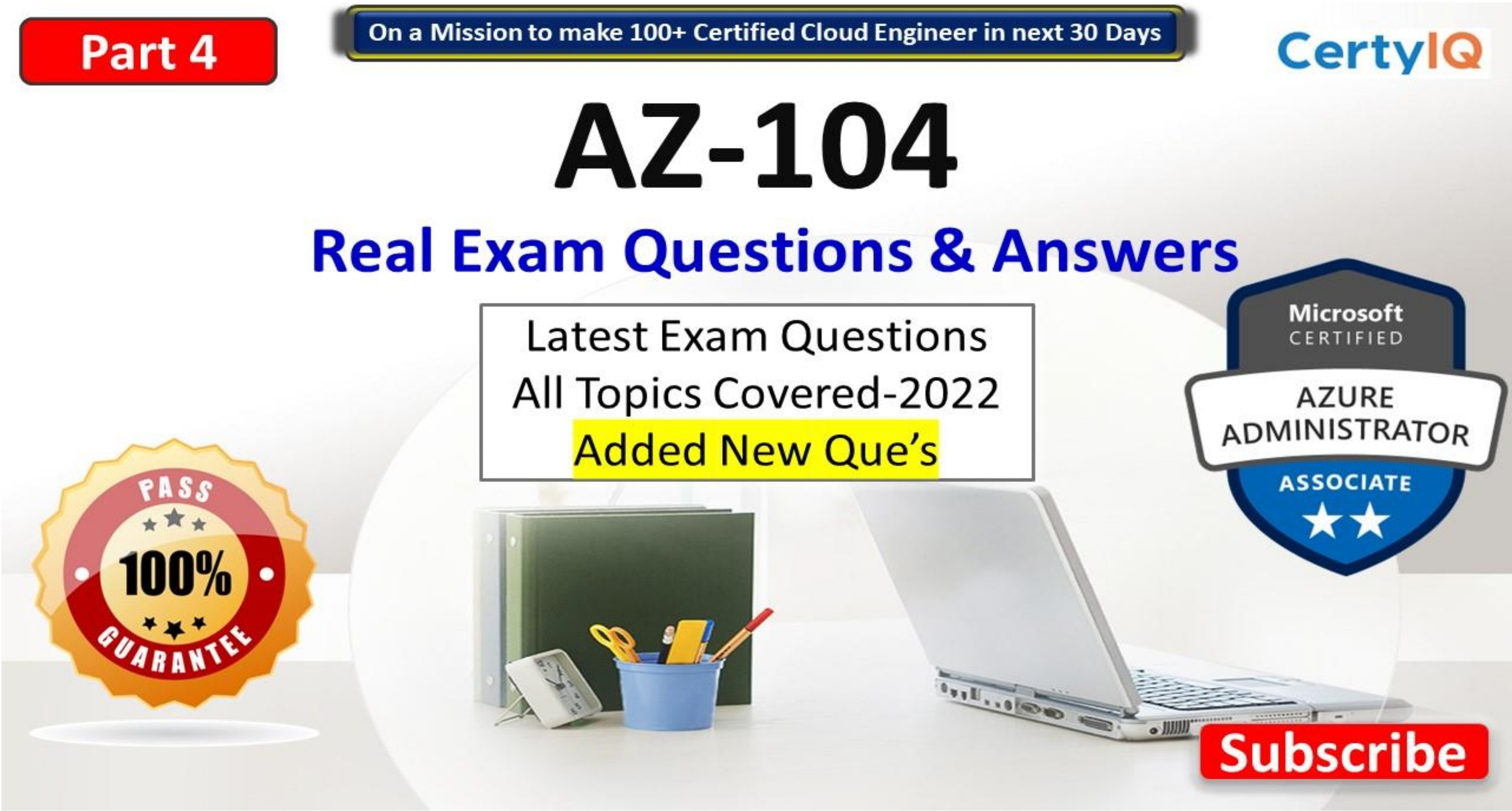
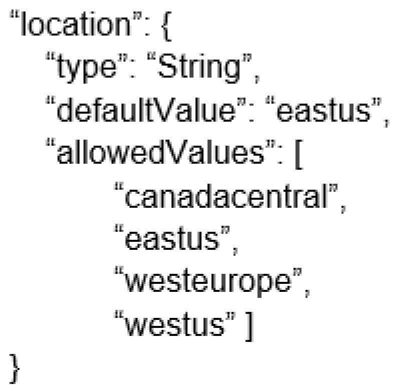


Question 121

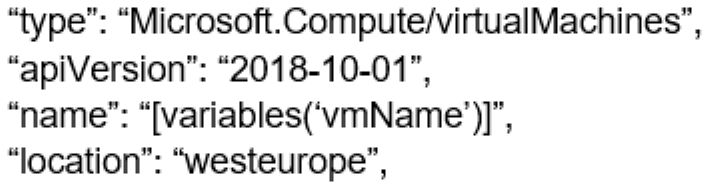
CertyIQ

You have an Azure Resource Manager template named Template1 that is used to deploy an Azure virtual machine.
Template1 contains the following text:



```
"location": {
   "type": "String",
   "defaultValue": "eastus",
   "allowedValues": [
         "canadacentral",
         "eastus",
         "westeurope",
         "westus" ]
}
```

The variables section in Template1 contains the following text:
"location": "westeurope"
The resources section in Template1 contains the following text:



```
"type": "Microsoft.Compute/virtualMachines",
"apiVersion": "2018-10-01",
"name": "[variables('vmName')]",
"location": "westeurope",
```

You need to deploy the virtual machine to the West US location by using Template1.
What should you do?

A. Modify the location in the resources section to westus

B. Select West US during the deployment

C. Modify the location in the variables section to westus

Explanation:

Correct Answer: A

You can change the location in resources. Parameters used to define the value of some variables to be able to use in different places in the template resources. Resources are used only for complicated expressions. In any case, RM will only deploy from resources. In case the value is not mentioned directly, then it will check parameters if it is specified in the resources. Based on this question, the value of location is defined directly in resources. so you change the resources location value.

Use location parameter. To allow flexibility when deploying your template, use a parameter to specify the location for resources. Set the default value of the parameter to resourceGroup().location.

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/resource-location?tabs=azure-powershell

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

Question 122 CertyIQ

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?

A. From Plan1, scale up the App Service plan

B. From webapp1, modify the Application settings

C. From webapp1, add a custom domain

D. From Plan1, scale out the App Service plan

Explanation:

Correct Answer: A

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.

Scale out: Increase the number of VM instances that run your app. You can scale out to as many as 30 instances

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

Question 123 CertyIQ

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?

A. one virtual machine scale set that has 10 virtual machines instances

B. one Availability Set that has three fault domains and one update domain

C. one Availability Set that has 10 update domains and one fault domain

D. one virtual machine scale set that has 12 virtual machines instances

Explanation:

Correct Answer: A

VM Scale Set consists of a set of identically configured VMs.

Availability Set consists of a set of discrete VMs.

No more than 20% of the Scale Set upgrading at any time, then 2 machines out of 10 will have maintenance, the 8 remaining VMs will be up.

Virtual machine scale sets are created with five fault domains by default in Azure regions with no zones. For the regions that support zonal deployment of virtual machine scale sets and this option is selected, the default value of the fault domain count is 1 for each of the zones. FD=1 in this case implies that the VM instances belonging to the scale set will be spread across many racks on a best effort basis.

Reference:

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

https://docs.microsoft.com/en-us/learn/modules/build-app-with-scale-sets/2-features-benefits-virtual-machine-scale-sets

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-automatic-upgrade

Question 124 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure virtual machine named VM1 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?

[✓ A. Yes]

[✓ B. No]

Explanation:

Correct Answer: B - No

You need to specify Log Analytics as the source for this alert, and not the VM as source for the alert.

1. You create an Azure Log Analytics workspace and configure the data settings.

2. You install the Microsoft Monitoring Agent on VM1.

3. 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

Question 125

CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure virtual machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.
You receive a notification that VM1 will be affected by maintenance.
You need to move VM1 to a different host immediately.
Solution: From the Overview blade, you move the virtual machine to a different subscription.
Does this meet the goal?

A. Yes

[✓ B. No]

Explanation:

Correct Answer: B - No

Changing Subscription won't affect the downtime, it will just you change the billing. You would need to redeploy the VM. After you redeploy a VM, the temporary disk is lost, and dynamic IP addresses associated with virtual network interface are updated.

From Overview there is no option to move the VM to another hardware to skip the maintenance.

Ideally you need an Availability Set and defining the Update Domains.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/redeploy-to-new-node

Question 126 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure virtual machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.
You receive a notification that VM1 will be affected by maintenance.
You need to move VM1 to a different host immediately.
Solution: From the Redeploy blade, you click Redeploy.
Does this meet the goal?

A. Yes

B. No

Explanation:

Correct Answer: A - Yes

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.

Use the Azure portal. Select the VM you wish to redeploy, then select the Redeploy button in the Settings blade. You may need to scroll down to see the Support and Troubleshooting section that contains the 'Redeploy' button.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/redeploy-to-new-node

Question 127 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure virtual machine named VM1. VM1 was deployed by using a custom Azure Resource Manager template named ARM1.json.
You receive a notification that VM1 will be affected by maintenance.
You need to move VM1 to a different host immediately.

Solution: From the Update management blade, you click Enable.
Does this meet the goal?

A. Yes

B. No

Explanation:

Correct Answer: B - No

You would need to redeploy the VM.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/redeploy-to-new-node

Question 128 CertyIQ

You have an Azure subscription that contains a web app named webapp1.
You need to add a custom domain named www.contoso.com to webapp1.
What should you do first?

A. Create a DNS record

B. Add a connection string

C. Upload a certificate.

D. Stop webapp1.

Explanation:

Correct Answer: A

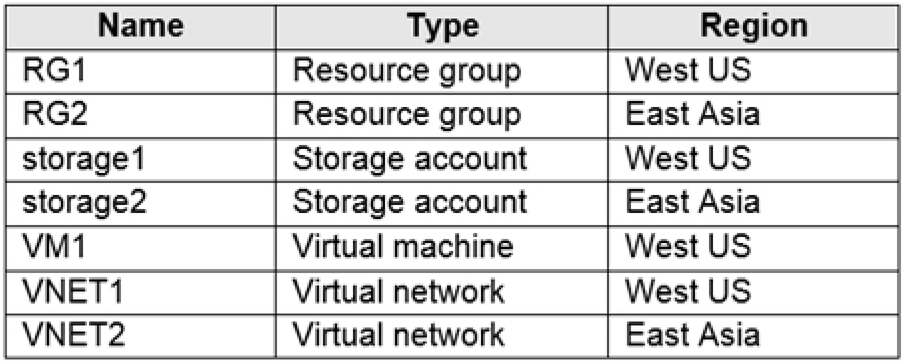
You can use either a CNAME record or an A record to map a custom DNS name to App Service.

You should use CNAME records for all custom DNS names except root domains (for example, contoso.com). For root domains, use A records.

Reference: https://docs.microsoft.com/en-us/Azure/app-service/app-service-web-tutorial-custom-domain

Question 129 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Region
RG1	Resource group	West US
RG2	Resource group	East Asia
storage1	Storage account	West US
storage2	Storage account	East Asia
VM1	Virtual machine	West US
VNET1	Virtual network	West US
VNET2	Virtual network	East Asia

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?

A. Yes

B. No

Explanation:

Correct Answer: B - No

Instead, you should delete VM1. Then recreate VM1 and add the network interface for VM1.

To migrate a VM from a VNET to another VNET. The only option is to delete the VM and redeploy it using a new NIC and NIC connected to VNET2.

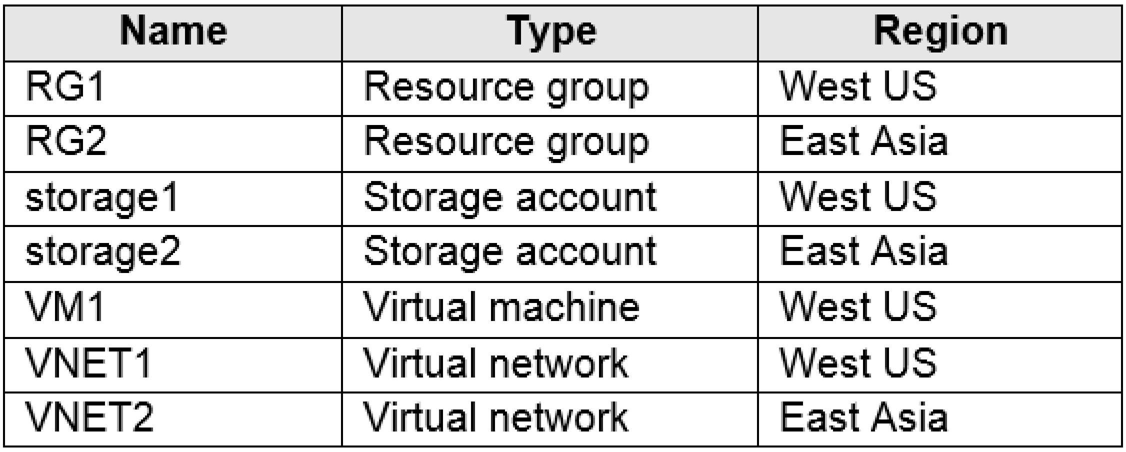
Note: When you create an Azure Virtual Machine (VM), you must create a Virtual Network (VNet) or use an existing VNet. You can change the subnet a VM is connected to after it's created, but you cannot change the VNet. You can also change the size of a VM.

Reference:

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

Question 130 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Region
RG1	Resource group	West US
RG2	Resource group	East Asia
storage1	Storage account	West US
storage2	Storage account	East Asia
VM1	Virtual machine	West US
VNET1	Virtual network	West US
VNET2	Virtual network	East Asia

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?

A. Yes

B. No

Explanation:

Correct Answer: A - Yes

You should delete VM1. Then recreate VM1 and add the network interface for VM1.

To migrate a VM from a VNET to another VNET. The only option is to delete the VM and redeploy it using a new NIC and NIC connected to VNET2.

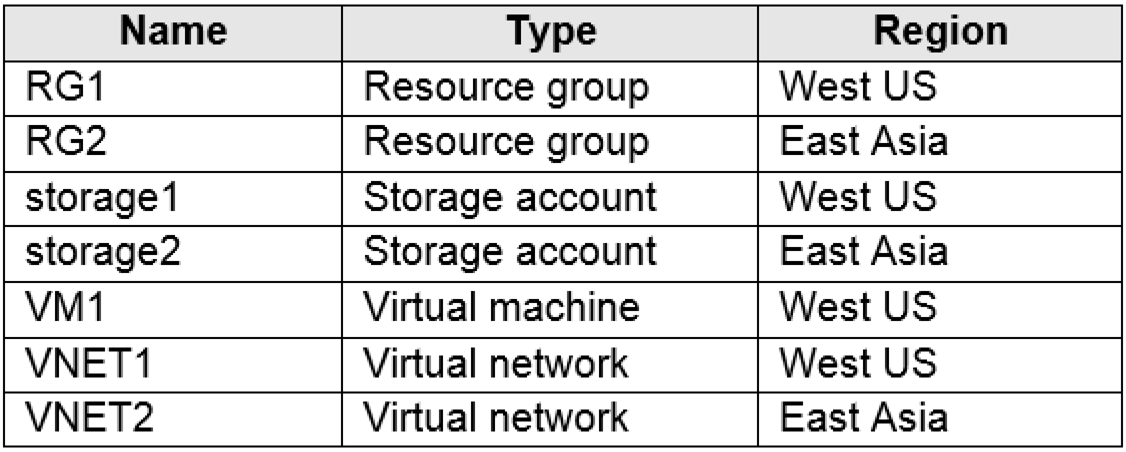
Note: When you create an Azure Virtual Machine (VM), you must create a Virtual Network (VNet) or use an existing VNet. You can change the subnet a VM is connected to after it's created, but you cannot change the VNet. You can also change the size of a VM.

Reference:

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

Question 131 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Region
RG1	Resource group	West US
RG2	Resource group	East Asia
storage1	Storage account	West US
storage2	Storage account	East Asia
VM1	Virtual machine	West US
VNET1	Virtual network	West US
VNET2	Virtual network	East Asia

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?

A. Yes

B. No

Explanation:

Correct Answer: B - No

Instead, you should delete VM1. Then recreate VM1 and add the network interface for VM1.

To migrate a VM from a VNET to another VNET. The only option is to delete the VM and redeploy it using a new NIC and NIC connected to VNET2.

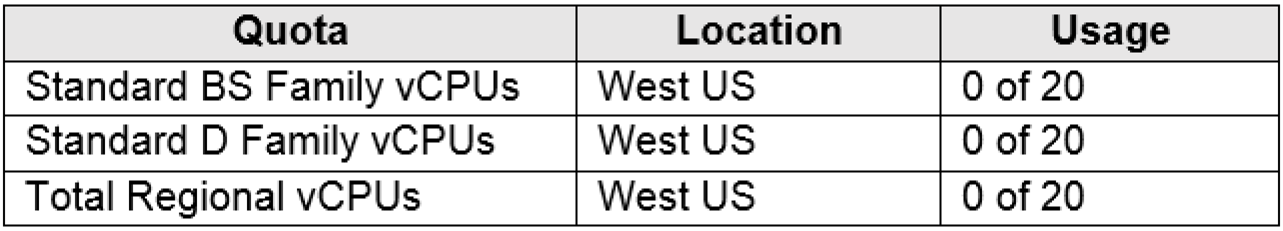
Note: When you create an Azure Virtual Machine (VM), you must create a Virtual Network (VNet) or use an existing VNet. You can change the subnet a VM is connected to after it's created, but you cannot change the VNet. You can also change the size of a VM.

Reference:

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

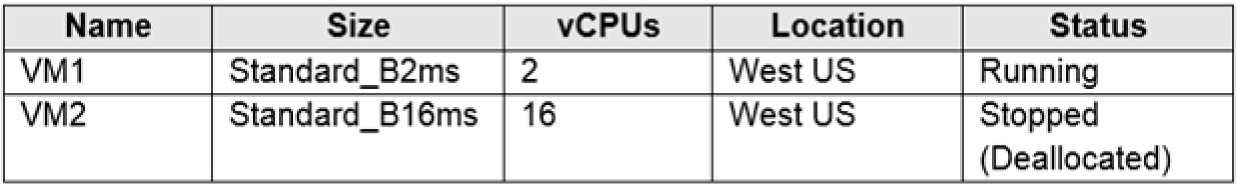
Question 132 CertyIQ

HOTSPOT -
You have an Azure subscription named Subscription1 that contains the quotas shown in the following table.



