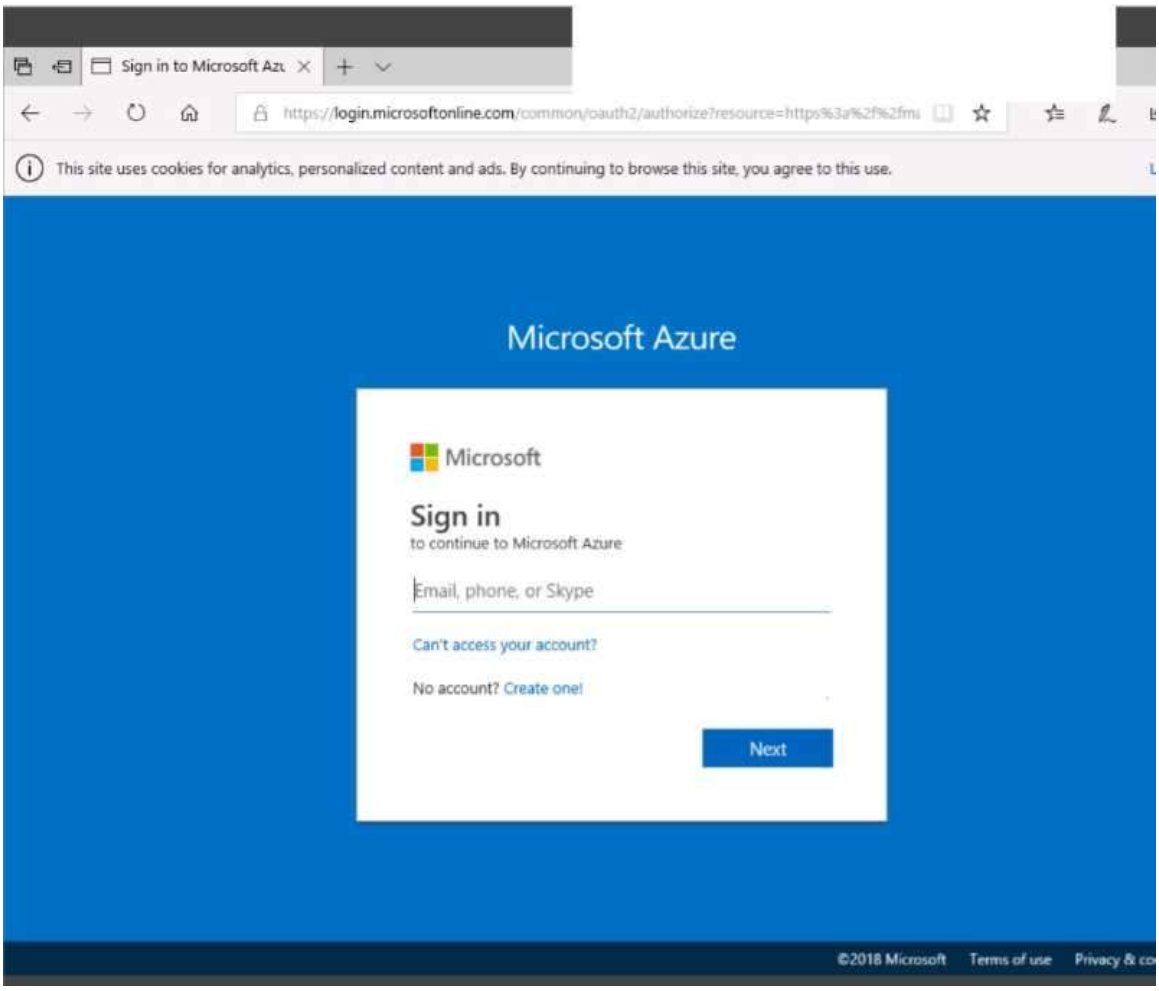
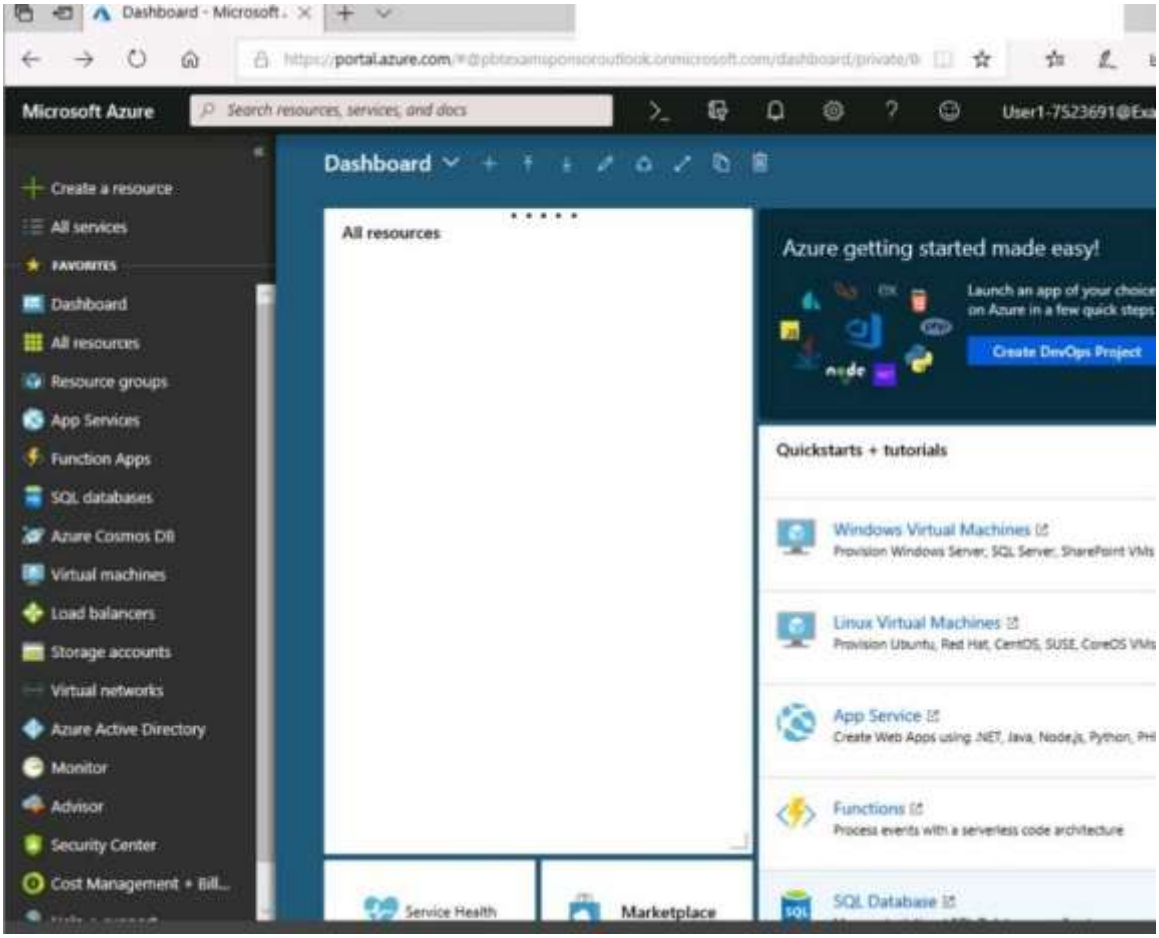
- **Vendor:** Microsoft
- **Exam Code:** AZ-100
- **Exam Name:** Microsoft Azure Infrastructure and Deployment
- **New Updated Questions from Braindump2go**
- **(Updated in December/2021)**

QUESTION 93
SIMULATION
Click to expand each objective. To connect to the Azure portal, type https://portal.azure.com in the browser address bar.




Dashboard - Microsoft
Microsoft Azure
Search resources, services, and docs
Dashboard
Create a resource
All services
FAVORITES
Dashboard
All resources
Resource groups
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
All resources
Azure getting started made easy!
Create DevOps Project
Quickstarts + tutorials
Windows Virtual Machines
Linux Virtual Machines
App Service
Functions
SQL Database
Service Health
Marketplace

Home > Storage accounts > Create storage account

Create storage account

Validation passed

Basics | Advanced | Tags | Review + create

BASICS

Subscription	Microsoft AZ-100 5
Resource group	corpdatalod7523690
Location	East US
Storage account name	corpdata7523690n1
Deployment model	Resource manager
Account kind	StorageV2 (general purpose v2)
Replication	Read-access geo-redundant storage (RA-GRS)
Performance	Standard
Access tier (default)	Hot

ADVANCED

Secure transfer required	Enabled
Hierarchical namespace	Disabled

Create | Previous | Next | Download a template for automation

Home > Storage accounts > Create storage account

Create storage account

Submitting deployment...

Submitting the deployment template for resourc 'corpdatalod7523690'.

