Cosmos DB accounts, one for the databases that use the MongoDB API, one for CosmosDB1, and one for CosmosDB3.
Answer: BD
Explanation:
Note: Microsoft recommends using the same API for all access to the data in a given account.
One throughput provisioned container per subscription for SQL, Gremlin API, and Table accounts. Up to three throughput provisioned collections per subscription for MongoDB accounts. The throughput provisioned on an Azure Cosmos container is exclusively reserved for that container. The container receives the provisioned throughput all the time.
Incorrect Answers:
A: DB2 and DB4 can use the same account.
C: The most costly alternative.
Reference:
https://docs.microsoft.com/en-us/azure/cosmos-db/set-throughput#set-throughput-on-a-container

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

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

You plan to specify sqlserver1 as the primary server in a failover group.
Which servers can be used as a secondary server?
A. sqlserver4 and sqlserver5 only
B. sqlserver2 and sqlserver3 only
C. sqlserver1 and sqlserver3 only
D. sqlserver2 and sqlserver4 only
Answer: D
Explanation:
The Resource Group must be the same. The secondary server can have another location. The secondary server cannot be the same as the primary server.
Reference: https://docs.microsoft.com/en-us/azure/azure-sql/database/auto-failover-group-configure

55.You have two Azure SQL Database managed instances in different Azure regions. You plan to configure the managed instances in an instance failover group.
What should you configure before you can add the managed instances to the instance failover group?
A. an internal Azure Load Balancer instance that has managed instance endpoints in a backend pool
B. Azure Private Link that has endpoints on two virtual networks
C. an Azure Application Gateway that has managed instance endpoints in a backend pool
D. a Site-to-Site VPN between the virtual networks that contain the instances
Answer: D
Explanation:
For two managed instances to participate in a failover group, there must be either ExpressRoute or a gateway configured between the virtual networks of the two managed instances to allow network communication.
You create the two VPN gateways and connect them.
1. Create the gateway for the virtual network of your primary managed instance using the Azure portal.
2. Create the gateway for the virtual network of your secondary managed instance using the Azure portal.
3. Create a bidirectional connection between the two gateways of the two virtual networks.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/failover-group-add-instance-tutorial?tabs=azure-portal#4---create-a-primary-gateway