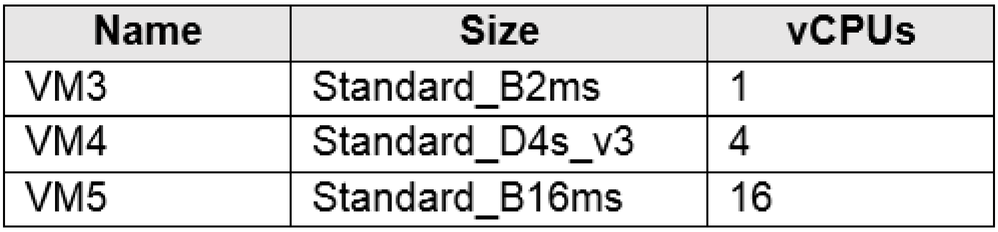
Quota	Location	Usage
Standard BS Family vCPUs	West US	0 of 20
Standard D Family vCPUs	West US	0 of 20
Total Regional vCPUs	West US	0 of 20

You deploy virtual machines to Subscription1 as shown in the following table.



Name	Size	vCPUs	Location	Status
VM1	Standard_B2ms	2	West US	Running
VM2	Standard_B16ms	16	West US	Stopped (Deallocated)

You plan to deploy the virtual machines shown in the following table.

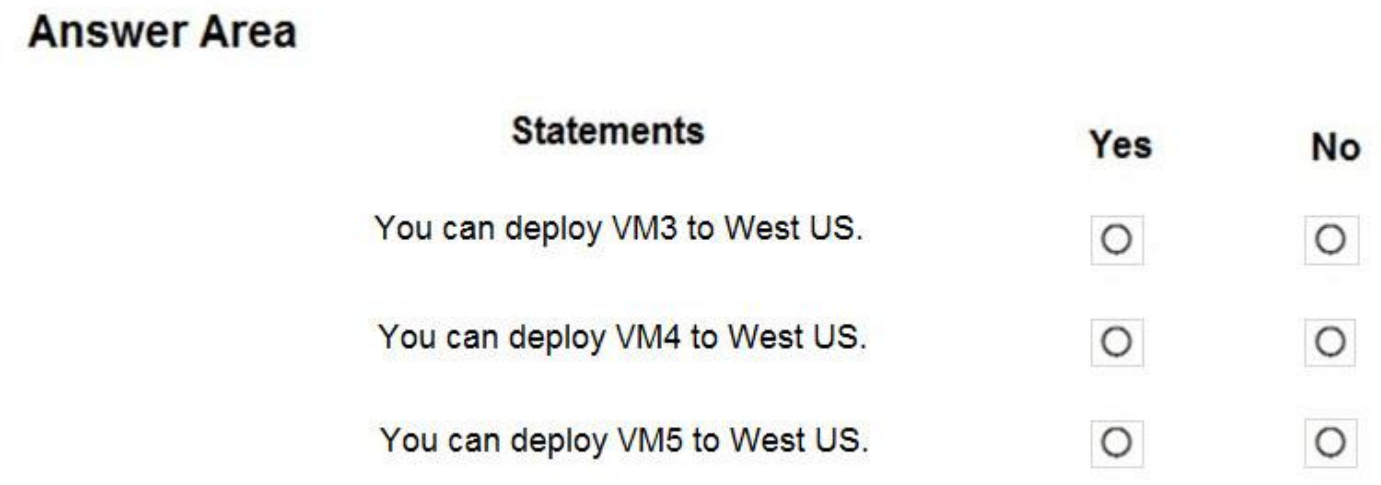


Name	Size	vCPUs
VM3	Standard_B2ms	1
VM4	Standard_D4s_v3	4
VM5	Standard_B16ms	16

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

NOTE: Each correct selection is worth one point.

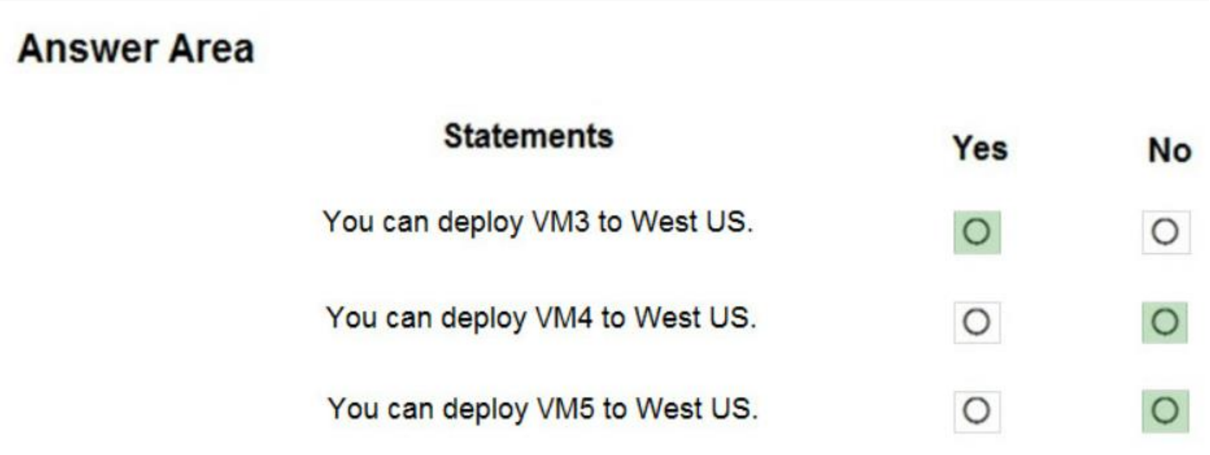
Hot Area:



Answer Area

Statements	Yes	No
You can deploy VM3 to West US.	○	○
You can deploy VM4 to West US.	○	○
You can deploy VM5 to West US.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
You can deploy VM3 to West US.	●	○
You can deploy VM4 to West US.	○	●
You can deploy VM5 to West US.	○	●

Explanation:

Correct Answer:

Total regional vCPUs = 20

2 vCPUs (VM1) + 16 vCPUs (VM20) = 18 vCPUs, which means that only 2 vCPUs left to exceed usage limit.

Box 1: Yes

We can add 1 vCPU. 2 vCPUs (VM1) + 16 vCPUs (VM20) + 1 vCPU (VM3) = 19 vCPUs

Box 2: No

We cannot add 4 vCPUs. 2 vCPUs (VM1) + 16 vCPUs (VM20) + 4 vCPU (VM4) = 22 vCPUs

Box 3: No

We cannot add 16 vCPU. 2 vCPUs (VM1) + 16 vCPUs (VM20) + 16 vCPU (VM5) = 34 vCPUs

Reference:

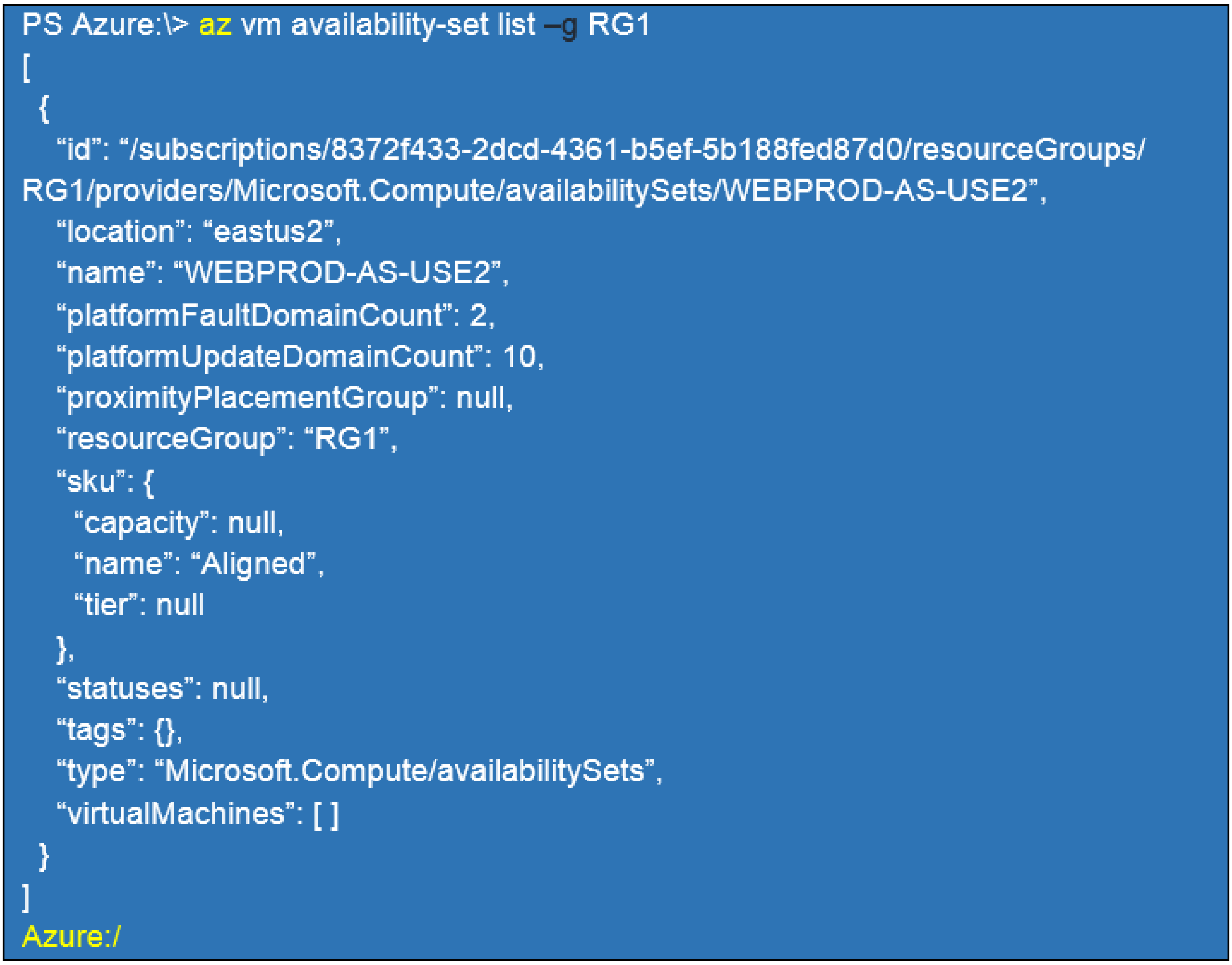
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quota

Question 133

CertyIQ

HOTSPOT -

You have an Azure subscription that contains an Azure Availability Set named WEBPROD-AS-USE2 as shown in the following exhibit.



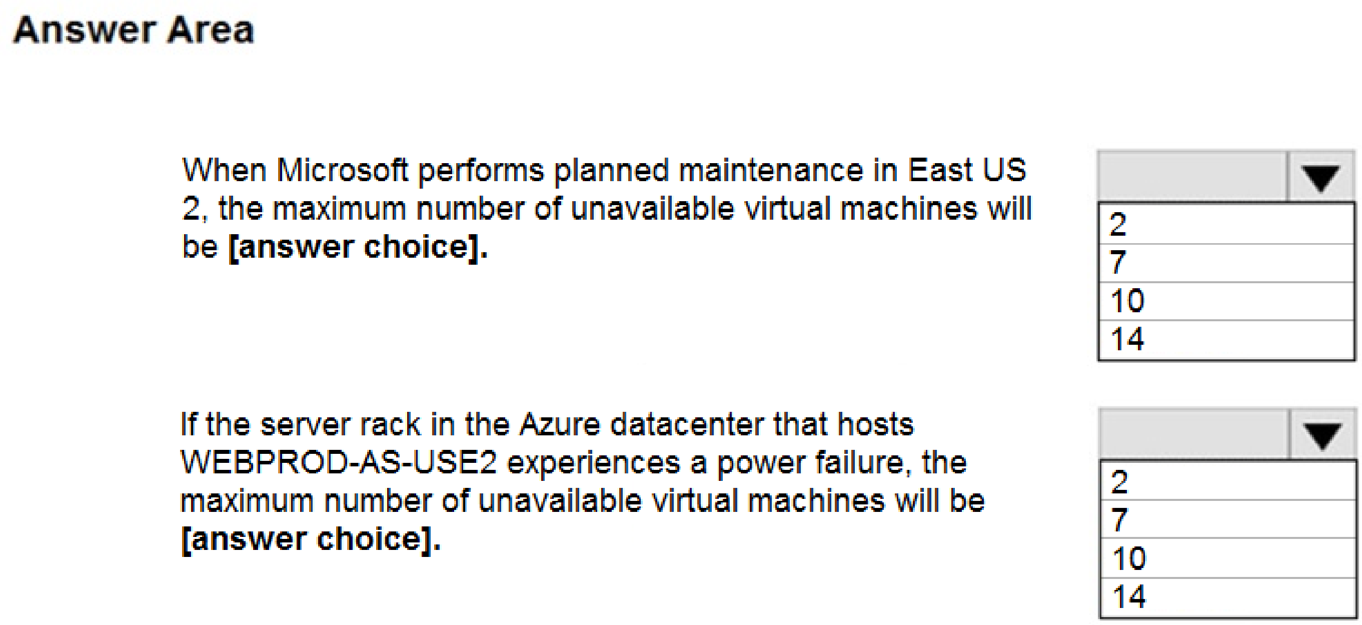
```
PS Azure:\> az vm availability-set list –g RG1
[
  {
    “id”: “/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/
RG1/providers/Microsoft.Compute/availabilitySets/WEBPROD-AS-USE2”,
    “location”: “eastus2”,
    “name”: “WEBPROD-AS-USE2”,
    “platformFaultDomainCount”: 2,
    “platformUpdateDomainCount”: 10,
    “proximityPlacementGroup”: null,
    “resourceGroup”: “RG1”,
    “sku”: {
      “capacity”: null,
      “name”: “Aligned”,
      “tier”: null
    },
    “statuses”: null,
    “tags”: {},
    “type”: “Microsoft.Compute/availabilitySets”,
    “virtualMachines”: [ ]
  }
]
Azure:/
```

You add 14 virtual machines to WEBPROD-AS-USE2.

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.

Hot Area:



Answer Area

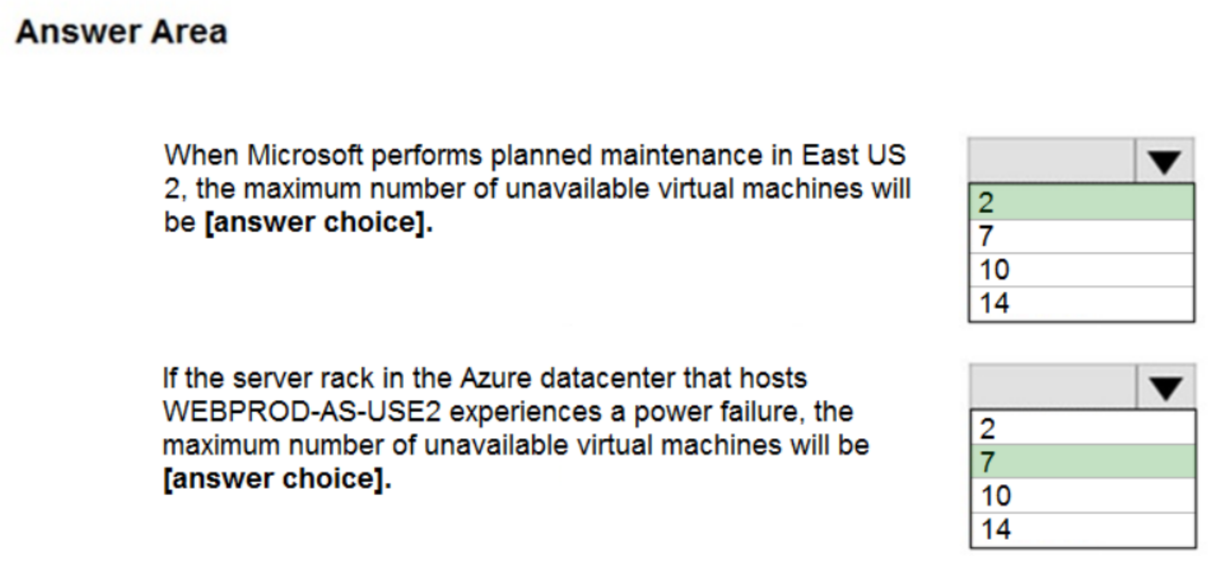
When Microsoft performs planned maintenance in East US 2, the maximum number of unavailable virtual machines will be **[answer choice].**

- 2
- 7
- 10
- 14

If the server rack in the Azure datacenter that hosts WEBPROD-AS-USE2 experiences a power failure, the maximum number of unavailable virtual machines will be **[answer choice].**

- 2
- 7
- 10
- 14

Correct Answer:



Answer Area

When Microsoft performs planned maintenance in East US 2, the maximum number of unavailable virtual machines will be **[answer choice].**

- [✓ 2]
- 7
- 10
- 14

If the server rack in the Azure datacenter that hosts WEBPROD-AS-USE2 experiences a power failure, the maximum number of unavailable virtual machines will be **[answer choice].**

- 2
- [✓ 7]
- 10
- 14

Explanation:

Correct Answer:

Box 1: 2

There are 10 update domains. The 14 VMs are shared across the 10 update domains, so 4 update domains will have 2 VMs and 6 update domains will have 1 VM. Only one update domain is rebooted at a time.
D1 D2 D3 D4 D5 D6 D7 D8 D9 D10
vm1 vm2 vm3 vm4 vm5 vm6 vm7 vm8 vm9 vm10
vm11 vm12 vm13 vm14
Maximum Down = 2
Minimum Down = 1

Box 2: 7

There are 2 fault domains. The 14 VMs are shared across the 2 fault domains, so 7 VMs in each fault domain. A rack failure will affect one fault domain so 7 VMs will be offline.
14 VM in 2 Fault Domain
Rack 1 Rack 2

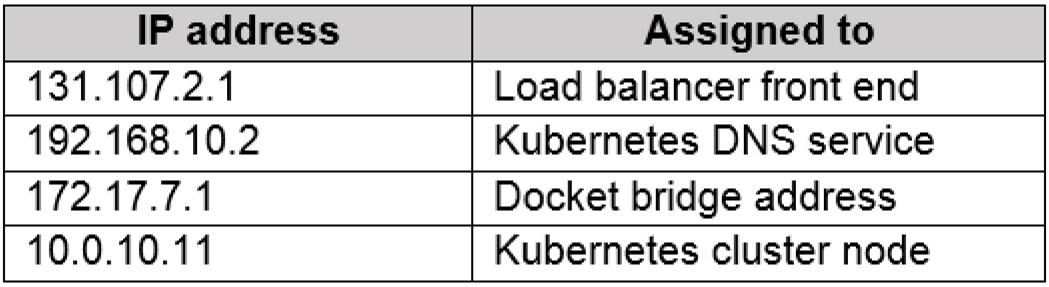
vm1 vm8
vm2 vm9
vm3 vm10
vm4 vm11
vm5 vm12
vm6 vm13
vm7 vm14
Maximum Down = 7
Minimum Down = 7

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

Question 134

CertyIQ

You deploy an Azure Kubernetes Service (AKS) cluster named Cluster1 that uses the IP addresses shown in the following table.