Basics Advanced Tags Review + create

BASICS

Subscription	Microsoft AZ-100 5
Resource group	corpdatalod7523690
Location	East US
Storage account name	corpdata7523690n1
Deployment model	Resource manager
Account kind	StorageV2 (general purpose v2)
Replication	Read-access geo-redundant storage (RA-GRS)
Performance	Standard
Access tier (default)	Hot

ADVANCED

Secure transfer required	Enabled
Hierarchical namespace	Disabled

Home > Microsoft.StorageAccount-20181011170335 - Overview

Microsoft.StorageAccount-20181011170335 - Overview

Deployment

Search (Ctrl+/)

Overview

Outputs

Inputs

Template

Delete Cancel Redeploy Refresh

Your deployment is underway

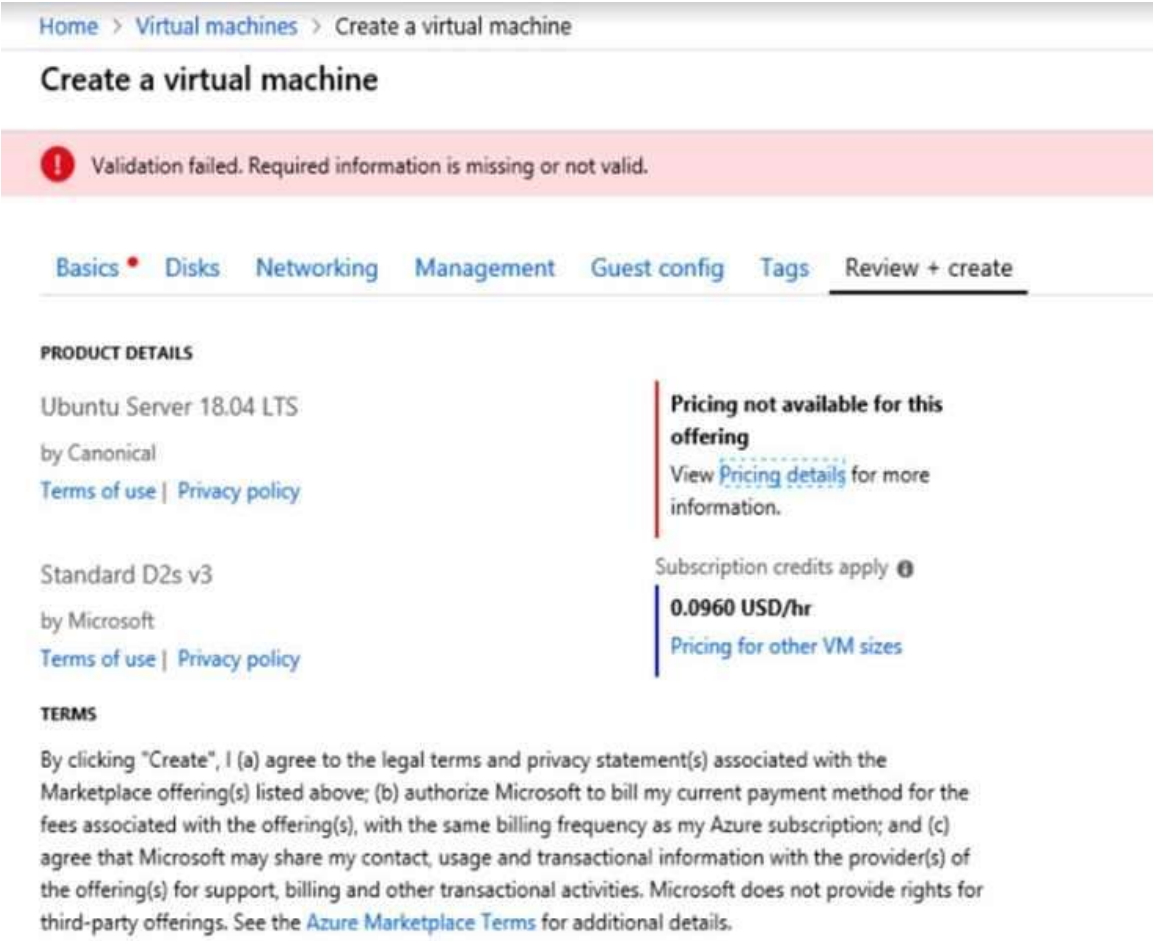
Check the status of your deployment, manage resources, or troubleshoot deployment issues. Pin this page to your dashboard to easily find it next time.

Deployment name: Microsoft.StorageAccount-20181011170335
Subscription: Microsoft AZ-100 5
Resource group: corpdatalod7523690

DEPLOYMENT DETAILS (Download)

Start time: 10/11/2018 5:04:06 PM
Duration: 17 seconds
Correlation ID: bd0806a4-d1bd-42db-be6b-55e0ec38f49b

RESOURCE	TYPE	STATUS	OPERATI...
No results.			



When you are finished performing all the tasks, click the `Next' button. Note that you cannot return to the lab once you click the `Next' button. Scoring occur in the background while you complete the rest of the exam.
Overview
The following section of the exam is a lab. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design. Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
To start the lab
You may start the lab by clicking the Next button.
You need to create a virtual network named VNET1008 that contains three subnets named subnet0, subnet1, and subnet2. The solution must meet the following requirements:
Connections from any of the subnets to the Internet must be blocked. Connections from the Internet to any of the subnets must be blocked. The number of network security groups (NSGs) and NSG rules must be minimized.
What should you do from the Azure portal?

A. See solution below explanation

Answer: A
Explanation:
Step 1: Click Create a resource in the portal.
Step 2: Enter Virtual network in the Search the Marketplace box at the top of the New pane that appears. Click Virtual

network when it appears in the search results. Step 3: Select Classic in the Select a deployment model box in the Virtual Network pane that appears, then click Create.
Step 4: Enter the following values on the Create virtual network (classic) pane and then click Create:
Name: VNET1008
Address space: 10.0.0.0/16
Subnet name: subnet0
Resource group: Create new
Subnet address range: 10.0.0.0/24
Subscription and location: Select your subscription and location.
Step 5: In the portal, you can create only one subnet when you create a virtual network. Click Subnets (in the SETTINGS section) on the Create virtual network (classic) pane that appears. Click +Add on the VNET1008 - Subnets pane that appears.
Step 6: Enter subnet1 for Name on the Add subnet pane. Enter 10.0.1.0/24 for Address range. Click OK.
Step 7: Create the third subnet: Click +Add on the VNET1008 - Subnets pane that appears. Enter subnet2 for Name on the Add subnet pane. Enter 10.0.2.0/24 for Address range. Click OK. References: https://docs.microsoft.com/en-us/azure/virtual-network/create-virtual-network-classic

QUESTION 94
Note: This question is part of a series questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage a virtual network named Vnet1 that is hosted in the West US Azure region. VNet hosts two virtual machines named VM1 and VM2 run Windows Server.
You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.
Solution: From Azure Network Watcher, you create a connection monitor.
Does this meet the goal?

A. YES
B. NO

Answer: A
Explanation:
Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network.
Capture packets to and from a VM
Advanced filtering options and fine-tuned controls, such as the ability to set time and size limitations, provide versatility. The capture can be stored in Azure Storage, on the VM's disk, or both. You can then analyze the capture file using several standard network capture analysis tools. Network Watcher variable packet capture allows you to create packet capture sessions to track traffic to and from a virtual machine. Packet capture helps to diagnose network anomalies both reactively and proactivity.
References:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

QUESTION 95
You have a virtual network named VNet1 as shown in the exhibit.

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

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

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

QUESTION 96
You have an Azure subscription that contains three virtual networks named VNet1, VNet2, VNet3.
VNet2 contains a virtual appliance named VM2 that operates as a router. You are configuring the virtual networks in a hub and spoke topology that uses VNet2 as the hub network.
You plan to configure peering between VNet1 and VNet2 and between VNet2 and VNet3.
You need to provide connectivity between VNet1 and VNet3 through VNet2.
Which two configurations should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. On the peering connections, allow forwarded traffic.
B. On the peering connections, allow gateway transit.

C. Create route tables and assign the table to subnets.
D. Create a route filter.
E. On the peering connections, use remote gateways.

Answer: BE
Explanation:
Allow gateway transit: Check this box if you have a virtual network gateway attached to this virtual network and want to allow traffic from the peered virtual network to flow through the gateway. The peered virtual network must have the Use remote gateways checkbox checked when setting up the peering from the other virtual network to this virtual network.
References: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints

QUESTION 97
You are the global administrator for an Azure Active Directory (Azure AD) tenant named adatum.com.
You need to enable two-step verification for Azure users.
What should you do?

A. Configure a playbook in Azure AD conditional access policy.
B. Create an Azure AD conditional access policy.
C. Create and configure the Identify Hub.
D. Install and configure Azure AD Connect.

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

QUESTION 98
From the MFA Server blade, you open the Block/unblock users blade as shown in the exhibit.
Block/unblock users
A blocked user will not receive Multi-Factor Authentication requests. Authentication attempts for that user will be automatically denied. A user will remain blocked for 90 days from the time they are blocked. To manually unblock a user, click the "Unblock" action.

Blocked users

USER	REASON	DATE	ACTION
AlexW@M365x832514.OnMicrosoft.com	Lost phone	06/14/2018, 8:26:38 PM	Unblock

What caused AlexW to be blocked?

A. The user entered an incorrect PIN four times within 10 minutes.
B. The user account password expired.
C. An administrator manually blocked the user.
D. The user reported a fraud alert when prompted for additional authentication.

Answer: D

QUESTION 99
You have the Azure virtual networks shown in the following table.

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

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

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

Answer: C
Explanation:
The virtual networks you peer must have non-overlapping IP address spaces. The VNet1 and VNhet2 address spaces overlap. The range of VNet2 is contained inside the range of VNet1.
References:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage- peering#requirements-and-constraints

QUESTION 100
You have two Azure virtual networks named VNet1 and VNet2. VNet1 contains an Azure virtual machine named VM1. VNet2 contains an Azure virtual machine named VM2. VM1 hosts a frontend application that connects to VM2 to retrieve data. Users report that the frontend application is slower than usual.
You need to view the average round-trip time (RTT) of the packets from VM1 to VM2.
Which Azure Network Watcher feature should you use?