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

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

A. 131.107.2.1

B. 10.0.10.11

C. 172.17.7.1

D. 192.168.10.2

Explanation:

Correct Answer: A

To be able to access applications on Kubernetes, you need an application Load Balancer created by Azure which have public IP.

Note: 10.X.X.X range is private.

Reference:

https://docs.microsoft.com/en-us/azure/aks/load-balancer-standard

Question 135

CertyIQ

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?

A. five Azure Application Gateways

B. one App Service plan

C. 10 App Service plans

D. one Azure Traffic Manager

E. one Azure Application Gateway

Explanation:

Correct Answer: B

Creating one App Service Plan, you can support up to 10 Web Apps. Adding any of the other resources are pointless and not noted as a requirement.

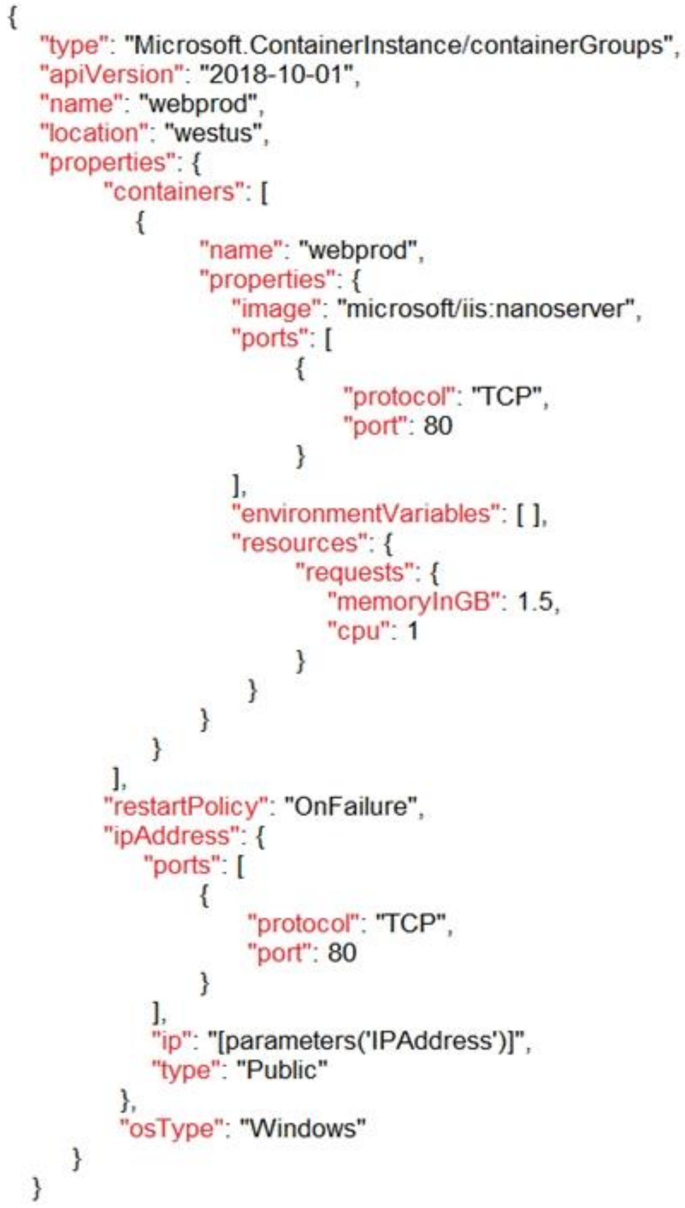
Reference:

https://docs.microsoft.com/en-us/azure/app-service/overview-hosting-plans

Question 136

CertyIQ

HOTSPOT -
You plan to deploy an Azure container instance by using the following Azure Resource Manager template.

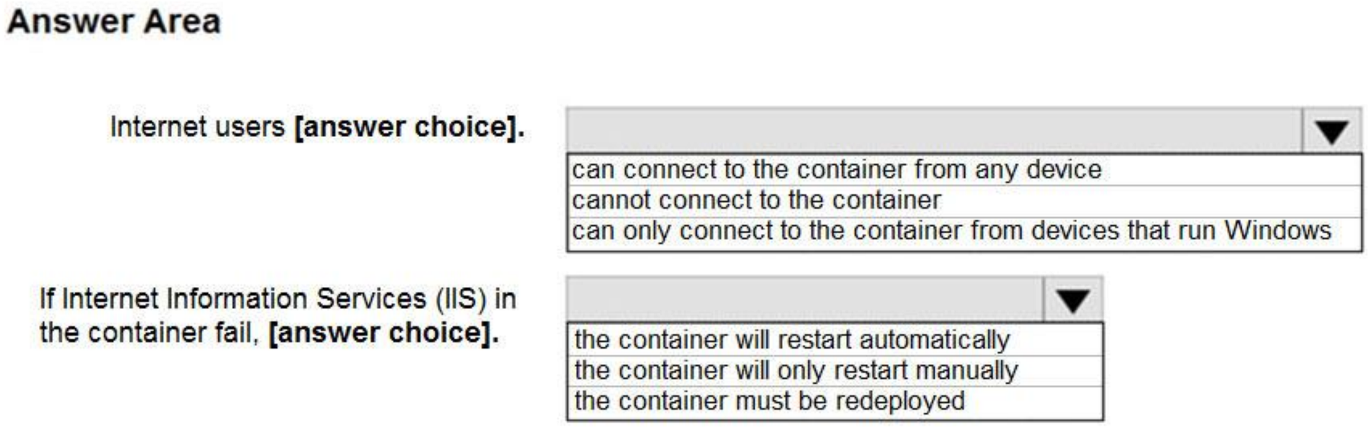


```
{
    "type": "Microsoft.ContainerInstance/containerGroups",
    "apiVersion": "2018-10-01",
    "name": "webprod",
    "location": "westus",
    "properties": {
          "containers": [
             {
                   "name": "webprod",
                   "properties": {
                      "image": "microsoft/iis:nanoserver",
                      "ports": [
                            {
                                  "protocol": "TCP",
                                  "port": 80
                            }
                      ],
                      "environmentVariables": [ ],
                      "resources": {
                            "requests": {
                               "memoryInGB": 1.5,
                               "cpu": 1
                            }
                      }
                   }
             }
          ],
          "restartPolicy": "OnFailure",
          "ipAddress": {
              "ports": [
                   {
                         "protocol": "TCP",
                         "port": 80
                   }
              ],
              "ip": "[parameters('IPAddress')]",
              "type": "Public"
          },
          "osType": "Windows"
     }
 }
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the template.

NOTE: Each correct selection is worth one point.

Hot Area:



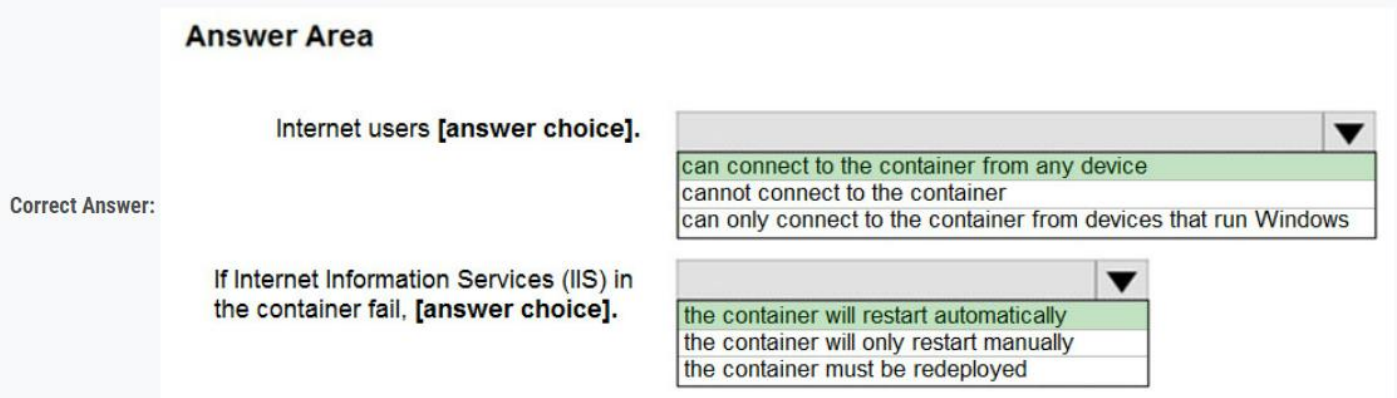
Answer Area

Internet users **[answer choice].**

- can connect to the container from any device
- cannot connect to the container
- can only connect to the container from devices that run Windows

If Internet Information Services (IIS) in the container fail, **[answer choice].**

- the container will restart automatically
- the container will only restart manually
- the container must be redeployed


Correct Answer:

Answer Area

Internet users **[answer choice].**

- [✓ can connect to the container from any device]
- cannot connect to the container
- can only connect to the container from devices that run Windows

If Internet Information Services (IIS) in the container fail, **[answer choice].**

- [✓ the container will restart automatically]
- the container will only restart manually
- the container must be redeployed

Explanation:

- Can connect from any dev.
- Will restart automatically.

```
"port": {
"type": "int",
"defaultValue": 80,
"metadata": {
"description": "Port to open on the container and the public IP address."
}
"restartPolicy": {
"type": "string",
"defaultValue": "Always",
"allowedValues": [
"Always",
"Never",
"OnFailure"
```

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-quickstart-template

Question 137 CertyIQ

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?

A. Enable Desired State Configuration Management

B. Add a 500-GB managed disk

C. Change the size to D8s v3

D. Add the Puppet Agent extension

Explanation:

Correct Answer: C

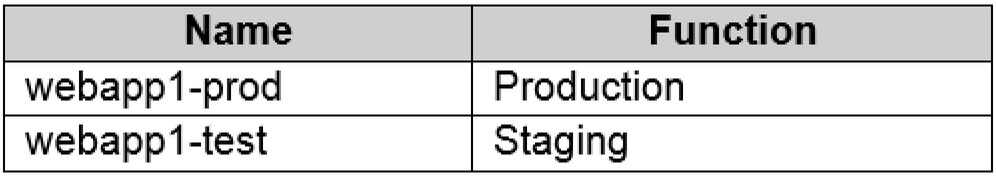
While resizing, the VM must be in a stopped state, therefore there will be a downtime.

Reference:

https://azure.microsoft.com/en-us/blog/resize-virtual-machines

Question 138 CertyIQ

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.



Name	Function
webapp1-prod	Production
webapp1-test	Staging

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

A. Swap the slots

B. Deploy the App1 update to webapp1-prod, and then test the update

C. Stop webapp1-prod

D. Deploy the App1 update to webapp1-test, and then test the update

E. Stop webapp1-test

Explanation:

1.Deploy the App to “webapp1-test” which is staging environment and test it there.

2.Once the test is success swap the slots, so the new changes will be available under production.

Question 139 CertyIQ

You have an Azure subscription named Subscription1 that has the following providers registered:

- Authorization
- Automation
- Resources
- Compute
- KeyVault
- Network

⊶ Storage
⊶ Billing
⊶ 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? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Enable Azure Network Watcher in the East US Azure region.

B. Add an Azure Network Watcher connection monitor.

C. Register the MicrosoftLogAnalytics provider.

D. Create an Azure Storage account.

E. Register the Microsoft.Insights resource provider.

F. Enable Azure Network Watcher flow logs.

Explanation:

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

When you create or update a virtual network in your subscription, Network Watcher will be enabled automatically in your Virtual Network's region. There is no impact to your resources or associated charge for automatically enabling Network Watcher. For more information, see Network Watcher create.

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal

Create a VM with a network security group

Enable Network Watcher (done by default with the vnet/subnet creation)

-- and register the Microsoft.Insights provider ---------todo

Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability --todo BUT !

NSG flow log data is written to an Azure Storage account. Complete the following steps to create a storage account for the log data.

So you need to create a storage account before enable the NSG flow

Download logged data

View logged data

Question 140

CertyIQ

You need to deploy an Azure virtual machine scale set that contains five instances as quickly as possible. What should you do?

A. Deploy five virtual machines. Modify the Availability Zones settings for each virtual machine.

B. Deploy five virtual machines. Modify the Size setting for each virtual machine.

C. Deploy one virtual machine scale set that is set to VM (virtual machines) orchestration mode.

D. Deploy one virtual machine scale set that is set to ScaleSetVM orchestration mode.

Explanation:

Correct Answer: D

ScaleSetVM orchestration mode: 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. It the current default VMSS behavior. (Scale set VMs are created in a single shot).

VM (virtual machines) orchestration mode: Virtual machines created outside of the scale set can be explicitly added to the scale set. The orchestration mode VM will only create an empty VMSS without any instances, and you will have to manually add new VMs into it by specifying the VMSS ID during the creation of the VM. (Separately VMs are created and added to scale set later)

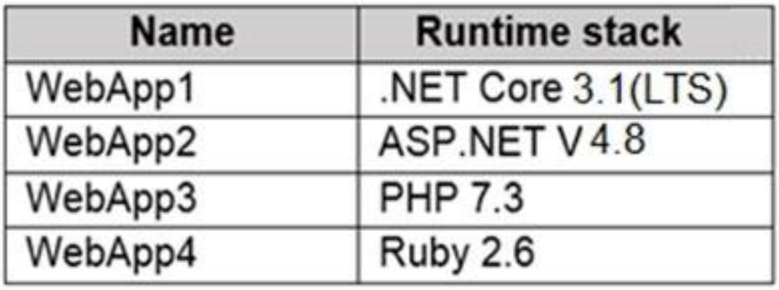
Reference:

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/orchestration-modes

Question 141

CertyIQ

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



Name	Runtime stack
WebApp1	.NET Core 3.1(LTS)
WebApp2	ASP.NET V 4.8
WebApp3	PHP 7.3
WebApp4	Ruby 2.6

What is the minimum number of App Service plans you should create for the web apps?

A. 1

B. 2

C. 3

D. 4

Explanation:

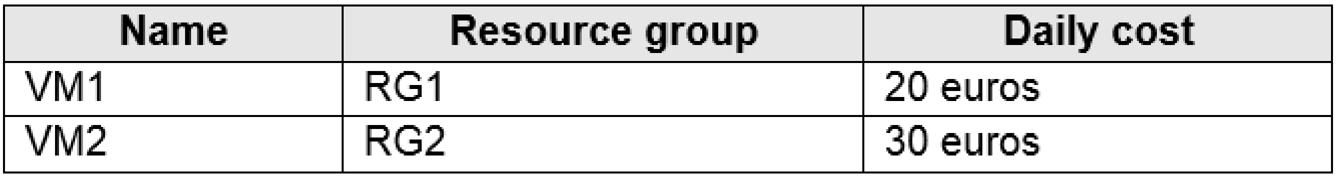
Correct Answer is B

ASP.Net - Win ONLY
Ruby - Linux ONLY
So need a minimum of 2 ASPs

NET Core 3.0: Windows and Linux ASP
.NET V4.7: Windows only
PHP 7.3: Windows and Linux
Ruby 2.6: Linux only
Also, you can’t use Windows and Linux Apps in the same App Service Plan, because when you create a new App Service plan you have to choose the OS type. You can't mix Windows and Linux apps in the same App Service plan. So, you need 2 ASPs.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview

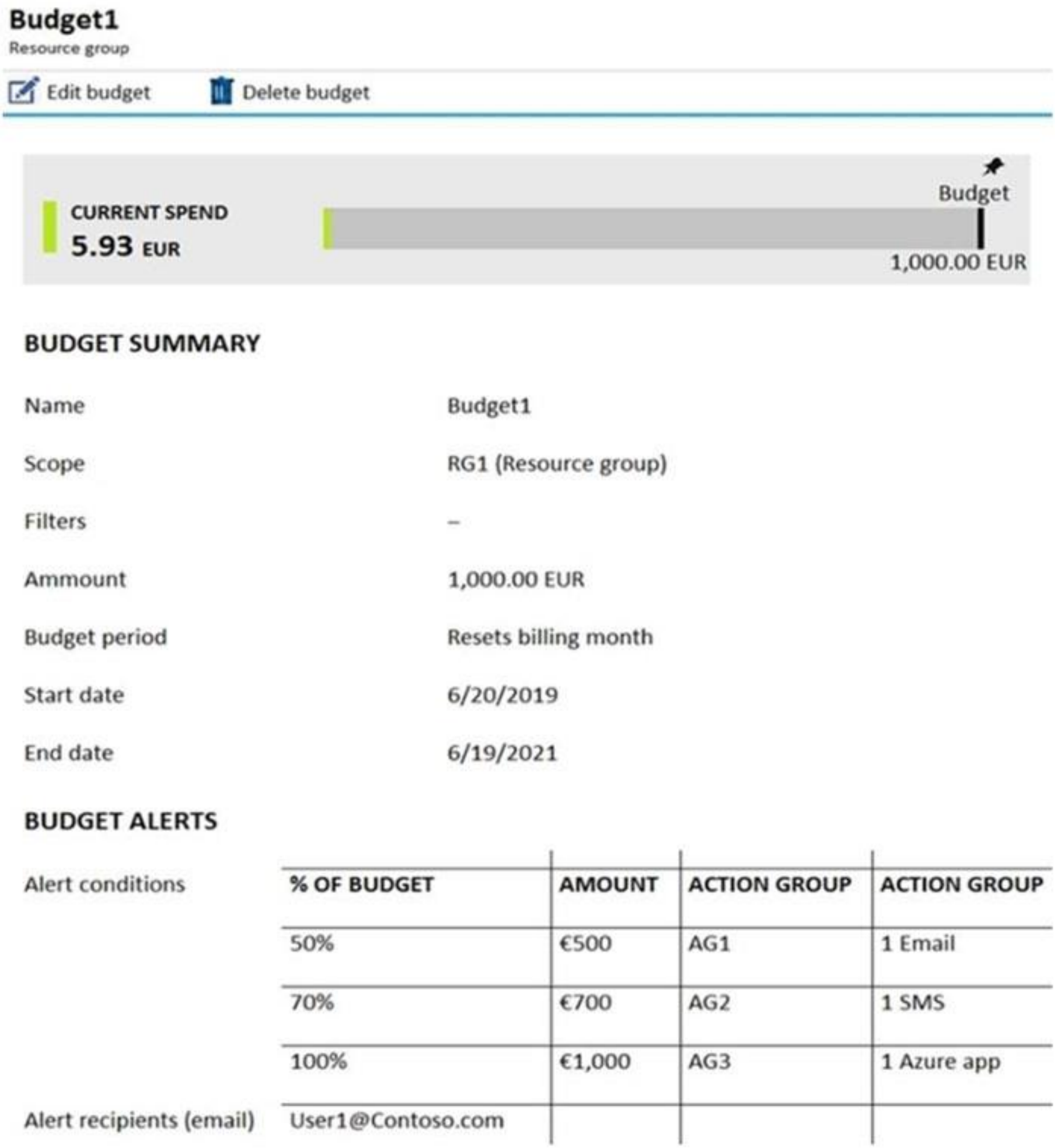
Question 142 CertyIQ

HOTSPOT -
You have a pay-as-you-go Azure subscription that contains the virtual machines shown in the following table.



Name	Resource group	Daily cost
VM1	RG1	20 euros
VM2	RG2	30 euros

You create the budget shown in the following exhibit.



Budget1

Resource group

CURRENT SPEND
5.93 EUR

1,000.00 EUR

BUDGET SUMMARY

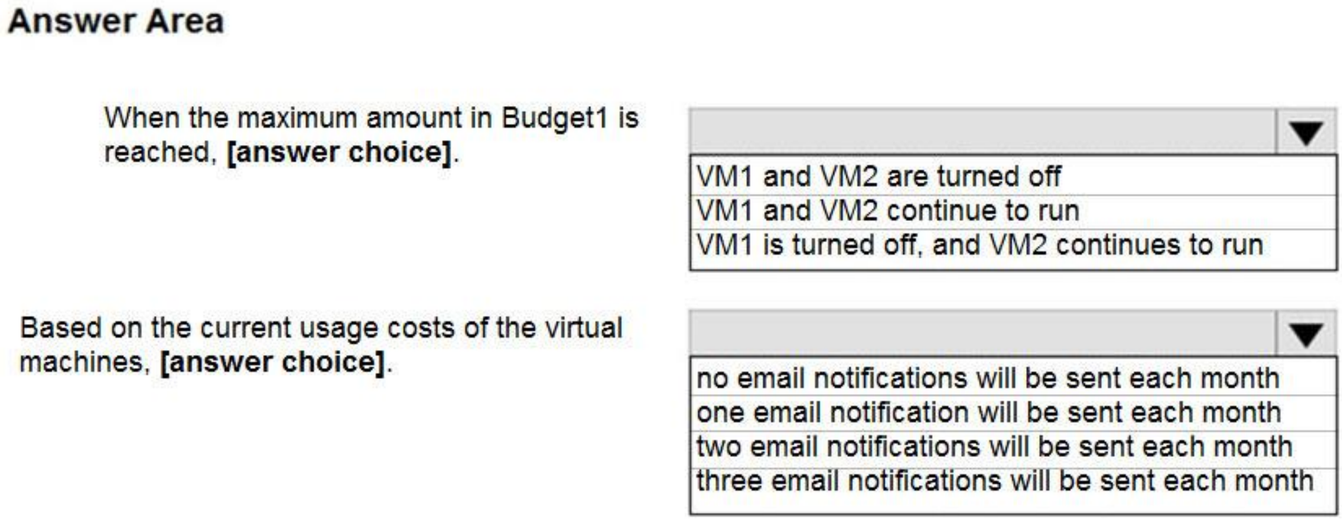
Name	Budget1
Scope	RG1 (Resource group)
Filters	–
Ammount	1,000.00 EUR
Budget period	Resets billing month
Start date	6/20/2019
End date	6/19/2021

BUDGET ALERTS

Alert conditions	% OF BUDGET	AMOUNT	ACTION GROUP	ACTION GROUP
	50%	€500	AG1	1 Email
	70%	€700	AG2	1 SMS
	100%	€1,000	AG3	1 Azure app
Alert recipients (email)	User1@Contoso.com			

The AG1 action group contains a user named admin@contoso.com only.
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

Hot Area:



Answer Area

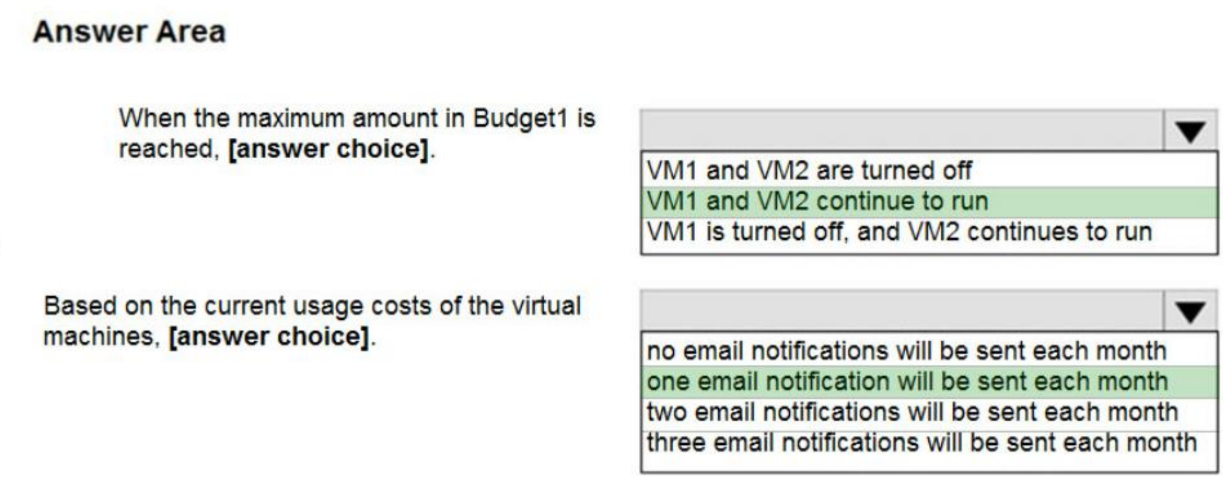
When the maximum amount in Budget1 is reached, **[answer choice]**.

- VM1 and VM2 are turned off
- VM1 and VM2 continue to run
- VM1 is turned off, and VM2 continues to run

Based on the current usage costs of the virtual machines, **[answer choice]**.

- no email notifications will be sent each month
- one email notification will be sent each month
- two email notifications will be sent each month
- three email notifications will be sent each month

Correct Answer:



Answer Area

When the maximum amount in Budget1 is reached, **[answer choice]**.

- VM1 and VM2 are turned off
- [✓ VM1 and VM2 continue to run]
- VM1 is turned off, and VM2 continues to run

Based on the current usage costs of the virtual machines, **[answer choice]**.

- no email notifications will be sent each month
- [✓ one email notification will be sent each month]
- two email notifications will be sent each month
- three email notifications will be sent each month

Explanation:

Correct Answer:

Box 1: VM1 and VM2 continue to run

The Budget’s scope is RG1, so only VM1 will be handled.

When the budget thresholds you've created are exceeded, only notifications are triggered.

To stop resources, you need to setup additional things, none of which are mentioned in the question.

Box 2: one email notification will be sent each month.

Budget alerts have scope in Resource Group RG1, which includes VM1, but not VM2.

VM1 consumes 20 Euro/day, so 20 euros * 30 days = 600 euros.

The 50%, 500 Euro limit, will be reached in 25 days (25*20 = 500), so an email will be sent.

The 70% and 100% alert conditions will not be reached within a month, and they don't trigger email actions anyway, because AG1 action group contains a user.

Credit alerts: Credit alerts are generated automatically at 90% and at 100% of your Azure credit balance. Whenever an alert is generated, it's reflected in cost alerts and in the email sent to the account owners. 90% and 100% will not be reached though.