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

Answer: D
Explanation:
The Connection Monitor feature in Azure Network Watcher is now generally available in all public regions. Connection Monitor provides you RTT values on a per-minute granularity. You can monitor a direct TCP connection from a virtual machine to a virtual machine, FQDN, URI, or IPv4 address.
References:
https://azure.microsoft.com/en-us/updates/general-availability-azure-network-watcher-connection-monitor-in-all-public-regions/

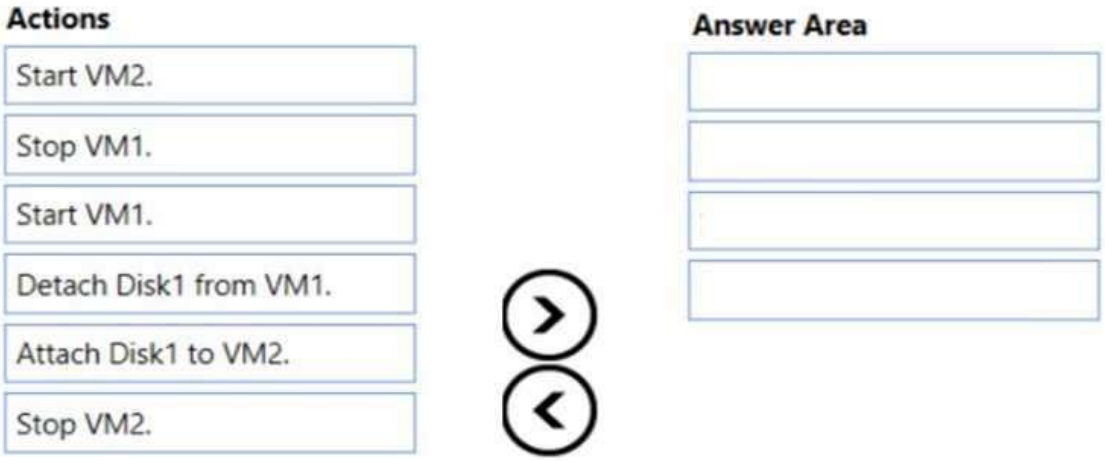
QUESTION 101
You are troubleshooting a performance issue for an Azure Application Gateway.
You need to compare the total requests to the failed requests during the past six hours.
What should you use?

A. Metrics in Application Gateway
B. Diagnostics logs in Application Gateway
C. NSG flow logs in Azure Network Watcher
D. Connection monitor in Azure Network Watcher

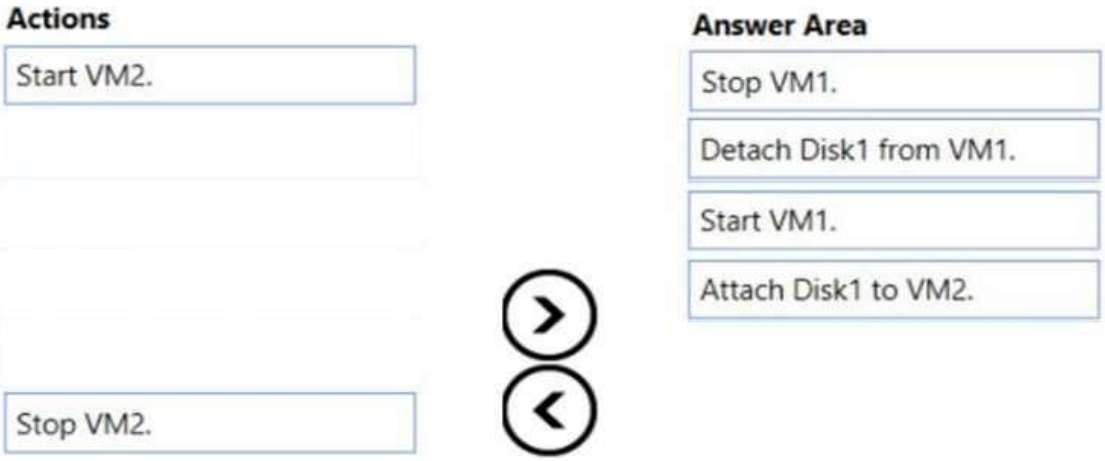
Answer: A
Explanation:
Application Gateway currently has seven metrics to view performance counters. Metrics are a feature for certain Azure resources where you can view performance counters in the portal. For
Application Gateway, the following metrics are available:

Total Requests
Failed Requests
Current Connections
Healthy Host Count
Response Status
Throughput
Unhealthy Host count
You can filter on a per backend pool basis to show healthy/unhealthy hosts in a specific backend pool
References: https://docs.microsoft.com/en-us/azure/application-gateway/application-gatewaydiagnostics#Metrics

QUESTION 102
Drag and Drop Question
You have two Azure virtual machines named VM1 and VM2. VM1 has a single data disk named Disk1.
You need to attach Disk1 to VM2. The solution must minimize downtime for both virtual machines.
Which four 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.



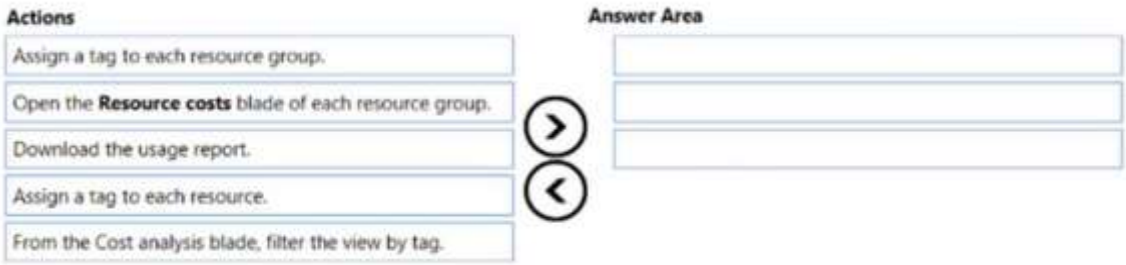
Answer:



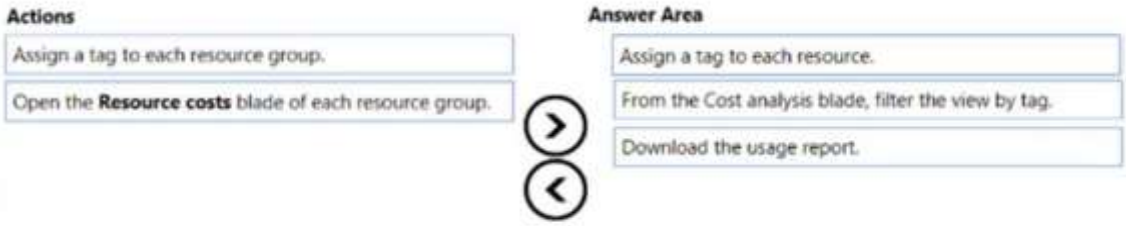
Explanation:
Step 1: Stop VM1.
Step 2: Detach Disk1 from VM1.
Step 3: Start VM1.
Detach a data disk using the portal
In the left menu, select Virtual Machines.
Select the virtual machine that has the data disk you want to detach and click Stop to deallocate the VM.
In the virtual machine pane, select Disks.
At the top of the Disks pane, select Edit.
In the Disks pane, to the far right of the data disk that you would like to detach, click the Detach button image detach

button.
After the disk has been removed, click Save on the top of the pane. In the virtual machine pane, click Overview and then click the Start button at the top of the pane to restart the VM.
The disk stays in storage but is no longer attached to a virtual machine.
Step 4: Attach Disk1 to VM2
Attach an existing disk
Follow these steps to reattach an existing available data disk to a running VM. Select a running VM for which you want to reattach a data disk.
From the menu on the left, select Disks.
Select Attach existing to attach an available data disk to the VM.
From the Attach existing disk pane, select OK.
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/detach-disk
https://docs.microsoft.com/en-us/azure/lab-services/devtest-lab-attach-detach-data-disk

QUESTION 103
Drag and Drop Question
You have an Azure subscription that is used by four departments in your company.
The subscription contains 10 resource groups. Each department uses resources in several resource groups.
You need to send a report to the finance department.
The report must detail the costs for each department.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:
Box 1: Assign a tag to each resource.
You apply tags to your Azure resources giving metadata to logically organize them into a taxonomy. After you apply tags, you can retrieve all the resources in your subscription with that tag name and value. Each resource or resource group can have a maximum of 15 tag name/value pairs. Tags applied to the resource group are not inherited by the resources in that resource group.
Box 2: From the Cost analysis blade, filter the view by tag After you get your services running, regularly check how much they're costing you. You can see the current spend and burn rate in Azure portal.
Visit the Subscriptions blade in Azure portal and select a subscription. You should see the cost breakdown and burn rate in the popup blade. Click Cost analysis in the list to the left to see the cost breakdown by resource. Wait 24 hours after you add a service for the data to populate.
You can filter by different properties like tags, resource group, and timespan. Click Apply to confirm the filters and Download if you want to export the view to a Comma-Separated Values (.csv) file.
Box 3: Download the usage report
References:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags
https://docs.microsoft.com/en-us/azure/billing/billing-getting-started