Reference:
https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/cost-mgt-alerts-monitor-usage-spending
https://docs.microsoft.com/en-gb/azure/cost-management-billing/costs/tutorial-acm-create-budgets

Question 143 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates.
You need to view the date and time when the resources were created in RG1.
Solution: From the Subscriptions blade, you select the subscription, and then click Programmatic deployment.
Does this meet the goal?

A. Yes

B. No

Explanation:

Correct Answer: B - No

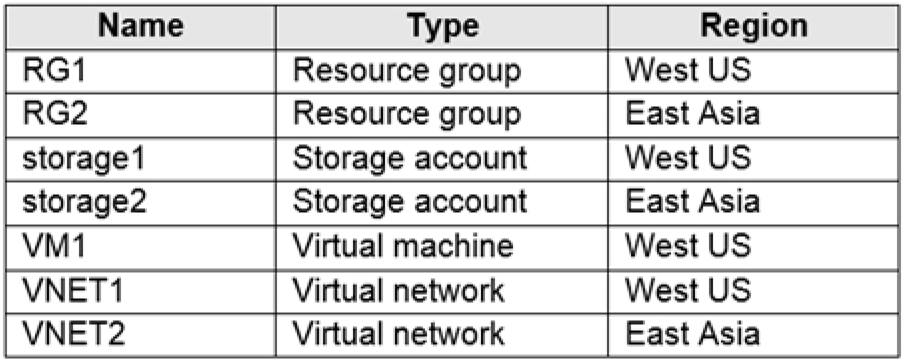
From the RG1 blade, click Deployments. You see a history of deployment for the resource group.

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial-create-first-template?tabs=azure-powershell

Question 144 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Region
RG1	Resource group	West US
RG2	Resource group	East Asia
storage1	Storage account	West US
storage2	Storage account	East Asia
VM1	Virtual machine	West US
VNET1	Virtual network	West US
VNET2	Virtual network	East Asia

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?

A. Yes

B. No

Explanation:

Correct Answer: B - No

Instead, you should delete VM1. Then recreate VM1 and add the network interface for VM1.

To migrate a VM from a VNET to another VNET. The only option is to delete the VM and redeploy it using a new NIC and NIC connected to VNET2.

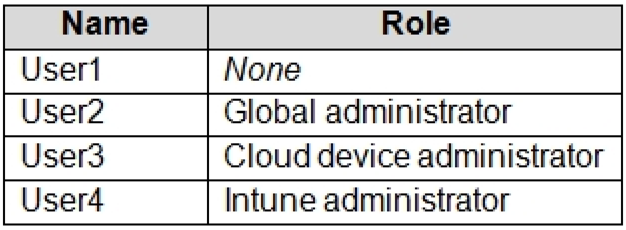
Note: When you create an Azure Virtual Machine (VM), you must create a Virtual Network (VNet) or use an existing VNet. You can change the subnet a VM is connected to after it's created, but you cannot change the VNet. You can also change the size of a VM.

Reference:

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

Question 145 CertyIQ

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



Name	Role
User1	*None*
User2	Global administrator
User3	Cloud device administrator
User4	Intune administrator

Adatum.com has the following configurations:
✑ Users may join devices to Azure AD is set to User1.
✑ Additional local administrators on Azure AD joined devices is set to None.
You deploy Windows 10 to a computer named Computer1. User1 joins Computer1 to adatum.com.
You need to identify the local Administrator group membership on Computer1.
Which users are members of the local Administrators group?

A. User1 only

B. User2 only

C. User1 and User2 only

D. User1, User2, and User3 only

E. User1, User2, User3, and User4

Explanation:

Correct Answer: *C*

User 1 and User 2 only.

First the only user who can join Azure AD devices is User 1 . since User1 is admin on machine. So, the machine can be added.

Second, the ones that can be local admins on Windows 10 are managed under "Additional local administrators" , since this is not mentioned, so we can assume default.

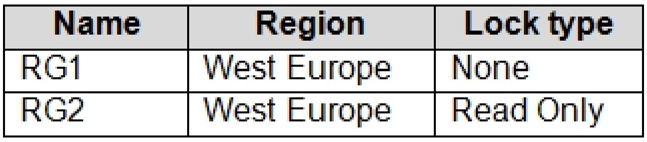
By default, the ones are global administrator and device owners (device administrators). This lead us to User1 and User2 only

Users may join devices to Azure AD - This setting enables you to select the users who can register their devices as Azure AD joined devices. The default is All.
Additional local administrators on Azure AD joined devices - You can select the users that are granted local administrator rights on a device. Users added here are added to the Device Administrators role in Azure AD. Global administrators, here User2, in Azure AD and device owners are granted local administrator rights by default.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

Question 146

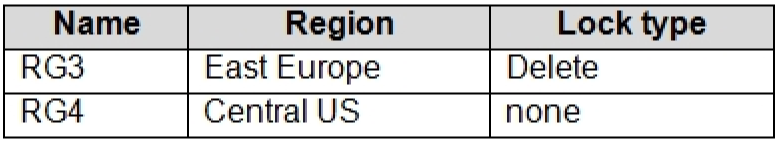
CertyIQ

HOTSPOT -
You have Azure subscriptions named Subscription1 and Subscription2.
Subscription1 has following resource groups:



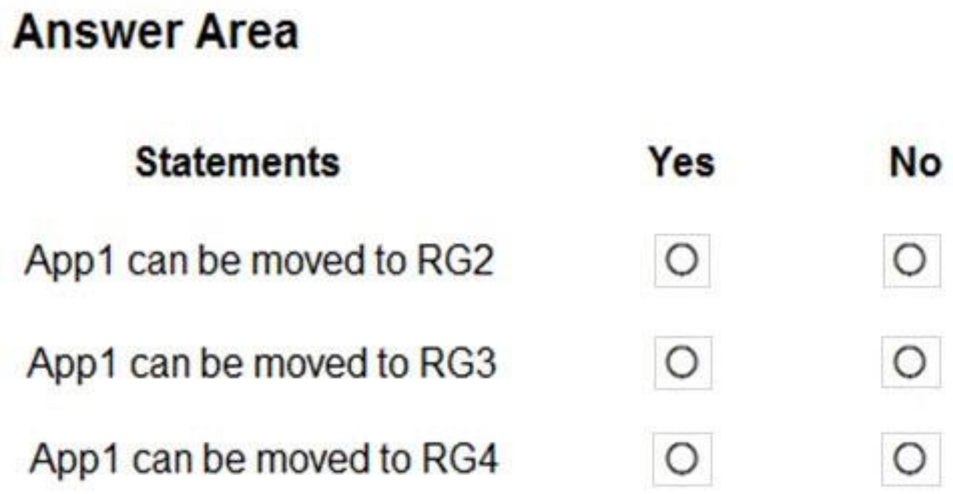
Name	Region	Lock type
RG1	West Europe	None
RG2	West Europe	Read Only

RG1 includes a web app named App1 in the West Europe location.
Subscription2 contains the following resource groups:



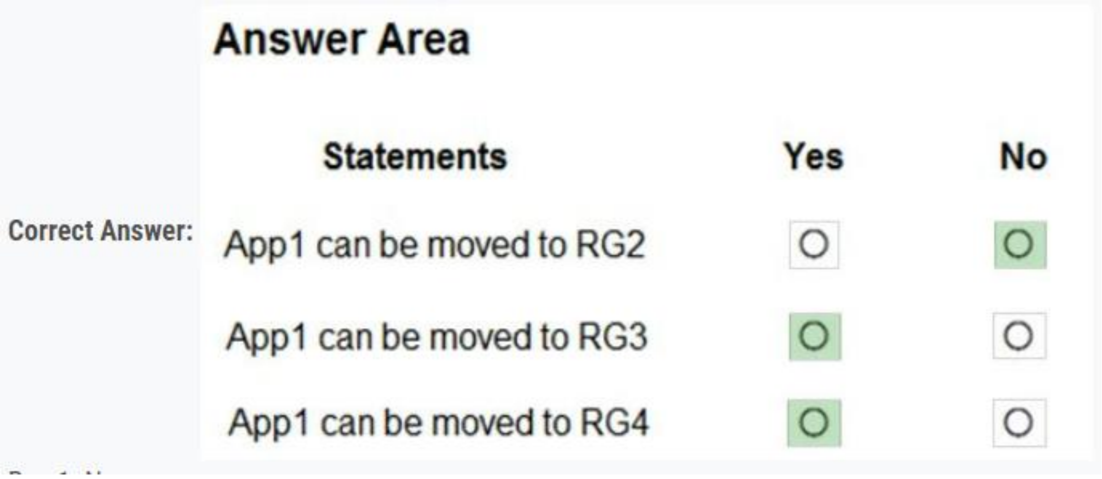
Name	Region	Lock type
RG3	East Europe	Delete
RG4	Central US	none

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



Answer Area

Statements	Yes	No
App1 can be moved to RG2	○	○
App1 can be moved to RG3	○	○
App1 can be moved to RG4	○	○



Correct Answer:

Answer Area

Statements	Yes	No
App1 can be moved to RG2	○	[✓ ○]
App1 can be moved to RG3	[✓ ○]	○
App1 can be moved to RG4	[✓ ○]	○

Explanation:

Box 1: No -
RG2 is read only. ReadOnly means authorized users can read a resource, but they cannot delete or update the resource.
The first question was tested on Azure.

Created RG1, RG2. both are in West Europe. RG2 has assigned READ-ONLY lock.

Created web-App name App11223344 (same location as RG1,RG2) in RG1.

Removing App11223344 to RG2 failed.

{"code":"ResourceMovePolicyValidationFailed","message":"Resource move policy validation failed. Please see details. Diagnostic information: request correlation id 'fd5981c2-705b-4966-b438-cd760bd1a13f'.","details":[{"code":"ResourceMovePolicyValidationFailed","target":"Microsoft.Web/Microsoft.Web/sites/App11223344","message":"{\"error\":{\"code\":\"ScopeLocked\",\"message\":\"The scope '/subscriptions/2df00a78-a9c5-4c98-92ef-aa1fbbb50e6f/resourcegroups/RG2/providers/Microsoft.Web/sites/App11223344' cannot perform write operation because following scope(s) are locked: '/subscriptions/2df00a78-a9c5-4c98-92ef-aa1fbbb50e6f/resourceGroups/RG2'. Please remove the lock and try again.\"}}"}]}

Box 2: Yes -

Box 3: Yes -
Note:
App Service resources are region-specific and cannot be moved directly across regions. You can move the App Service resource by creating a copy of your existing App Service resource in the target region, then move your content over to the new app. You can then delete the source app and App Service plan.
To make copying your app easier, you can clone an individual App Service app into an App Service plan in another region.
Reference:
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

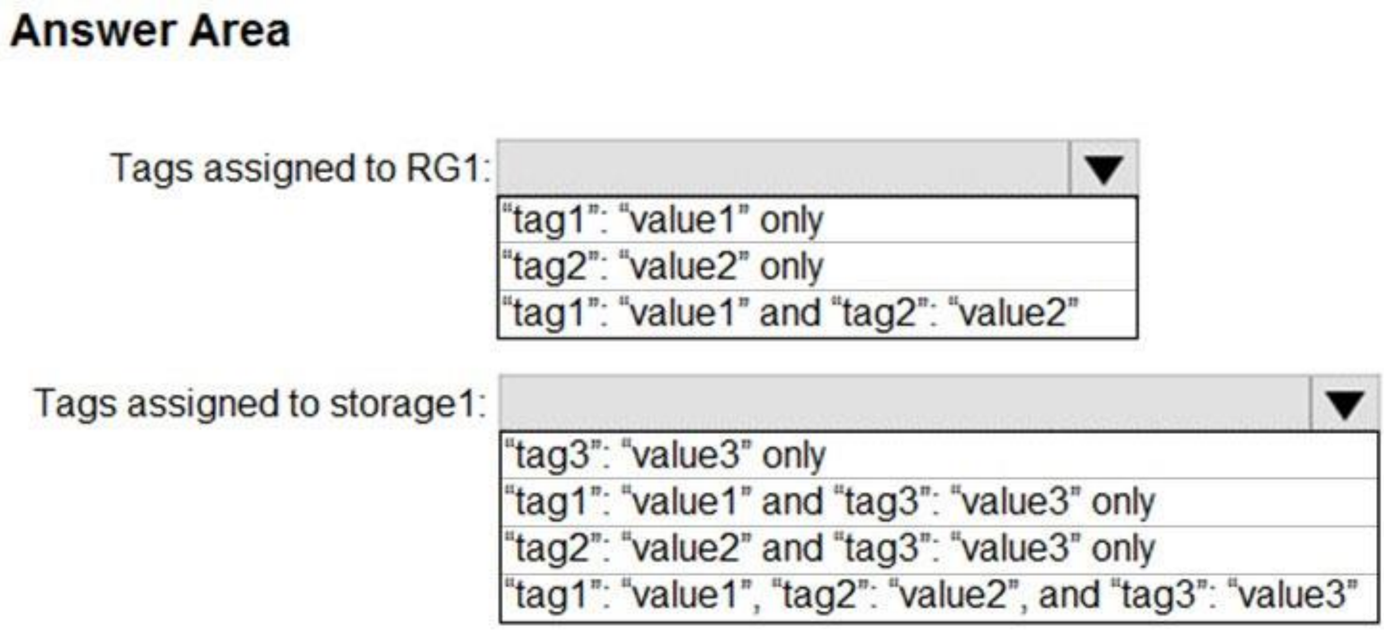
Question 147 CertyIQ

HOTSPOT -
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? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

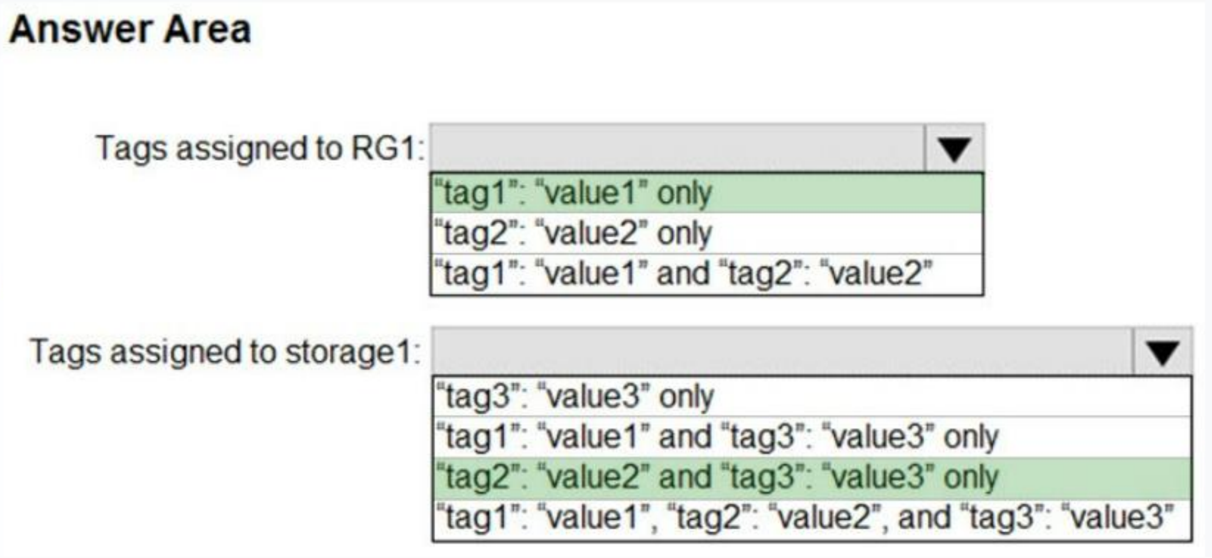


Answer Area

Tags assigned to RG1:
“tag1”: “value1” only
“tag2”: “value2” only
“tag1”: “value1” and “tag2”: “value2”

Tags assigned to storage1:
“tag3”: “value3” only
“tag1”: “value1” and “tag3”: “value3” only
“tag2”: “value2” and “tag3”: “value3” only
“tag1”: “value1”, “tag2”: “value2”, and “tag3”: “value3”

Correct Answer:



Answer Area

Tags assigned to RG1:
“tag1”: “value1” only
“tag2”: “value2” only
“tag1”: “value1” and “tag2”: “value2”

Tags assigned to storage1:
“tag3”: “value3” only
“tag1”: “value1” and “tag3”: “value3” only
“tag2”: “value2” and “tag3”: “value3” only
“tag1”: “value1”, “tag2”: “value2”, and “tag3”: “value3”

Explanation:

Tag assigned to RG1 - tag1: value1

Tag assigned to storage1: tag2: value2 and tag3: value3

RG1 already exists so does not receive tag2.

According to the documentation:

"Add a tag to resources"

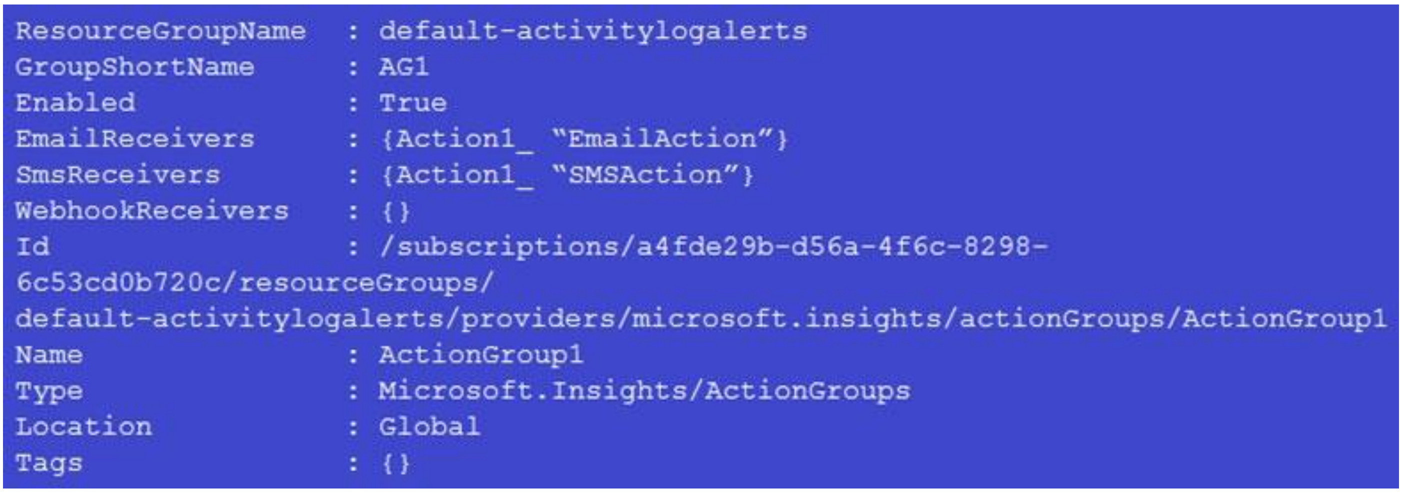
Adds the specified tag and value when any resource missing this tag is created or updated. Existing resources can be remediated by triggering a remediation task. If the tag exists with a different value it will not be changed. Does not modify tags on resource groups.

Tags applied to the resource group are not inherited by the resources in that resource group.
Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

Question 148

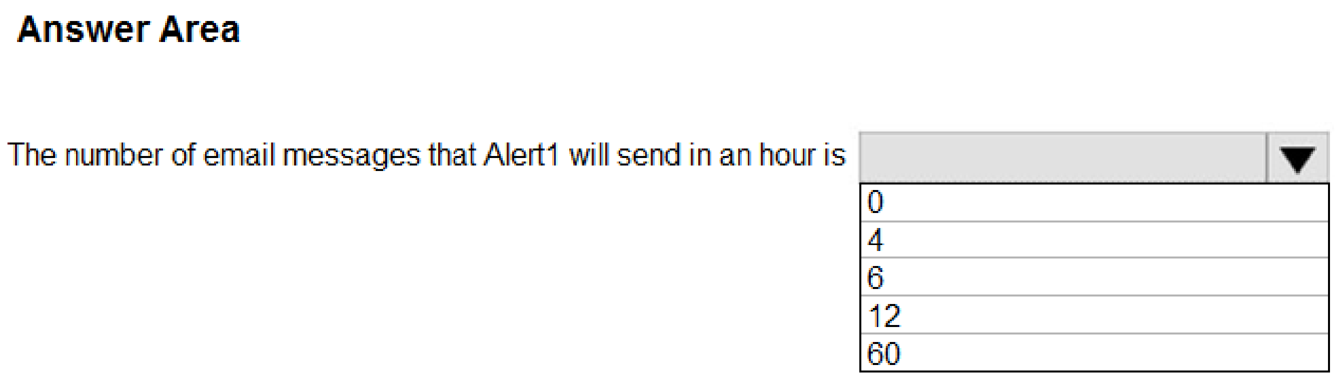
CertyIQ

HOTSPOT -
You have an Azure subscription named Subscription1.
In Subscription1, you create an alert rule named Alert1.
The Alert1 action group is configured as shown in the following exhibit.



```
ResourceGroupName    : default-activitylogalerts
GroupShortName       : AG1
Enabled              : True
EmailReceivers       : {Action1_ “EmailAction”}
SmsReceivers         : {Action1_ “SMSAction”}
WebhookReceivers     : {}
Id                   : /subscriptions/a4fde29b-d56a-4f6c-8298-
6c53cd0b720c/resourceGroups/
default-activitylogalerts/providers/microsoft.insights/actionGroups/ActionGroup1
Name                 : ActionGroup1
Type                 : Microsoft.Insights/ActionGroups
Location             : Global
Tags                 : {}
```

Alert1 alert criteria triggered every minute.
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.
Hot Area:



Answer Area

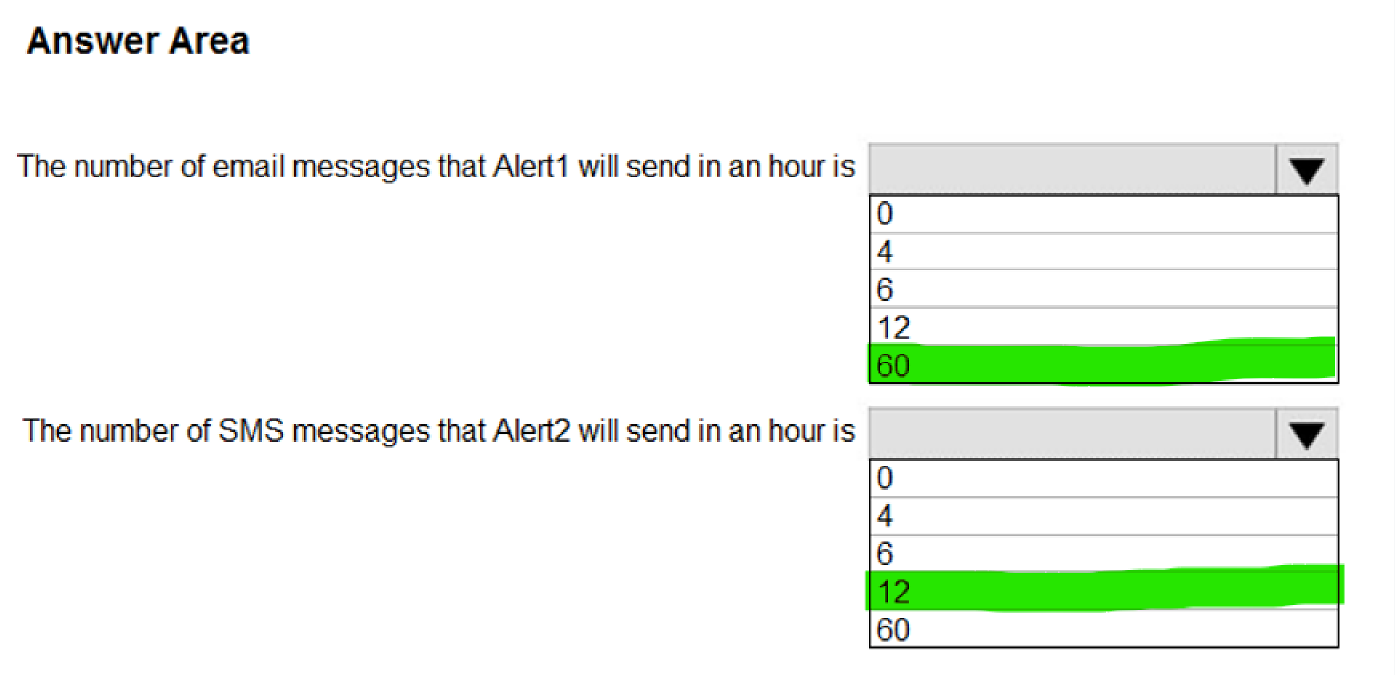
The number of email messages that Alert1 will send in an hour is ▼

0
4
6
12
60

The number of SMS messages that Alert2 will send in an hour is ▼

0
4
6
12
60

Correct Answer: -



Answer Area

The number of email messages that Alert1 will send in an hour is ▼

0
4
6
12
[✓ 60]

The number of SMS messages that Alert2 will send in an hour is ▼

0
4
6
[✓ 12]
60

Explanation:

Correct Answer:

Box 1: 60

One alert per minute will trigger one email per minute.

Box 2: 12

-If it's a typo and it means Alert1, then Answer = 12 (60/5 = 12)

-If it is actually Alert2 then Answer = 0

No more than 1 SMS every 5 minutes can be send, which equals 12 per hour (60/5 = 12).

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.

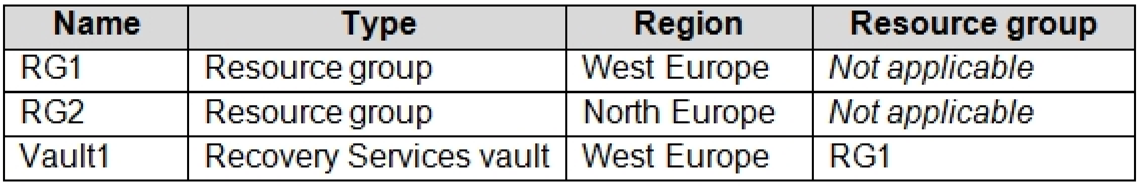
✑ Other actions are not rate limited.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-rate-limiting

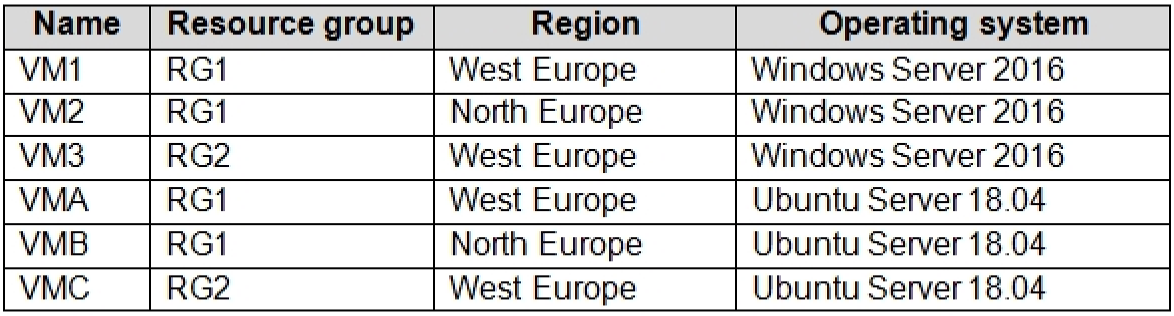
Question 149 CertyIQ

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



Name	Type	Region	Resource group
RG1	Resource group	West Europe	*Not applicable*
RG2	Resource group	North Europe	*Not applicable*
Vault1	Recovery Services vault	West Europe	RG1

You create virtual machines in Subscription1 as shown in the following table.



Name	Resource group	Region	Operating system
VM1	RG1	West Europe	Windows Server 2016
VM2	RG1	North Europe	Windows Server 2016
VM3	RG2	West Europe	Windows Server 2016
VMA	RG1	West Europe	Ubuntu Server 18.04
VMB	RG1	North Europe	Ubuntu Server 18.04
VMC	RG2	West Europe	Ubuntu Server 18.04

You plan to use Vault1 for the backup of as many virtual machines as possible.
Which virtual machines can be backed up to Vault1?

A. VM1 only

B. VM3 and VMC only

C. VM1, VM2, VM3, VMA, VMB, and VMC

D. VM1, VM3, VMA, and VMC only

E. VM1 and VM3 only

Explanation:

Correct Answer: D

To create a Recovery Services 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. It works with any resource group or any Operating System.

Reference:

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

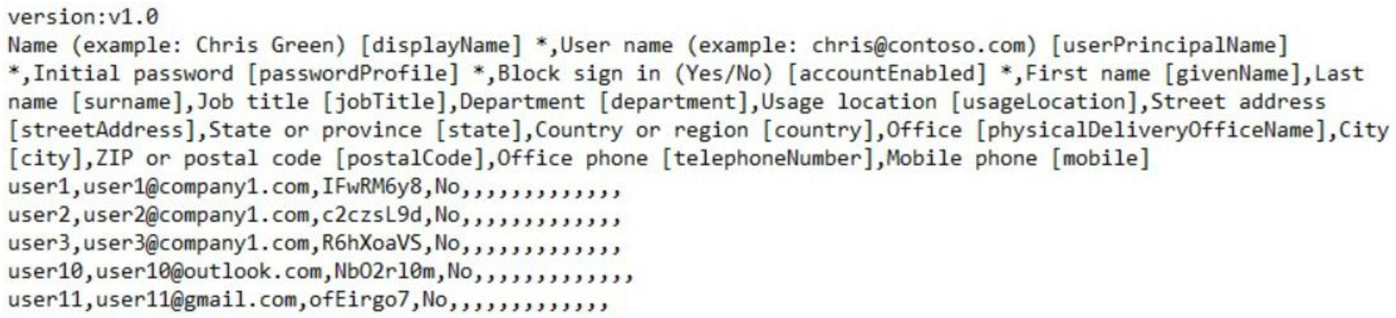
https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-vms-prepare

Question 150

CertyIQ

Your company has an Azure Active Directory (Azure AD) tenant named company1.com.

You want to create multiple users. You decide to use the bulk create feature in the portal. You have the CSV file as shown in the below exhibit.