QUESTION 104
Hotspot Question
You have a virtual network named VNet1 that has the configuration shown in the following exhibit.

```
PS C:\> Get-AzureRmVirtualNetwork -Name Vnet1 -ResourceGroupName Production


Name                    : VNet1
ResourceGroupName       : Production
Location                : westus
Id                      : /subscriptions/14d26092-8e42-4ea7-b770-9dcef70fb1ea/resourceGroups/Production/providers/Micros
                          oft.Network/virtualNetworks/VNet1
Etag                    : W/"76f7edd6-d022-455b-aeae-376059318e5d"
ResourceGuid            : 562096cc-b2ba-4cc5-9619-0a735d6c34c7
ProvisioningState       : Succeeded
Tags                    :
AddressSpace            : {
                            "AddressPrefixes": [
                              "10.2.0.0/16"
                            ]
                          }
DhcpOptions             : {}
Subnets                 : [
                            {
                              "Name": "default",
                              "Etag": "W/\"76f7edd6-d022-455b-aeae-376059318e5d\"",
                              "Id": "/subscriptions/14d26092-8e42-4ea7-b770-9dcef70fb1ea/resourceGroups/Production/provi
                          ders/Microsoft.Network/virtualNetworks/VNet1/subnets/default",
                              "AddressPrefix": "10.2.0.0/24",
                              "IpConfigurations": [],
                              "ResourceNavigationLinks": [],
                              "ServiceEndpoints": [],
                              "ProvisioningState": "Succeeded"
                            }
                          ]
VirtualNetworkPeerings  : []
EnableDDoSProtection    : false
EnableVmProtection      : false
```

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

Before a virtual machine on VNet1 can receive an IP address from 192.168.1.0/24, you must first **[answer choice]**.

- add a network interface
- add a subnet
- add an address space
- delete a subnet
- delete an address space

Before a virtual machine on VNet1 can receive an IP address from 10.2.1.0/24, you must first **[answer choice]**.

- add a network interface
- add a subnet
- add an address space
- delete a subnet
- delete an address space

Answer:

Answer Area

Before a virtual machine on VNet1 can receive an IP address from 192.168.1.0/24, you must first **[answer choice]**.

- add a network interface
- add a subnet
- add an address space
- delete a subnet
- delete an address space

Before a virtual machine on VNet1 can receive an IP address from 10.2.1.0/24, you must first **[answer choice]**.

- add a network interface
- add a subnet
- add an address space
- delete a subnet
- delete an address space

Explanation:
As 192.168.1.0/24 is outside of the configured address space of 10.2.0.0/16, the answer is to create an address space.
As 10.2.1.0/24 subnet doesn't exist (only 10.2.0.0/24) the answer is to create a subnet.

QUESTION 105
Hotspot Question
You have an Azure subscription named Subscrption1 that is associated to an Azure Active Directory (Azure AD) tenant named AAD1.
Subscription1 contains the objects in the following table:

Name	Type
Share1	Azure file share
Account1	Azure Storage account
RG1	Resource group
Vault1	Recovery Services vault

You plan to create a single backup policy for Vault1. To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

You can create an Azure backup policy for:

- AAD1 only
- Account1 only
- RG1 only
- Share1 only
- AAD1 and Share1 only
- AAD1, Share1 and Account1 only
- AAD1, Share1, Account1, and RG1

In the backup policy that you create, you can configure the backups to be retained for up to:

- 7 days
- 31 days
- 90 days
- 120 days
- 365 days
- 99 years

Answer:

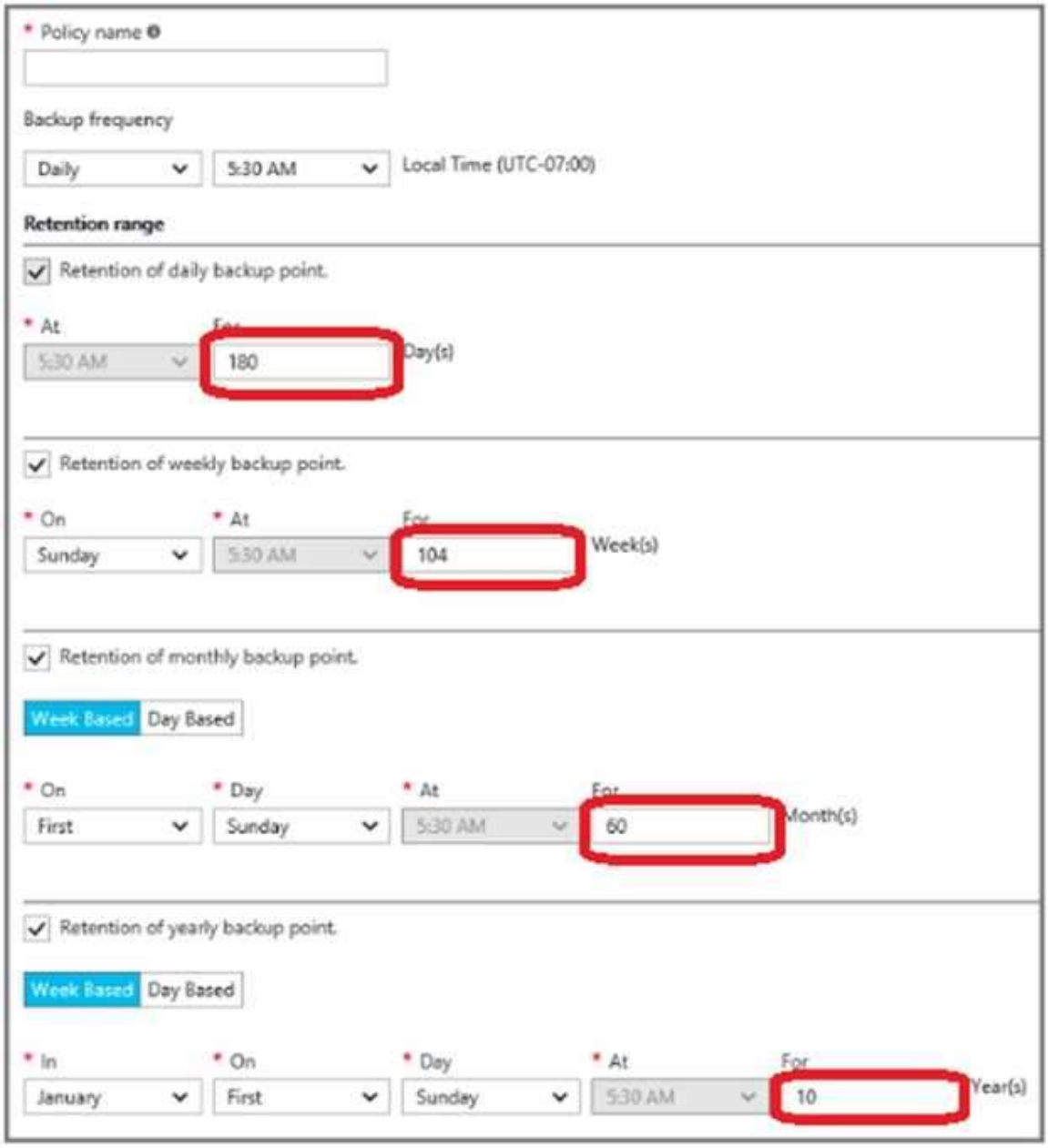
You can create an Azure backup policy for:

- AAD1 only
- Account1 only
- RG1 only
- Share1 only
- AAD1 and Share1 only
- AAD1, Share1 and Account1 only
- AAD1, Share1, Account1, and RG1

In the backup policy that you create, you can configure the backups to be retained for up to:

- 7 days
- 31 days
- 90 days
- 120 days
- 365 days
- 99 years

Explanation:
Box 1: Share1 only
Azure Backup policies can only back up an Azure VM, SQL in an Azure VM or File Share. As such the answer to the first part should be Share1 only.
Box 2: 99 years
With the latest update to Azure Backup, customers can retain their data for up to 99 years in Azure.
Note: A backup policy defines a matrix of when the data snapshots are taken, and how long those snapshots are retained.
The backup policy interface looks like this:



References: https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-first-look-arm#defining-a-backup-policy https://blogs.microsoft.com/firehose/2015/02/16/february-update-to-azure-backup-includes-data-retention-up-to-99-years-offline-backup-and-more/

QUESTION 106

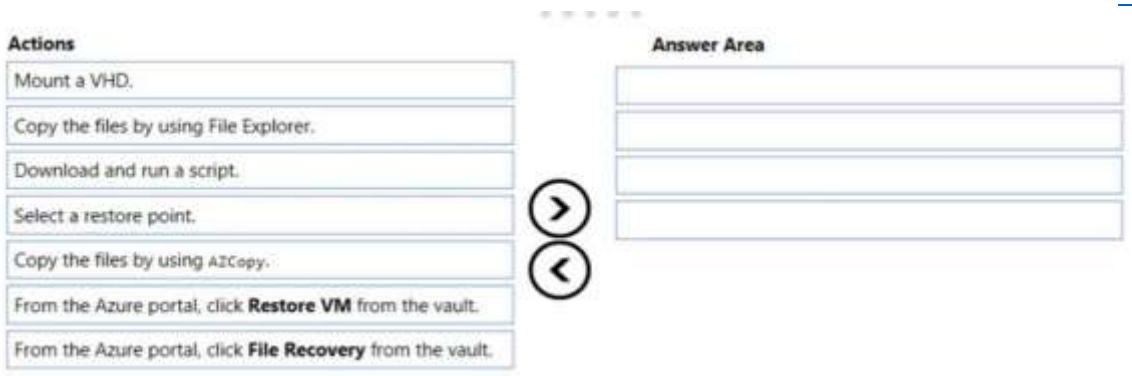
Drag and Drop Question

You have an Azure Linux virtual machine that is protected by Azure Backup.

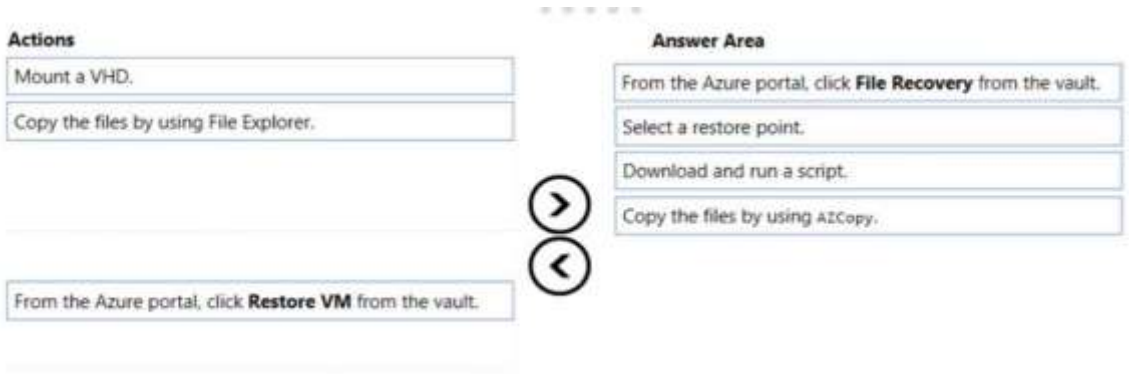
One week ago, two files were deleted from the virtual machine.

You need to restore the deleted files to an on-premises computer as quickly as possible.

Which four 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.



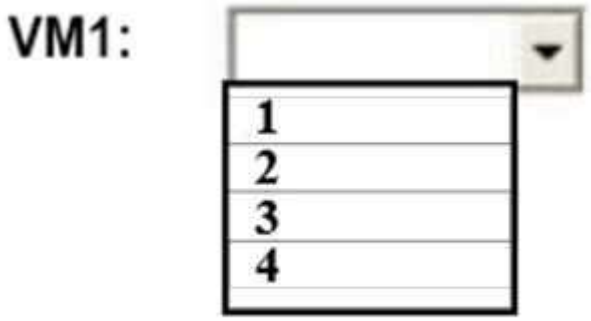
Answer:

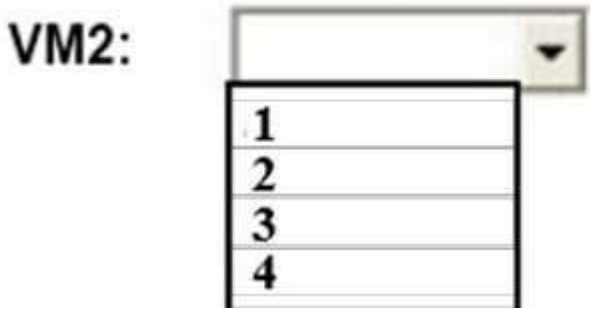


Explanation:
To restore files or folders from the recovery point, go to the virtual machine and choose the desired recovery point.
Step 0. In the virtual machine's menu, click Backup to open the Backup dashboard. Step 1. In the Backup dashboard menu, click File Recovery.
Step 2. From the Select recovery point drop-down menu, select the recovery point that holds the files you want. By default, the latest recovery point is already selected.
Step 3: To download the software used to copy files from the recovery point, click Download Executable (for Windows Azure VM) or Download Script (for Linux Azure VM, a python script is generated).
Step 4: Copy the files by using AzCopy
AzCopy is a command-line utility designed for copying data to/from Microsoft Azure Blob, File, and Table storage, using simple commands designed for optimal performance.
You can copy data between a file system and a storage account, or between storage accounts.
References:
https://docs.microsoft.com/en-us/azure/backup/backup-azure-restore-files-from-vm
https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy

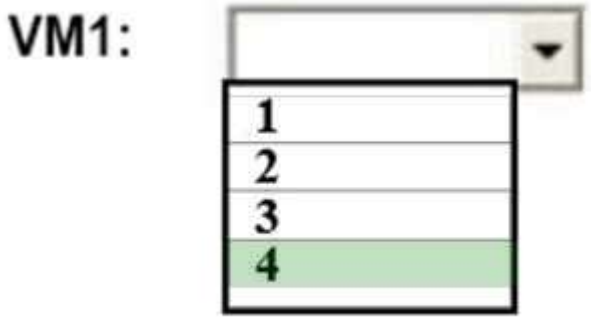
QUESTION 107
Hotspot Question
You have an Azure Migrate project that has the following assessment properties:
```
Target location: East US
Storage redundancy: Locally redundant.
Comfort factor: 2.0
Performance history: 1 month
Percentile utilization: 95th
Pricing tier: Standard
Offer: Pay as you go
```
You discover the following two virtual machines:
```
A virtual machine named VM1 that runs Windows Server 2016 and has 10 CPU cores at 20 percent utilization
A virtual machine named VM2 that runs Windows Server 2012 and has four CPU cores at 50 percent utilization
```
How many CPU cores will Azure Migrate recommend for each virtual machine? To answer, select the appropriate options in the answer area.

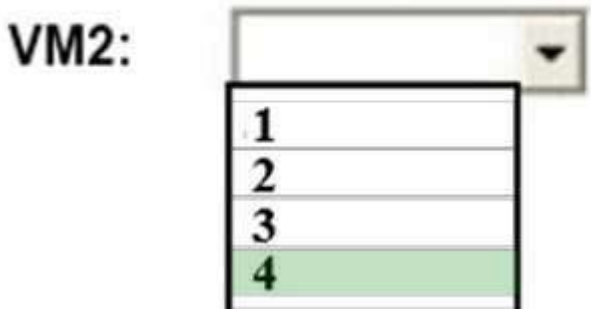
NOTE: Each correct selection is worth one point.





Answer:





Explanation:
Box 2: 4

4 *0.50 * 0.95* 2 = 3.8
Note: The number of cores in the machines must be equal to or less than the maximum number of cores (128 cores) supported for an Azure VM.
If performance history is available, Azure Migrate considers the utilized cores for comparison. If a comfort factor is specified in the assessment settings, the number of utilized cores is multiplied by the comfort factor.
If there's no performance history, Azure Migrate uses the allocated cores, without applying the comfort factor.
References:
https://docs.microsoft.com/en-us/azure/migrate/concepts-assessment-calculation