```
version:v1.0
Name (example: Chris Green) [displayName] *,User name (example: chris@contoso.com) [userPrincipalName]
*,Initial password [passwordProfile] *,Block sign in (Yes/No) [accountEnabled] *,First name [givenName],Last
name [surname],Job title [jobTitle],Department [department],Usage location [usageLocation],Street address
[streetAddress],State or province [state],Country or region [country],Office [physicalDeliveryOfficeName],City
[city],ZIP or postal code [postalCode],Office phone [telephoneNumber],Mobile phone [mobile]
user1,user1@company1.com,IFwRM6y8,No,,,,,,,,,,,,,
user2,user2@company1.com,c2czsL9d,No,,,,,,,,,,,,,
user3,user3@company1.com,R6hXoaVS,No,,,,,,,,,,,,,
user10,user10@outlook.com,NbO2rl0m,No,,,,,,,,,,,,,
user11,user11@gmail.com,ofEirgo7,No,,,,,,,,,,,,,
```

Users must log in using the e-mail addresses specified in the CSV file.

The creation of two user accounts fails, and the following error is displayed:

The user name in the uploaded file is not valid. Change the user name in the uploaded file to be a valid user name in your Azure AD. Ensure the domain portion of the user name is verified in your Azure AD or in the initial domain name (like *.onmicrosoft.com). Then resubmit your request.

You need to create the two user accounts that failed to import as guest users.

What should you do?

Choose the correct answer

A. Create a new CSV file for the two users and use the import-csv and New-AzureADMSInvitation PowerShell cmdlets to create the users. In the CSV file, specify the names and email addresses of the users.

B. Use the portal to create two users. Use user10@company1.onmicrosoft.com and user11@company1.onmicrosoft.com as email addresses.

C. Use the New-AzureADUser PowerShell cmdlet and set the parameter -UserType to Guest.

D. Create a new CSV file for the two users and use the import-csv and New-AzureADMSInvitation PowerShell cmdlets to create the users. In the CSV file, specify the names of the users, email addresses, and initial passwords.

Explanation:

You should perform the task by creating a new CSV file for the two users and using the import-csv and New-AzureADMSInvitation PowerShell cmdlets to create the users. In the CSV file, you only need to specify the names and email addresses of the users. The two user accounts that failed to be created are external user accounts (user10@outlook.com and user11@gmail.com). These are guest users and therefore do not have a password in the Azure tenant, seeing as authentication is performed by the guest user's identity provider (Microsoft or Google). A guest

user can be created with the New-AzureADMSInvitation cmdlet. This cmdlet sends an invitation email to the user. You should combine this with the import-csv cmdlet to use a CSV file as a source and create multiple accounts while running a single script. You should not specify an initial password in the CSV file.

You should not use the portal to create two users and change the email addresses to user10@company1.onmicrosoft.com and user11@company1.onmicrosoft.com. The users should use their own external identity provider.

You should not use the New-AzureADUser PowerShell cmdlet and set the -UserType parameter to Guest. This will not create a guest user, which is the thing you are trying to do. You can set the property User Type to Guest using this cmdlet, but you cannot create a user with an external identity provider.

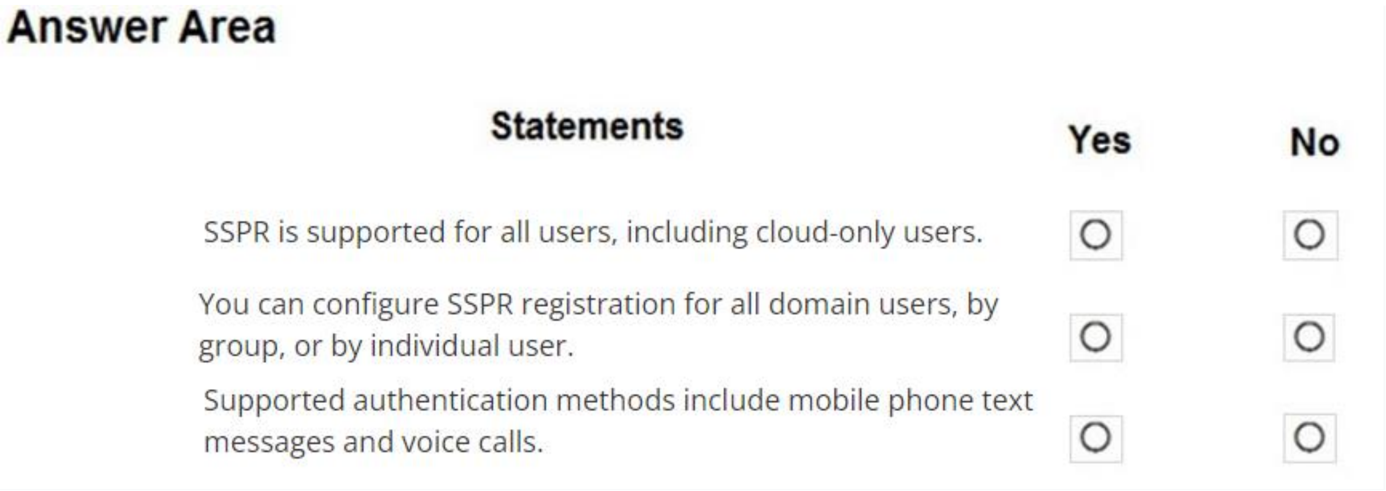
Question 151

CertyIQ

You have a hybrid network configuration. Most user accounts are in Azure Active Directory (Azure AD) and the on-premises domain. Some user accounts are Azure AD accounts only. Your company plans to deploy Azure AD self-service password reset (SSPR).

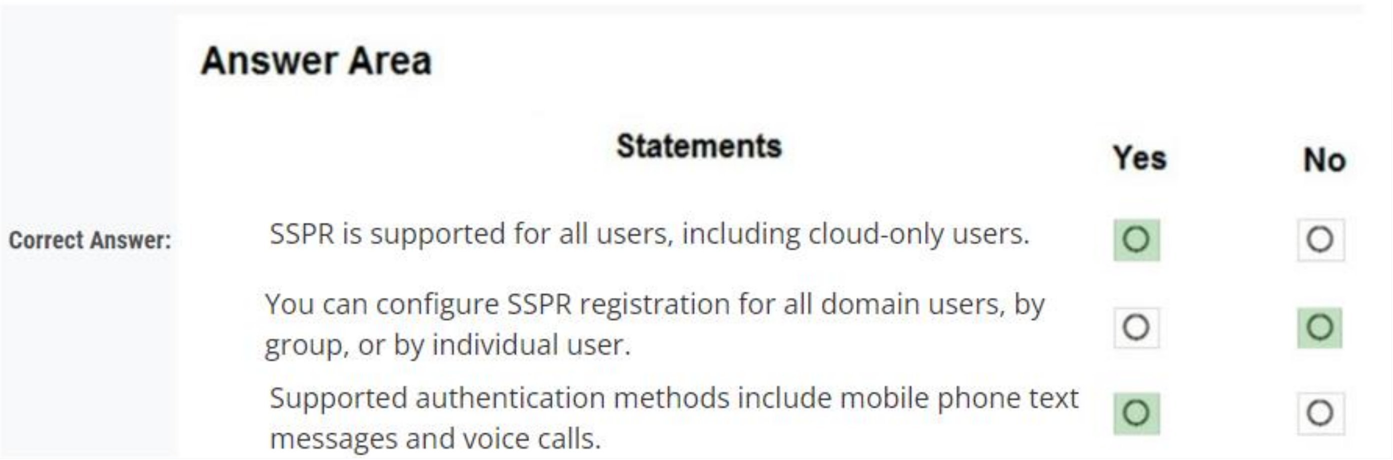
You need to ensure that SSPR meets your company's password reset requirements.

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



Answer Area

Statements	Yes	No
SSPR is supported for all users, including cloud-only users.	○	○
You can configure SSPR registration for all domain users, by group, or by individual user.	○	○
Supported authentication methods include mobile phone text messages and voice calls.	○	○



Correct Answer:

Answer Area

Statements	Yes	No
SSPR is supported for all users, including cloud-only users.	[✓ ○]	○
You can configure SSPR registration for all domain users, by group, or by individual user.	○	[✓ ○]
Supported authentication methods include mobile phone text messages and voice calls.	[✓ ○]	○

Explanation:

SSPR is supported for all users, including cloud-only users. You can configure password writeback to update on-premises passwords. For cloud-only users, passwords are stored in Azure AD.

You can configure SSPR registration by group or for all domain users. You cannot configure SSPR registration by user.

Supported authentication methods include mobile phone text messages and voice calls. Other supported authentication methods include:

- Password

- Security questions

. Email address

- Microsoft Authenticator app

When using security questions, Microsoft strongly recommends requiring at least one other authentication method.

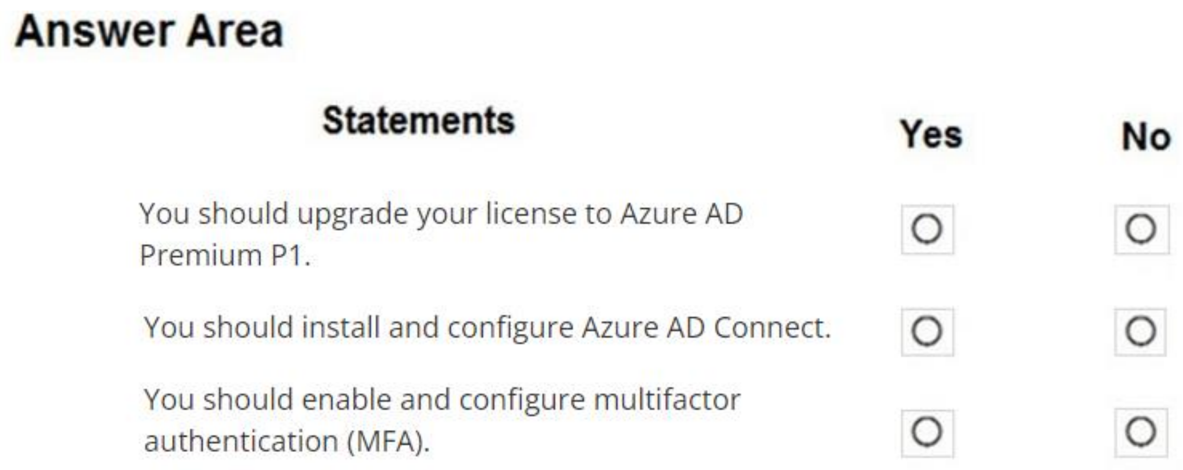
Question 152

CertyIQ

Your company has a Microsoft 365 Business Standard license. You configure Azure Active Directory (Azure AD) self-service password reset. You want to configure a hybrid environment with your on-premises Active Directory Domain Services (AD DS) network and enable writeback to your on-premises network.

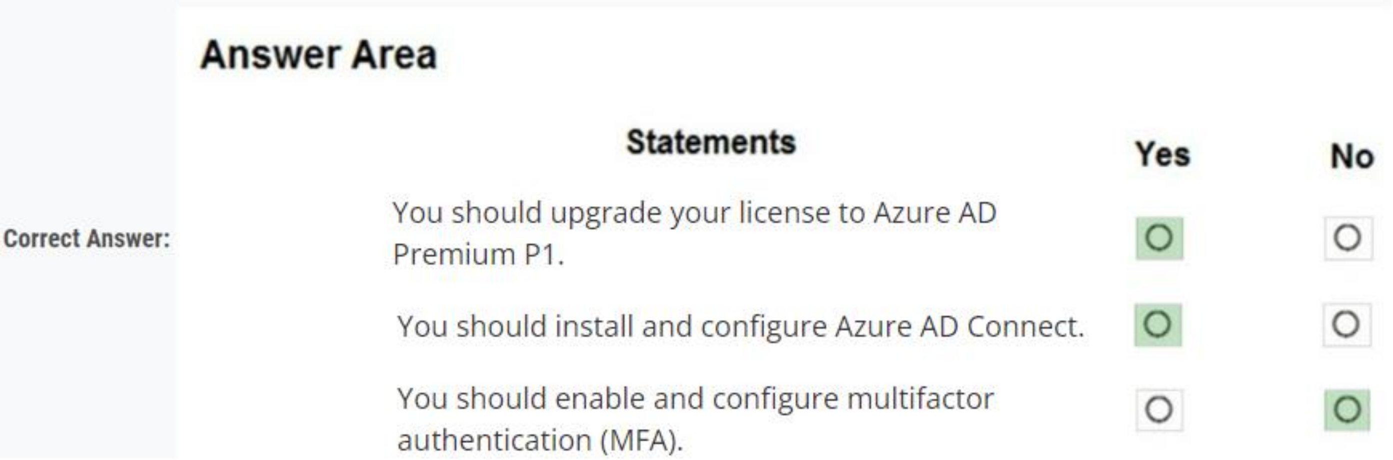
You need to ensure that prerequisites are met for supporting writeback.

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



Answer Area

Statements	Yes	No
You should upgrade your license to Azure AD Premium P1.	○	○
You should install and configure Azure AD Connect.	○	○
You should enable and configure multifactor authentication (MFA).	○	○



Correct Answer:

Answer Area

Statements	Yes	No
You should upgrade your license to Azure AD Premium P1.	[✓ ○]	○
You should install and configure Azure AD Connect.	[✓ ○]	○
You should enable and configure multifactor authentication (MFA).	○	[✓ ○]

Explanation:

You should upgrade your license to Azure Active Directory (Azure AD) Premium P1. Microsoft 365 Business Standard does not support writeback. Writeback requires Azure AD Premium P1 or P2 or Microsoft 365 Business Premium.

You should install and configure Azure AD Connect. This is a requirement for supporting writeback to your on-premises Active Directory Domain Services network (AD DS). Azure AD Connect provides a secure mechanism to send password updates back from Azure AD to your on-premises AD DS.

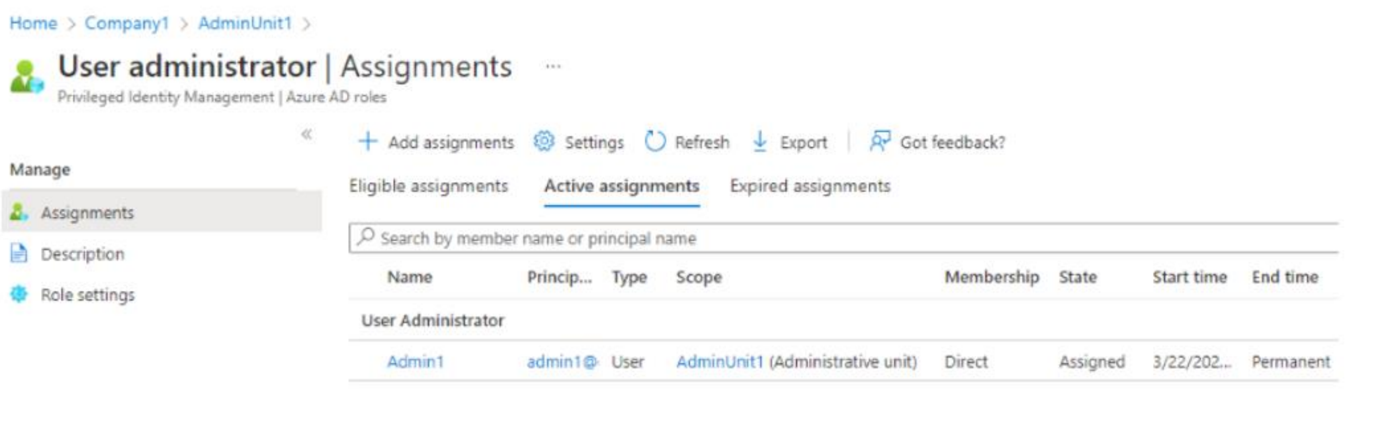
You are not required to enable and configure MFA MFA is recommended in situations where additional security is required but is not a prerequisite for supporting writeback.

Question 153

CertyIQ

You administer an Azure environment at Company1. You have been asked to restrict access for the administrator Admin1 to a portion of Azure Active Directory (Azure AD). You create the administrative unit AdminUnit1 and configure it as shown in the below exhibits:

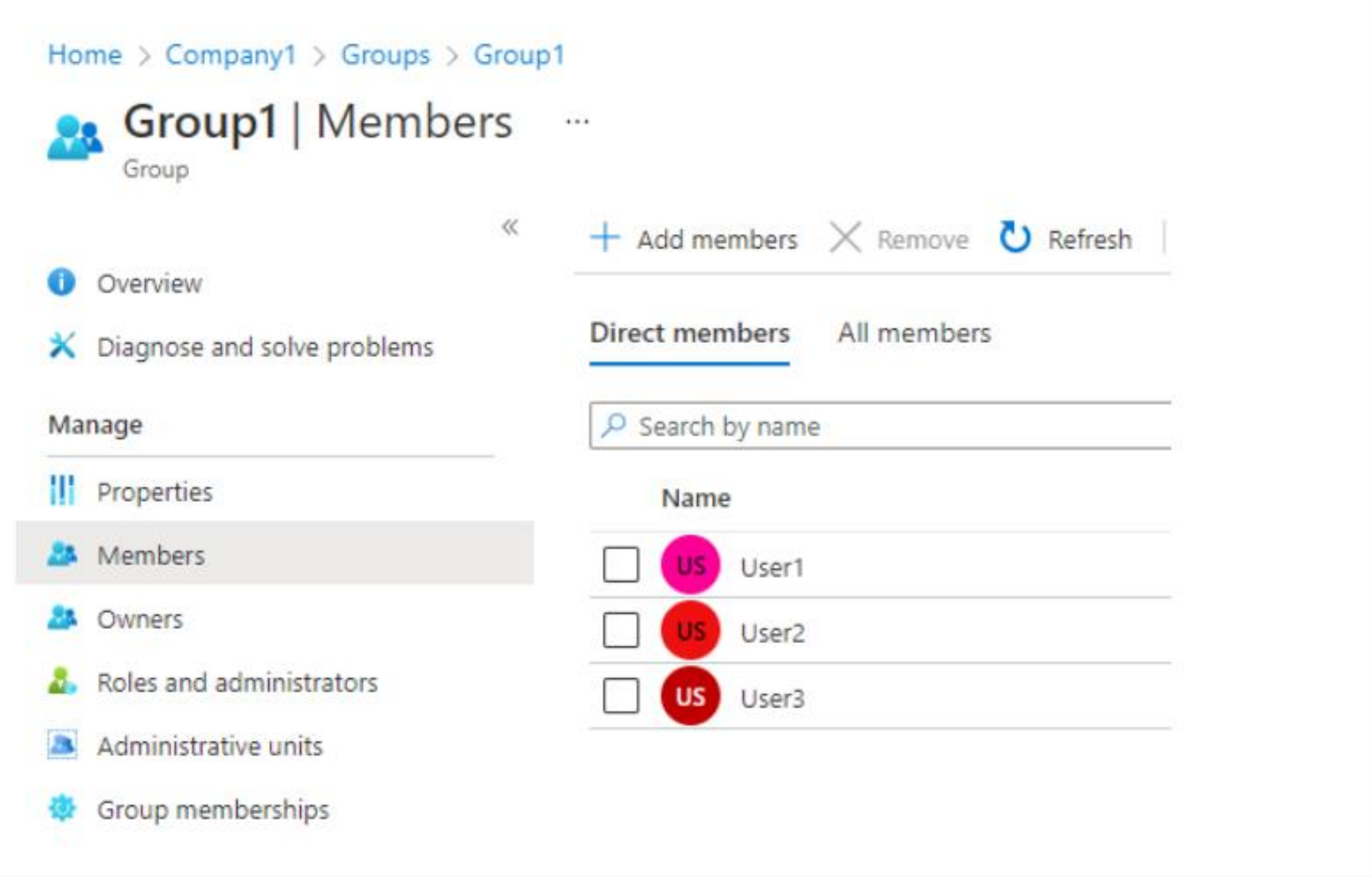
Administrative unit admin: -



Home > Company1 > AdminUnit1 >
User administrator | Assignments ...
Privileged Identity Management | Azure AD roles
+ Add assignments
Settings
Refresh
Export
Got feedback?
Manage
Assignments
Description
Role settings
Eligible assignments
Active assignments
Expired assignments
Search by member name or principal name

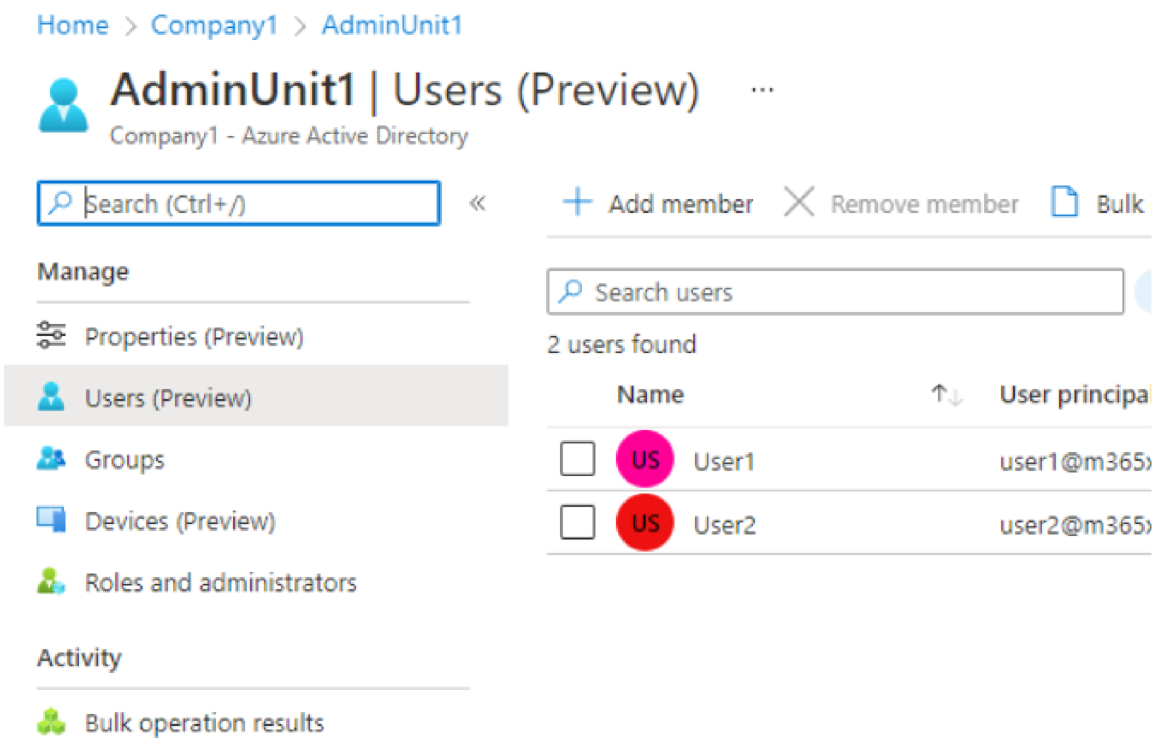
Name	Princip...	Type	Scope	Membership	State	Start time	End time
User Administrator							
Admin1	admin1@	User	AdminUnit1 (Administrative unit)	Direct	Assigned	3/22/202...	Permanent

Security Group: -



	Name
□	US User1
□	US User2
□	US User3

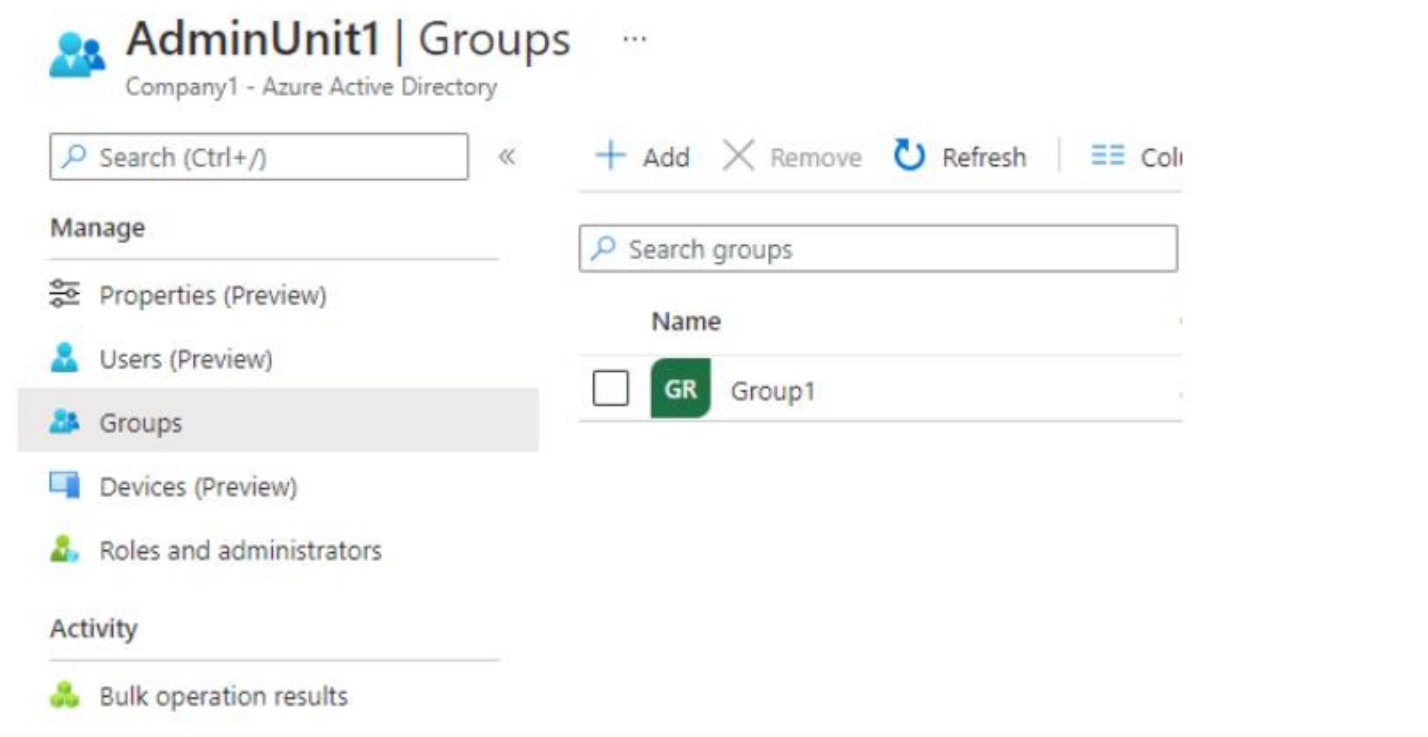
Administrative unit users: -



2 users found

	Name	User principa
□	US User1	user1@m365›
□	US User2	user2@m365›

Administrative unit group: -



Name
□ GR Group1

The configuration of the security group Group1 is shown in the Security Group exhibit. You need to identify the Azure AD objects that can be administered by Admin1.

Which Azure AD objects should you identify?

Choose the correct answer

A. User1, User2, and User3 only

B. User1, User2, and Group1 only

C. Group 1 only

D. User1, and User2 only

Explanation:

Admin1 can administer User1, User2, and Group1 only. With Azure administrative units, you can restrict access to any portion of Azure Active Directory (Azure AD). In this way, it is possible to restrict Admin's administrative access to the user and group objects that Admin1 is responsible for. Administrative units can only contain users and groups. Adding a security group to an administrative unit does not allow the administrative unit administrator to manage properties for individual members of that group. To allow the administrative unit administrator to manage individual members of the group, each group member must be added directly as a user to the administrative unit. In this scenario, Group1 and its members User1 and User2 are added directly to AdminUnit1. Therefore, only these Azure AD objects can be administered by Admin1.

Admin1 cannot administer User1, User2, and User3 only. Although Admin1 can modify the properties of Usert and User2, User3 is out of the administrative scope of AdminUnit1 and, as such, out of the administrative scope of Admin1. To allow Admin1 to modify User3, this user must be added directly as a user of AdminUnit1.

Admin1 cannot administer Group1 only. Although the properties of Group1 can be modified by Admin1, it is not the only Azure AD object that can be modified by Admin1 in this scenario.

Admin1 cannot administer User1 and User2 only. Although the properties of User1 and User2 can be modified by Admin1, they are not the only Azure AD objects that can be modified by Admin1 in this scenario.

Question 154 CertyIQ

An international organization has an existing Azure AD tenant that gives its users access to cloud-hosted applications and synchronizes with your on-premises Active Directory tenant. Users in the London office have hybrid user objects and they have been assigned the Azure AD P1 license.

A report from the support team shows that a large number of tickets have been raised concerning users asking for their passwords to be changed. The organization decides to enable self-service password reset (SSPR) in order to reduce the number of support tickets. You enable SSPR via the Azure portal and assign it to the All Users security group. However, tickets are still being raised by users in the London office

You need to find out what is causing SSPR to not work for users in the London office.

What is the root cause of the issue?

Choose the correct answer

A. Password writeback is not enabled.

B. The user group does not include hybrid users.

C. SSPR does not support hybrid users.

D. The London users do not have the correct license.

Explanation:

Password writeback is not enabled. You need to enable password writeback to allow hybrid users to utilize Self-Service Password Reset (SSPR). The identity objects of the London users are hosted on an on-premises Active Directory which synchronizes with Azure Active Directory (Azure AD). When a London user changes their password, it will update in Active Directory. By default, Azure AD Connect synchronizes passwords in one direction only: Azure AD to on-premises Active Directory. You need to enable and configure password writeback to allow users to update their password in the on-premises environment and synchronize it to Azure AD.

The All Users group includes cloud-only members, directory-synchronized members (hybrid) and guest users. The All Users security group is automatically created in Azure AD and it is one of the default groups to which all users within your tenant are added when they are created. This includes cloud-only, hybrid and guest accounts.

SSPR supports hybrid users that are synchronized from an on-premises Active Directory. You need to ensure that password writeback is enabled and configured in Azure AD Connect to facilitate hybrid user support.

The London users do have the relevant license. SSPR requires an Azure AD Premium 1 license or higher.

Question 155 CertyIQ

You are the owner of your organization's Microsoft Azure subscription. You hire a new administrator to help you manage a virtual network that contains nine Windows Server virtual machines (VMs). The deployment is contained in a resource group named prod-rg.

You need to provide the administrator with the least privilege access to the prod-rg resource group only.. The administrator should be allowed to manage all aspects of the Azure VMs. Your solution should minimize management effort.

What should you do?

Choose the correct answer

A. Assign the administrator to the Virtual Machine Operator role at the virtual machine scope.

B. Assign the Allowed virtual machine SKUs Azure Policy at the resource group scope.

C. Assign the administrator to the Contributor role at the resource group scope.

D. Assign a custom Azure Policy at the management group scope.

Explanation:

You should assign the administrator to the Contributor role at the resource group scope. The Contributor role-based access control (RBAC) role provides the new administrator with full read/write privileges at that scope. Inheritance ensures that the permissions cascade to the virtual machines (VMs) within the prod-rg resource group and management overhead is therefore minimized.

You should not assign the administrator to the Virtual Machine Operator role at the virtual machine scope. The Virtual Machine Operator role does not grant the administrator full access to all resources contained on the virtual network, which is required in this scenario.

You should not assign the Allowed virtual machine SKUs Azure Policy at the resource group scope. Doing this would only restrict the administrator from selecting VM instance stock-keeping units (SKUs) that are defined in the Azure Policy. The scenario states that the administrator should be able to fully manage existing VMs within the prod-rg resource group only.

You should not assign a custom Azure Policy at the management group scope. Azure Policy is a governance feature that restricts the types of resources administrators can select in Azure Resource Manager. In other words, Azure Policy is fundamentally different from RBAC, which limits the ability of administrators to take particular actions in the first place.

Question 156

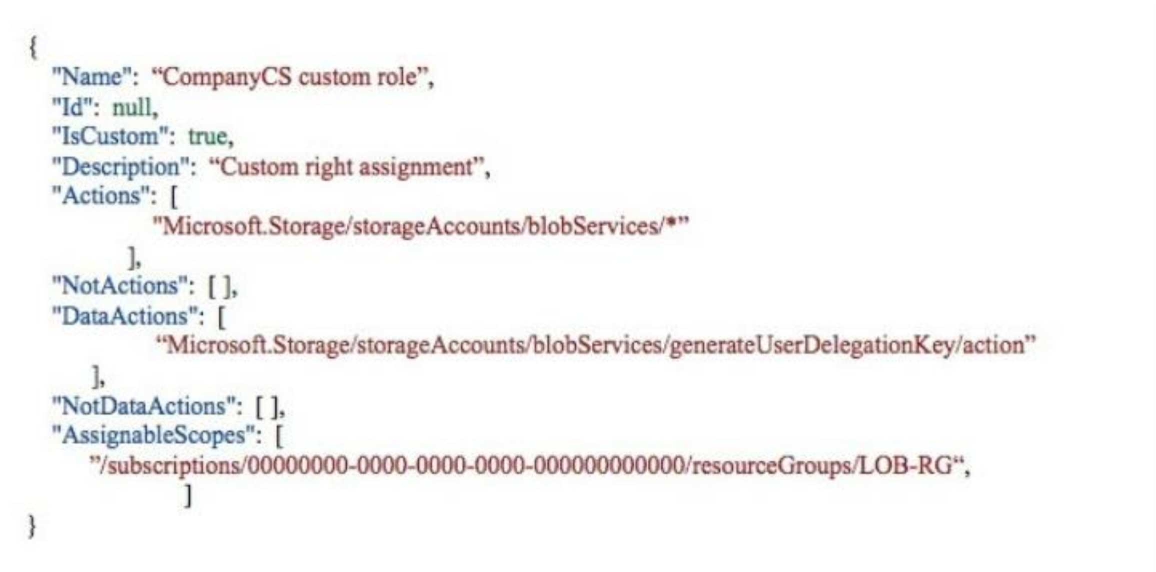
CertyIQ

Your company has hired a new cloud engineer. As global administrator, you need to delegate some privileges to this new engineer.

You decide to create a custom role using the following PowerShell command:

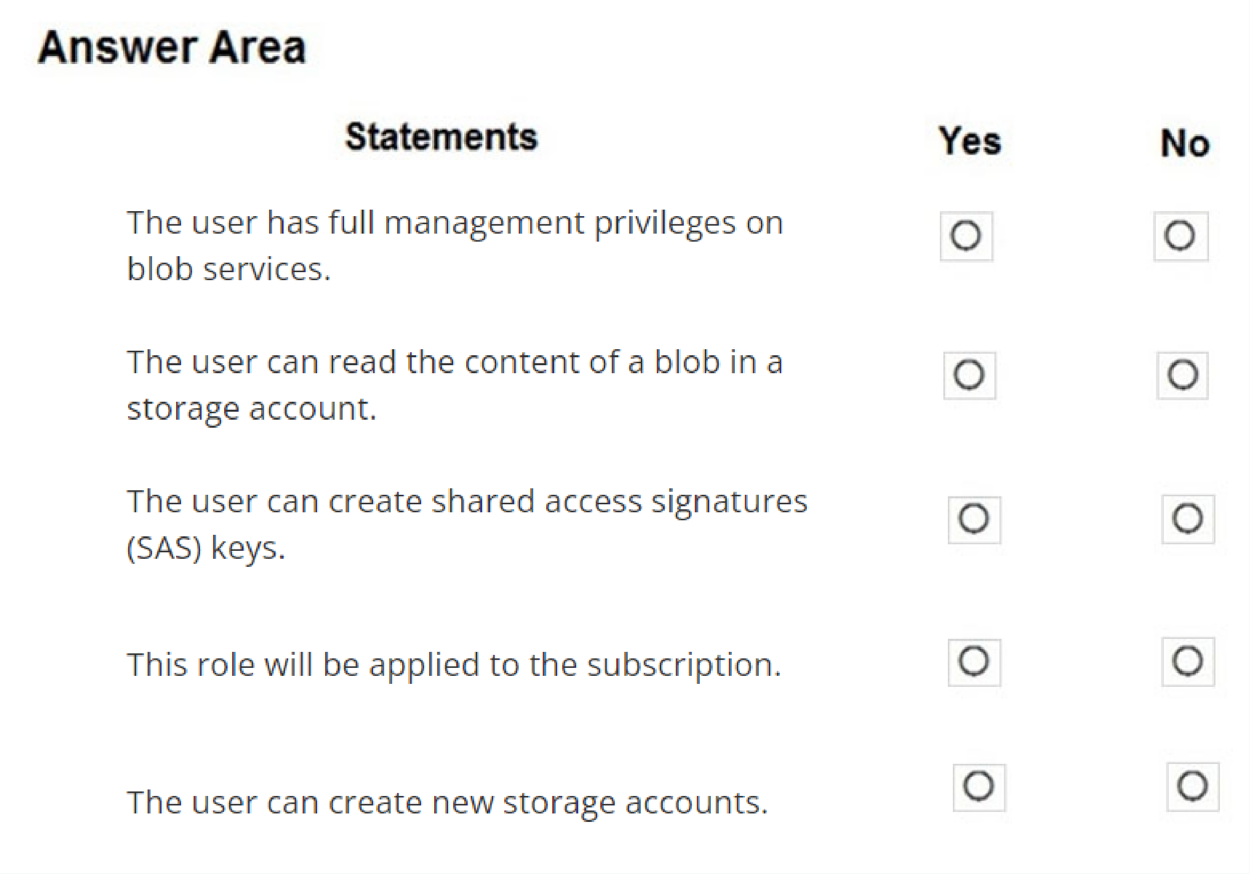
New-AzRoleDefinition -InputFile "C:\ARM templates\customrolel.json"

The content of the customrole1.json file is shown in the below exhibit.