QUESTION 108
Hotspot Question
You have an Azure subscription named Subscroption1.
In Subscription1, you create an alert rule named Alert1. The Alert1 action group is configured as shown in the following exhibit.

```
PS Azure:\> Get-AzureRmActionGroup

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

Alert1 alert criteria is 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.

The number of email messages that Alert1 will send in an hour is **[answer choice]**.

- 0
- 4
- 6
- 12
- 60

The number of SMS messages that Alert1 will send in an hour is **[answer choice]**.

- 0
- 4
- 6
- 12
- 60

Answer:

The number of email messages that Alert1 will send in an hour is **[answer choice].**

- 0
- 4
- 6
- 12
- 60

The number of SMS messages that Alert1 will send in an hour is **[answer choice].**

- 0
- 4
- 6
- 12
- 60

Explanation:
Box 1: 60
One alert per minute will trigger one email per minute.
Box 2: 12
No more than 1 SMS every 5 minutes can be send, which equals 12 per hour. Note: Rate limiting is a suspension of notifications that occurs when too many are sent to a particular phone number, email address or device. Rate limiting ensures that alerts are manageable and actionable.
The rate limit thresholds are:
SMS: No more than 1 SMS every 5 minutes.
Voice: No more than 1 Voice call every 5 minutes.
Email: No more than 100 emails in an hour.
Other actions are not rate limited.
References:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/monitoring-and- diagnostics/monitoring-overview-alerts.md

QUESTION 109
Hotspot Question
You have an Azure subscription named Subscription1.
You have a virtualization environment that contains the virtualization servers in the following table.

Name	Hypervisor	Run virtual machine
Server1	Hyper-V	VM1, VM2, VM3
Server2	VMWare	VMA, VMB, VMC

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

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

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

Virtual machines that can be migrated from Server1:

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

Virtual machines that can be migrated from Server2:

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

Answer:

Virtual machines that can be migrated from Server1:

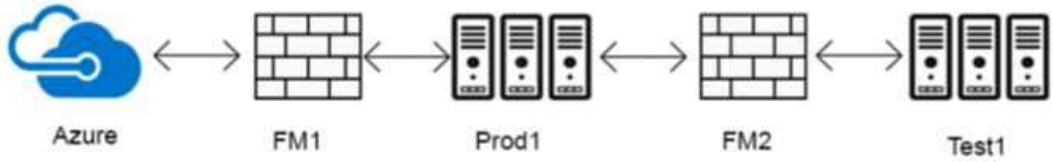
- VM1
- VM2
- VM3
- VM1 and VM2 only
- VM1 and VM3 only
- VM1 and VM2 and VM3

Virtual machines that can be migrated from Server2:

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

Explanation:
Box 1: VM3
Not VM1 as Bitlocker is not supported. BitLocker must be disabled before you enable replication for a VM.
Not VM2 as maximum Operating system disk size for a generation VM is 2,048 GB.
Box 2: VMA and VMB only
Not VMC as the max data disk size is 4,095 GB
References:
https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-support-matrix
https://docs.microsoft.com/en-us/azure/site-recovery/vmware-physical-azure-support-matrix#azure-vm-requirements

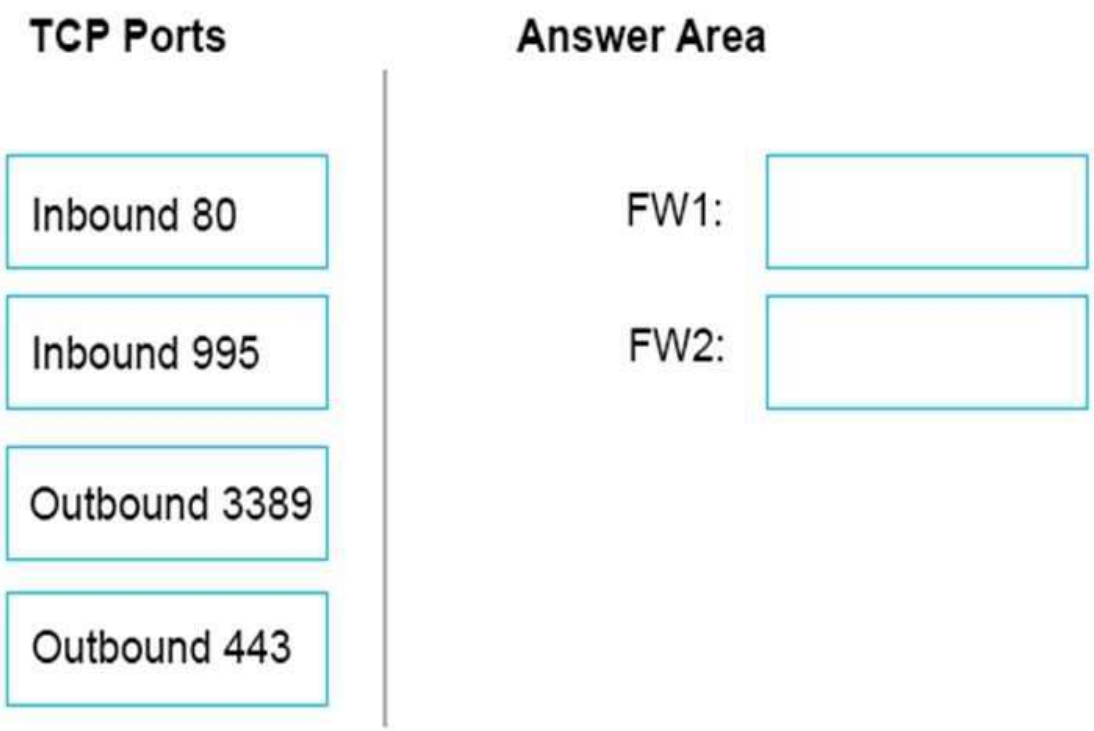
QUESTION 110
Drag and Drop Question
Your network is configured as shown in the following exhibit.



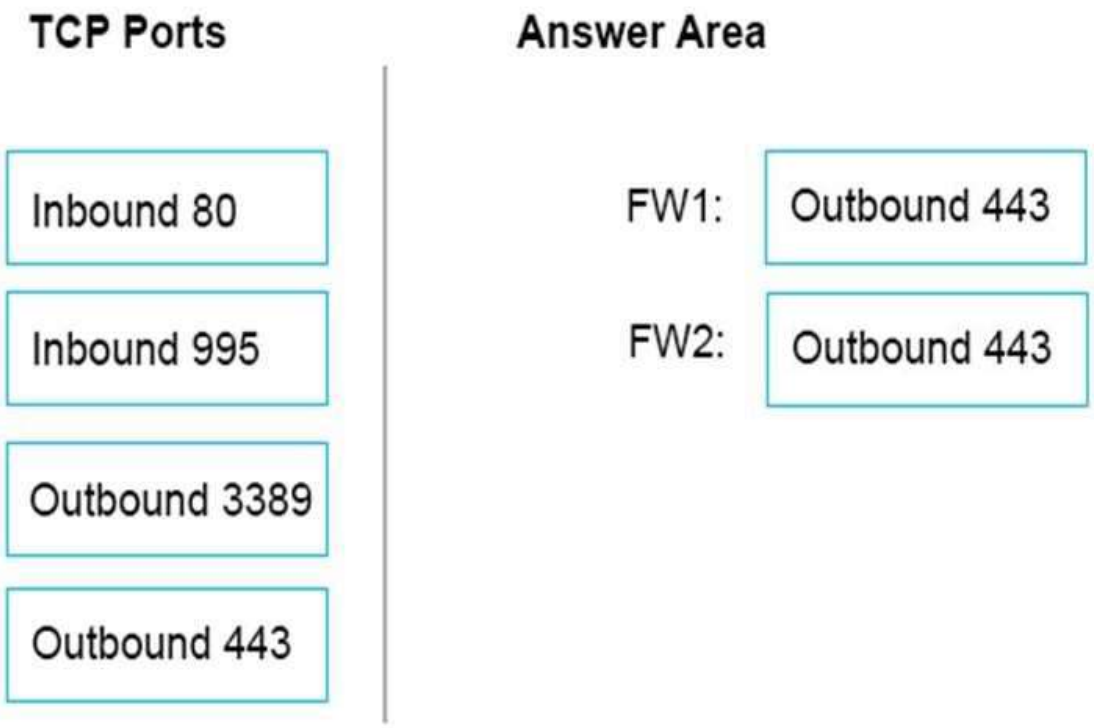
The firewalls are configured as shown in the following table.

Allowed port name	Inbound (TCP)	Outbound (TCP)
FW1	993, 3389	80, 993
FM2	443, 995, 3389	80, 995

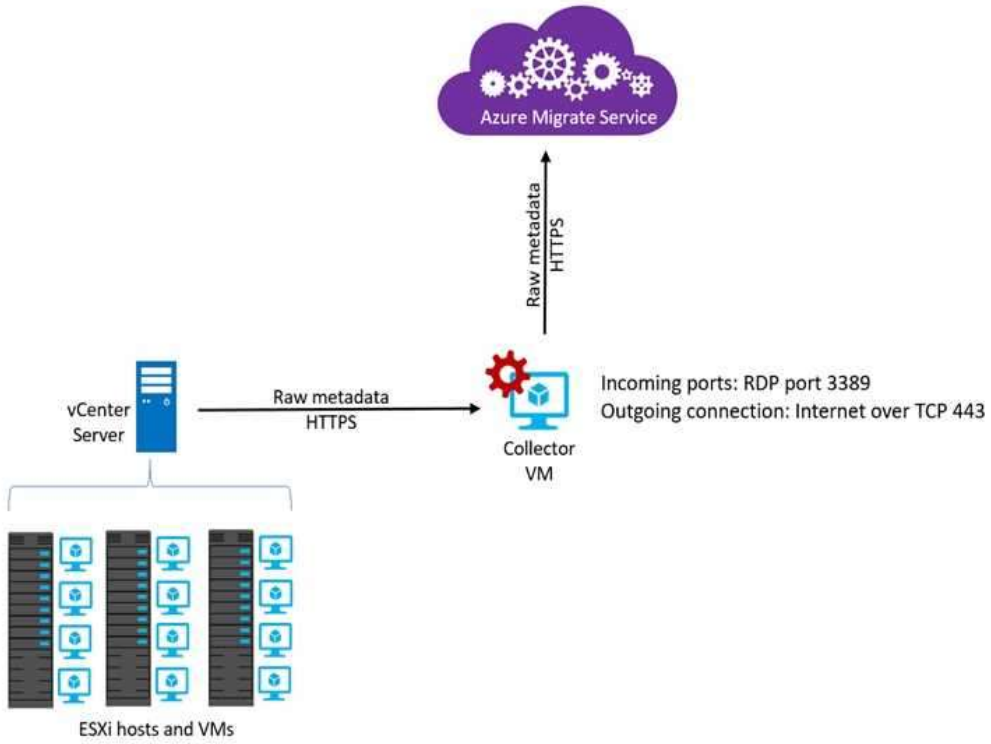
Prod1 contains a vCenter server.
You install an Azure Migrate Collector on Test1.
You need to discover the virtual machines.
Which TCP port should be allowed on each firewall? To answer, drag the appropriate ports to the correct firewalls. Each port may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:

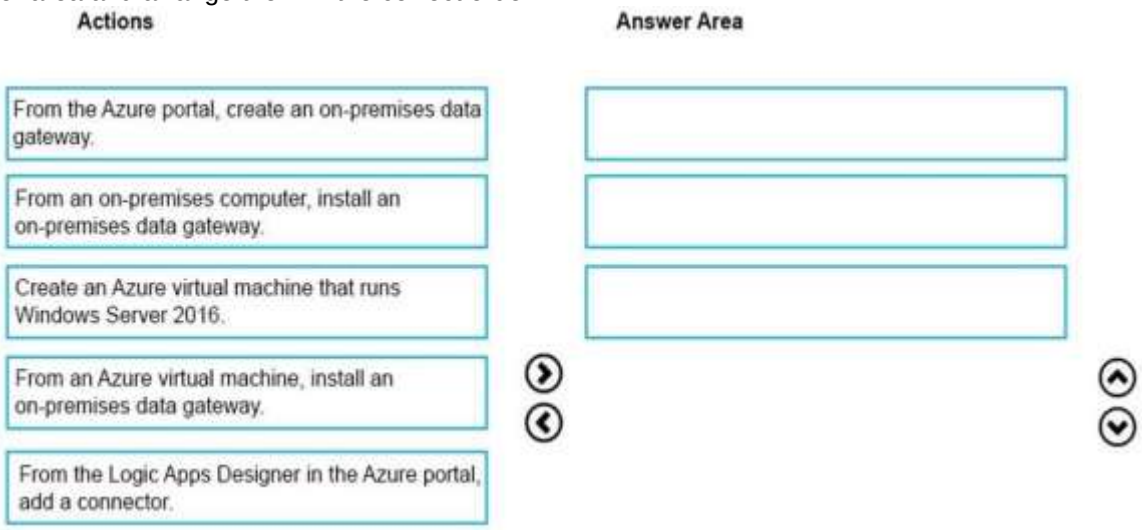


Explanation:
FW1: Outbound 443
Collector communicates with Azure Migrate service over SSL 443.
FW2: Outbound 443
The Collector must be able to communicate with the vCenter Server. By default, it connects to vCenter on 443.
Note: The collector communicates as summarized in the following diagram.

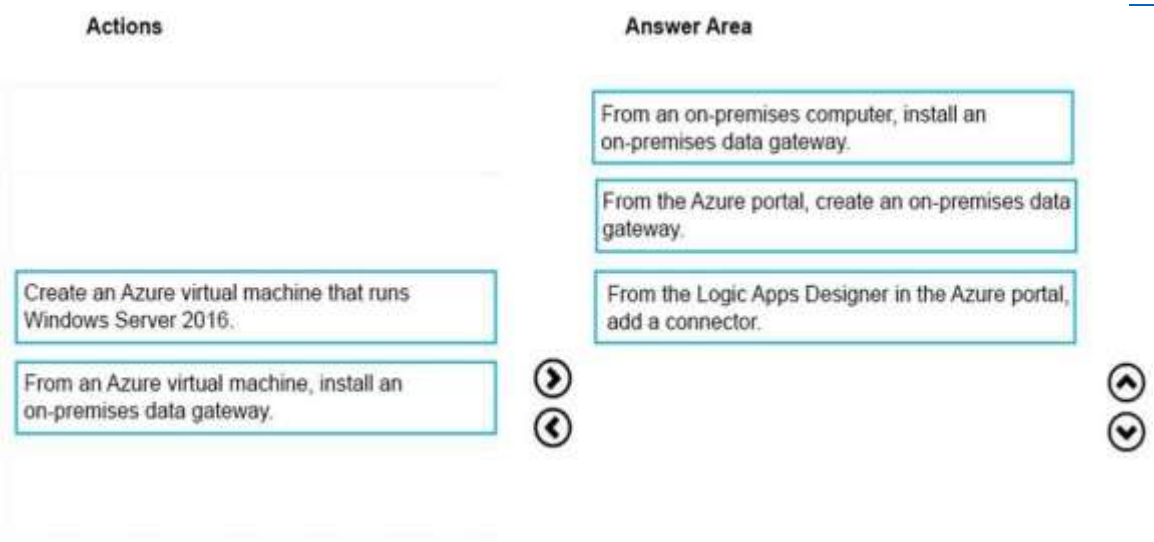


References:
https://docs.microsoft.com/en-us/azure/migrate/concepts-collector

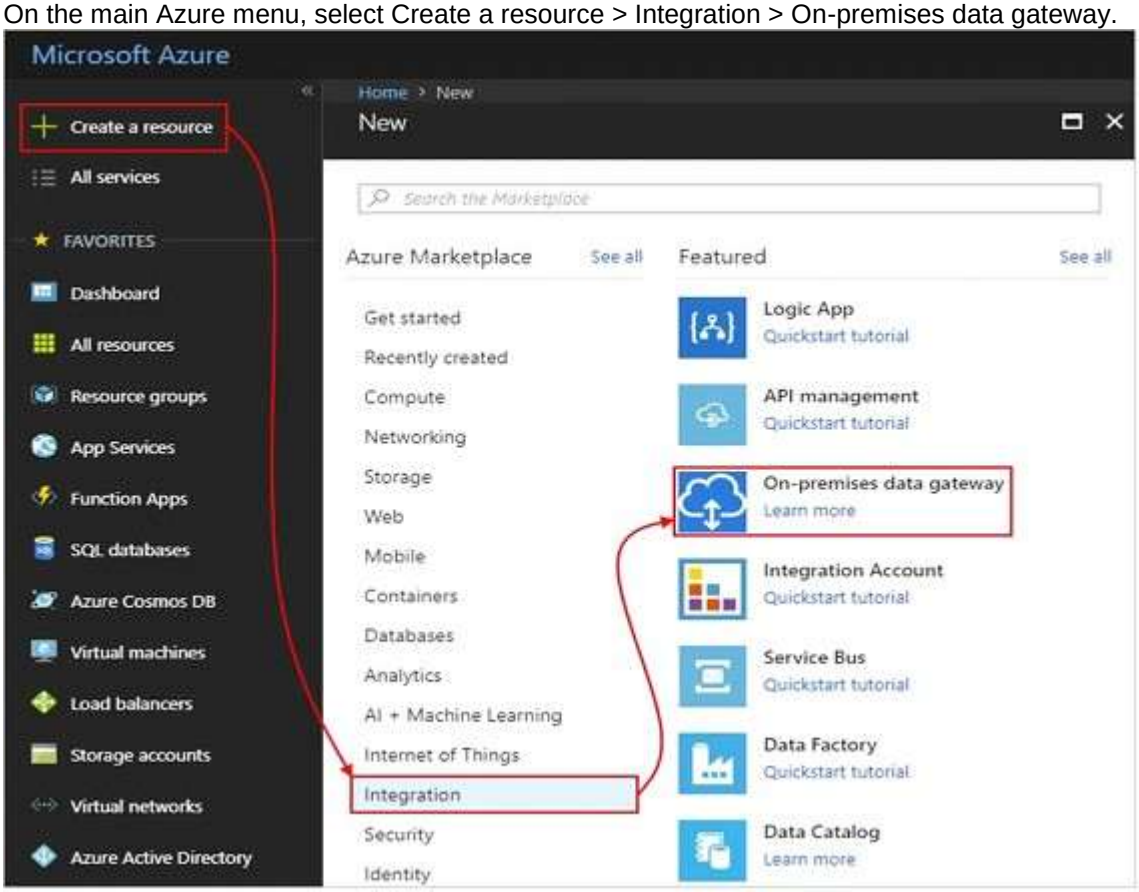
QUESTION 111
Drag and Drop Question
You have an on-premises network that includes a Microsoft SQL Server instance named SQL1.
You create an Azure Logic App named App1.
You need to ensure that App1 can query a database on SQL1.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:
To access data sources on premises from your logic apps, you can create a data gateway resource in Azure so that your logic apps can use the on-premises connectors. Box 1: From an on-premises computer, install an on-premises data gateway. Before you can connect to on-premises data sources from Azure Logic Apps, download and install the on-premises data gateway on a local computer.
Box 2: From the Azure portal, create an on-premises data gateway Create Azure resource for gateway
After you install the gateway on a local computer, you can then create an Azure resource for your gateway. This step also associates your gateway resource with your Azure subscription. Sign in to the Azure portal. Make sure you use the same Azure work or school email address used to install the gateway.
On the main Azure menu, select Create a resource > Integration > On-premises data gateway.



On the Create connection gateway page, provide this information for your gateway resource. To add the gateway resource to your Azure dashboard, select Pin to dashboard. When you're done, choose Create.
Box 3: From the Logic Apps Designer in the Azure portal, add a connector After you create your gateway resource and

associate your Azure subscription with this resource, you can now create a connection between your logic app and your on-premises data source by using the gateway.
In the Azure portal, create or open your logic app in the Logic App Designer. Add a connector that supports on-premises connections, for example, SQL Server.
Set up your connection.
References:
https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-gateway-connection

QUESTION 112
Hotspot Question
You configure the multi-factor authentication status for three users as shown in the following table.