```
{
   "Name": “CompanyCS custom role”,
   "Id": null,
   "IsCustom": true,
   "Description": “Custom right assignment”,
   "Actions": [
            "Microsoft.Storage/storageAccounts/blobServices/*”
          ],
   "NotActions": [ ],
   "DataActions": [
            “Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey/action”
       ],
   "NotDataActions": [ ],
   "AssignableScopes": [
      ”/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/LOB-RG“,
                 ]
}
```

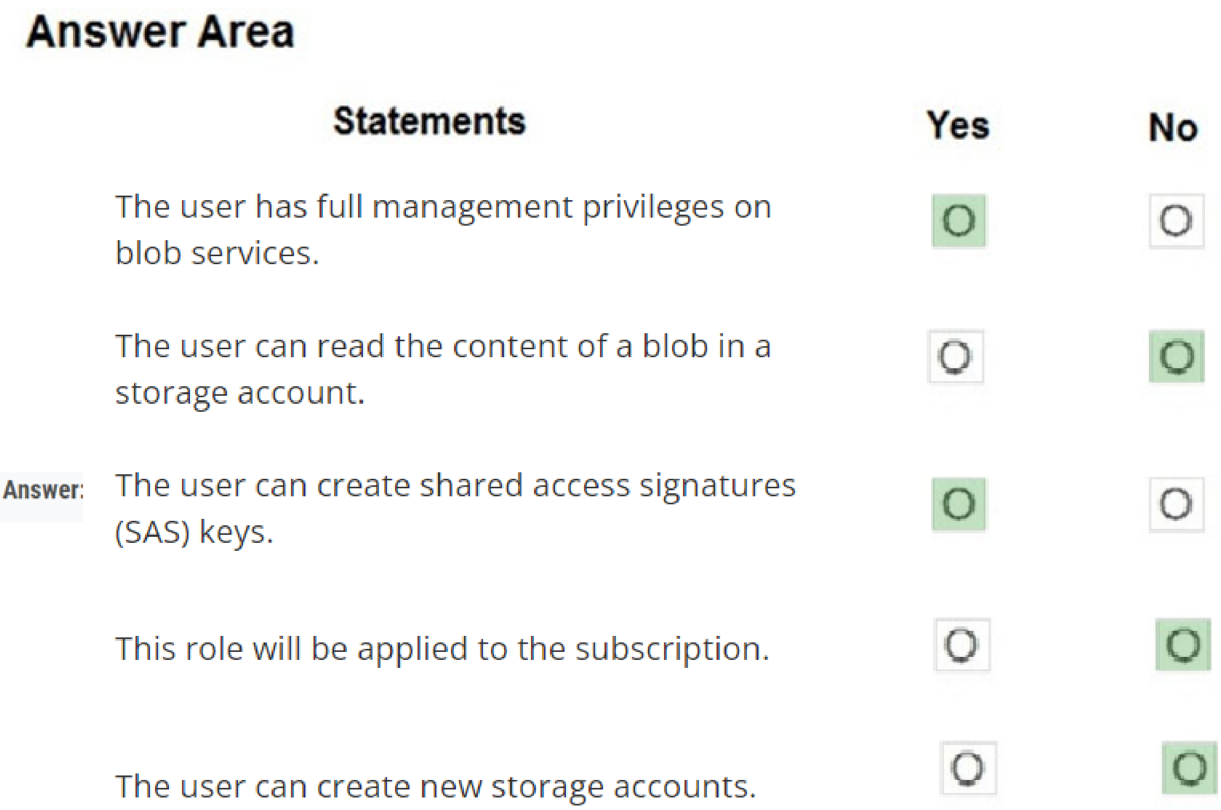
For each of the following statements, select Yes if the statement is true. Otherwise, select No.



Answer Area

Statements	Yes	No
The user has full management privileges on blob services.	○	○
The user can read the content of a blob in a storage account.	○	○
The user can create shared access signatures (SAS) keys.	○	○
This role will be applied to the subscription.	○	○
The user can create new storage accounts.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
The user has full management privileges on blob services.	[✓ ○]	○
The user can read the content of a blob in a storage account.	○	[✓ ○]
The user can create shared access signatures (SAS) keys.	[✓ ○]	○
This role will be applied to the subscription.	○	[✓ ○]
The user can create new storage accounts.	○	[✓ ○]

Explanation:

The user has full management privileges on blob services. When you create a custom role, you can configure two types of privileges: management and data privileges. Management privileges are used for performing actions on the resources without accessing the data itself. In this scenario, you can perform administrative actions on the blob service, like creating new containers or removing them. Management actions are managed by using the Actions/NotActions properties in the template JSON file. If you want to remove a specific privilege from the action privileges, you need to add that privilege to the NoAction section.

The user cannot read the content of a blob in a storage account Management and data access rights are managed separately. This means that you need to grant specific privileges to allow the user to read content from the blobs. In this case, you are not setting such a privilege, so the user will not be able to read the blob's content. Data access is managed by using the DataActions/NotDataActions properties in the template JSON file.

The user can create shared access signature (SAS) keys. You have specifically set this privilege in the DataActions properties in the template JSON file, so the user will be able to create user delegation keys, including SAS keys.

This role will not be applied to the subscription. This role will only be applied to the LOB-RG resource group. The level at which a custom role can be applied is controlled by the AssignableScopes property in the template JSON file. In this scenario, you set the LOB-RG resource group as the only scope in which you can apply this custom role. If you need to be able to apply this role to a subscription, you need to use the "/"value for this property.

The user cannot create new storage accounts. The administrative rights have been applied to the blobService node, not to the storageAccount parent node. If you need to grant privileges for creating new storage accounts on the LOB-RG resource group, you need to use the value Microsoft.Storage/storageAccounts/*.

Question 157

CertyIQ

Your company has several Azure subscriptions assigned to different departments. You configure a root management group for the organization and it. You configure a management group for each department to group the subscriptions that pertain to that department. The organization management group contains all these other department groups.

Your company hires two new cloud engineers. You need to delegate some restricted privileges to these new cloud engineers. You decide to create a custom role to delegate the correct permissions to the new engineers.

You need to apply this new role at the correct level. You need to ensure that you apply this new role with the least administrative effort.

What should you do?

Choose the correct answer

A. Apply the Owner role at the organization management group level.

B. Apply the custom role in each subscription.

C. Apply the custom role in each resource group in each subscription.

D. Apply the custom role in each resource in each subscription.

Explanation:

You should apply the custom role in each subscription. When you apply a role to a resource with children, all the resources within that resource also inherit the privileges from the parent container. In this scenario, because you apply the custom role at the subscription level, all the resources inside that subscription inherit the privileges granted by the role to the new engineers. The advantage of this approach is that any new resource or resource group that you create in any of the subscriptions of the company will automatically inherit the permissions granted by the custom role. If you create a new subscription, you need to remember to add the custom role to this new subscription.

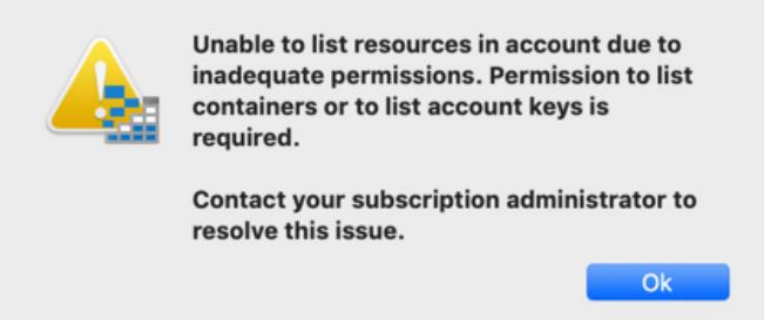
You should not apply the Owner role at the organization management group level. A management group is a way to efficiently manage policies, access, and compliance when your company has several subscriptions. Although you can apply the Owner role at the management group level, it provides assignees with full access to all resources down the hierarchy, i.e. the privileges are not restricted.

You should not apply the custom role in each resource or resource group in each subscription. Assigning the custom role at resource or resource group level grants the needed privileges for the new engineers, but it requires a lot of administrative effort. Another drawback of using this approach is that you need to remember to assign the custom role to any new resource groups or new resources within a group.

Question 158 CertyIQ

You have storage accounts in your Azure subscription for different purposes. The storage accounts have blob containers and file shares configured.

Some users access these storage accounts by using the Microsoft Azure Storage Explorer desktop application. They are reporting that they get the error message shown in the below exhibit when they try to browse the contents of the storage account.


Unable to list resources in account due to inadequate permissions. Permission to list containers or to list account keys is required.

Contact your subscription administrator to resolve this issue.

You need to resolve the issue.

What are two possible reasons why users are getting this error message? Each correct answer presents a complete solution.

Choose the correct answers

A. Your users have the Read role assigned in the storage accounts.

B. There is a CanNotDelete resource lock configured.

C. There is a ReadOnly resource lock configured.

D. Your users have the Storage Blob Data Contributor role assigned in the storage accounts.

E. Your users have the Storage Blob Data Reader role assigned in the storage accounts.

Explanation:

Your users are getting the error shown in the exhibit because there is a ReadOnly resource lock configured or because your users have the Read role assigned in the storage accounts. When a user or process needs to list the contents of a storage account, Azure needs to read the access keys of the storage account before listing the contents of the containers. Because the access keys of a storage account provide write access to the data and there is no read-only access key available in the storage account, you need read-write permissions to list the contents of a storage account. Neither the ReadOnly nor the Read role grants the Microsoft Storage/storageAccounts/listKeys/action permission that allows Azure to list the access keys.

The root cause of the error is not due to a CanNotDelete resource lock being configured. The CanNotDelete resource lock allows you to list the contents of the storage account. This resource lock prevents you from deleting the storage account or any of the children of the storage account. For example, if you assign a role to a user in a storage account with the CanNotDelete resource lock configured, you cannot later remove that role assignment from the storage account

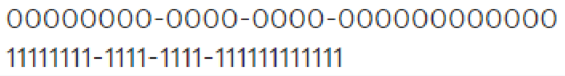
The root cause of the error is not due to your users having the Storage Blob Data Contributor role assigned in the storage accounts. This role allows the user to read, write, and delete Azure Storage containers and blobs. If you only assign this role to a user, they will not be able to see the storage account in the list of resources in the Azure Portal or Microsoft Azure Storage Explorer, because they are still missing the Microsoft Storage/storageAccounts/read privilege.

Having the Storage Blob Data Reader role assigned in the storage accounts would not generate the error reported. This role allows users to read and list Azure Storage containers and blobs.

Question 159

CertyIQ

You are the global administrator for the following Azure subscriptions in your company:



00000000-0000-0000-000000000000
1111111-1111-1111-11111111111

The company hires a new network engineer.

You need to grant this network engineer the required privileges to manage network-related resources in each subscription. You decide to create a custom role definition using a JSON template.

You need to set the AssignableScopes property. You need to ensure that your solution requires the least administrative effort.

Which scope should you use?

Choose the correct answer

A. "/"

B. "/subscriptions/00000000-0000-0000-000000000000/resourceGroups/Network".
"/subscriptions/11111111-1111-1111-111111111111/resourceGroups/Network"

C. "/subscriptions/00000000-0000-0000 000000000000/resourceGroups/Network/providers/Microsoft.Network/virtualNetworks/VNET/subnets/default",
"/subscriptions/11111111-1111-1111 111111111111/resourceGroups/Network/providers/Microsoft.Network/virtualNetworks/VNET/subnets/default"

D. "/subscriptions/00000000-0000-0000-000000000000",
"/subscriptions/11111111-1111-1111-111111111111"

Explanation:

You should use the value "/subscriptions/00000000-0000-0000-000000000000","/subscriptions/11111111 1111-1111-111111111111" for the AssignableScopes parameter. Using this value, you can use your custom role in any resource under the subscriptions 00000000-0000-0000-000000000000 and 11111111-1111-1111 111111111111. Because you need to grant access to network resources only, you need to create the custom role with the appropriate rights to allow access only to network resources.

You should not use the value "/". This value means that you could assign your custom role to any subscription. Unfortunately, this is a reserved value that cannot be used with a custom role. You see this value in built-in roles.

You should not use the values "/subscriptions/00000000-0000-0000 000000000000/resourceGroups/Network","/subscriptions/11111111-1111-1111 111111111111/resourceGroups/Network".

The general structure of a resource ID is:

/subscriptions/subscriptionid)/resourceGroups/(resourceGroupName]/providers/(resourceProvider Namespace) /[resourceType)/[resourceName).

As you can see in the general structure, the Network value corresponds to the name of a resource group, not the networking provider. Using these values would allow you to use your custom role only in the Network resource groups in both subscriptions. Using a resource ID like "/subscriptions/00000000-0000 0000-000000000000/resourceGroups/*/providers/Microsoft Network/*" is not a valid resource ID, because wildcards are not allowed in resource IDs.

You should not use the values:

"/subscriptions/00000000-0000-0000-000000000000/resourceGroups/Network/providers/ Microsoft Network/virtualNetworks/VNET/subnets/default","/subscriptions/11111111-1111-1111 111111111111/resourceGroups/Network/providers/Microsoft.Network/virtualNetworks /VNET/subnets/default"

This would allow you to use your custom role only in the default subnet in the virtual network in the Network resource group in each subscription. This is too specific and does not meet the requirements.

Question 160

CertyIQ

You are the administrator for your Azure subscription. Your company hires a new cloud engineer.

The cloud engineer needs to be able to manage other engineers' access to Azure resources. You need to follow the principle of least privilege.

Which role should you assign to the new engineer?

Choose the correct answer

A. Contributor

B. Co-Administrator

C. Owner

D. User Administrator

E. User Access Administrator

Explanation:

You should grant the User Access Administrator role. This role allows members to manage user access to Azure resources.

You should not grant the Owner role. This role allows members to manage user access to Azure resources but also grants full access to all resources. This role violates the principle of least privilege in this scenario.

You should not grant the Contributor role. This role allows members to create and manage all types of resources but it does not allow them to manage other users' access to Azure resources in the subscription.

You should not grant the Co-Administrator role. This is a classic subscription role that is equivalent to the Owner Role-Based Access Control (RBAC) role. This role violates the principle of least privilege in this scenario.

You should not grant the User Administrator role. This is an Azure Active Directory (Azure AD) administrator role that does not control access to any Azure resources. This role grants permissions to manage users and groups in the Azure AD tenant associated with the Azure subscription.

End of Part 4

We hope to see you again...

Please find the videos of this **AZ-900/AI-900/AZ-305/ AZ-104 /DP-900/ SC-900 and other Microsoft exam** series on

CertyIQ Official YouTube channel (**FREE PDFs**): -

Please Subscribe to CertyIQ YouTube Channel to get notified for latest exam dumps by clicking on the below image, it will redirect to the CertyIQ YouTube page.

Connect with us @ LinkedIn Telegram

Contact us for other dumps: -

contact.certyiqofficial@gmail.com

For any other enquiry, please drop us a mail at

enquiry.certyiqofficial@gmail.com