User name	Multi-factor authentication status
Admin1@contoso.com	Disabled
Admin2@contoso.com	Enforced
Admin3@contoso.com	Enabled

You create a group named Group1 and add Admin1, Admin2, and Admin3 to the group.
For all cloud apps, you create a conditional access policy that includes Group1. The policy requires multi-factor authentication.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
Admin1 must use multi-factor authentication to sign in to the Azure portal by using a web browser.	○	○
Admin2 must use multi-factor authentication to sign in to the Azure portal by using a web browser.	○	○
Admin3 must use multi-factor authentication to sign in to the Azure portal by using a web browser.	○	○

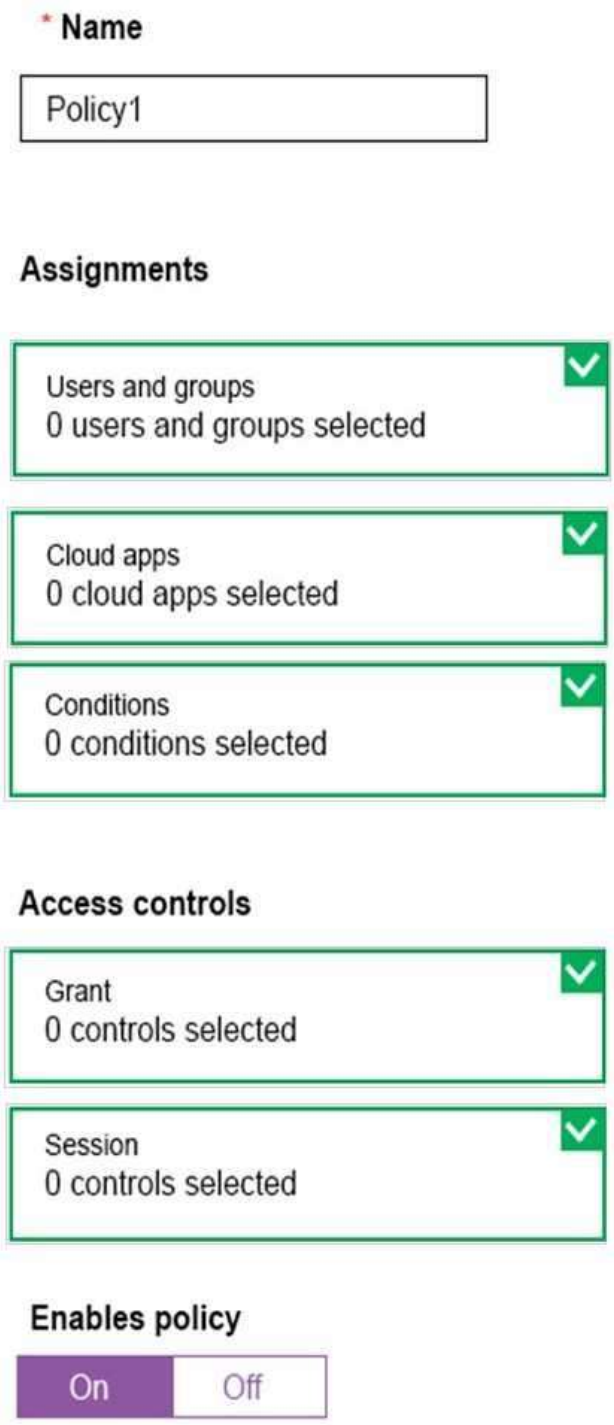
Answer:

Statements	Yes	No
Admin1 must use multi-factor authentication to sign in to the Azure portal by using a web browser.	○	○
Admin2 must use multi-factor authentication to sign in to the Azure portal by using a web browser.	○	○
Admin3 must use multi-factor authentication to sign in to the Azure portal by using a web browser.	○	○

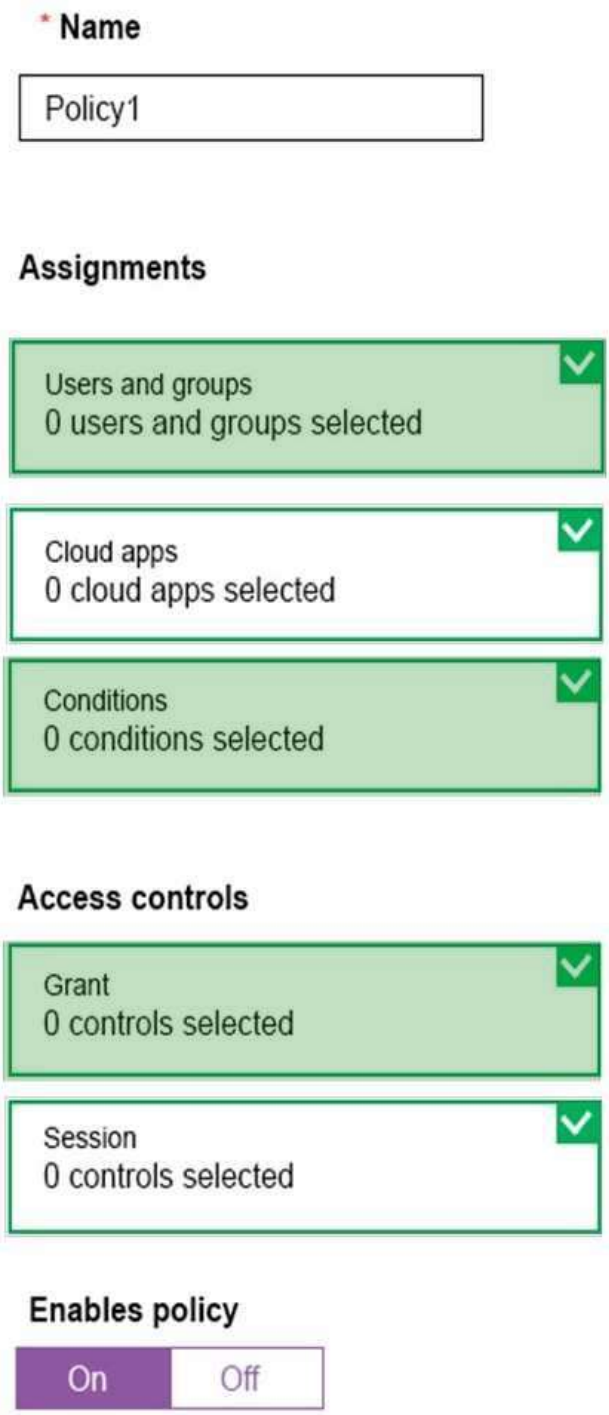
Explanation:
Box 1: No
Disabled is the default state for a new user not enrolled in Azure MFA.
Box 2: Yes
Enforced: The user has been enrolled and has completed the registration process for Azure MFA.
Web browser apps require login in this case.
Box 3: Yes
Enabled: The user has been enrolled in Azure MFA, but has not registered. They receive a prompt to register the next

time they sign in.
Web browser apps require login in this case.
References:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

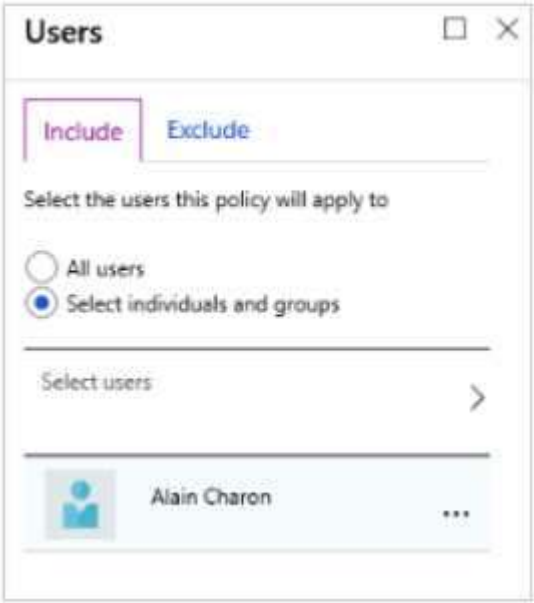
QUESTION 113
Hotspot Question
You have an Azure Active Directory (Azure AD) tenant.
You need to create a conditional access policy that requires all users to use multi-factor authentication when they access the Azure portal.
Which three settings should you configure? To answer, select the appropriate settings in the answer area.



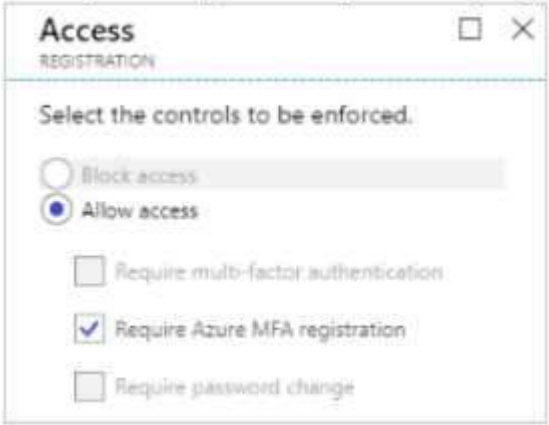
Answer:



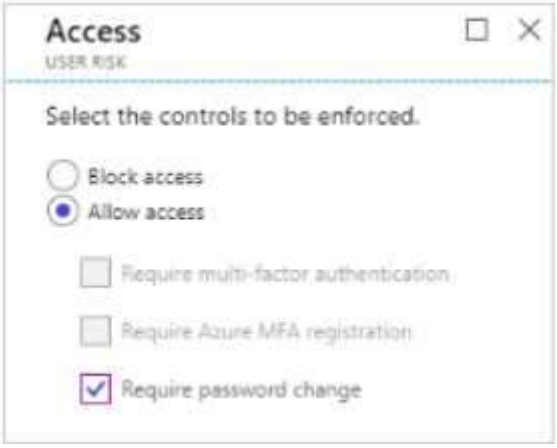
Explanation:
Box 1: Assignments, Users and Groups
When you configure the sign-in risk policy, you need to set:
The users and groups the policy applies to: Select Individuals and Groups



Box 2:
When you configure the sign-in risk policy, you need to set the type of access you want to be enforced.



Box 3:
When you configure the sign-in risk policy, you need to set:
The type of access you want to be enforced when your sign-in risk level has been met:



References:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-user-risk-policy

QUESTION 114
Hotspot Question

You plan to use Azure Network Watcher to perform the following tasks:
Task1: Identify a security rule that prevents a network packet from reaching an Azure virtual machine.
Task2: Validate outbound connectivity from an Azure virtual machine to an external host.
Which feature should you use for each task? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

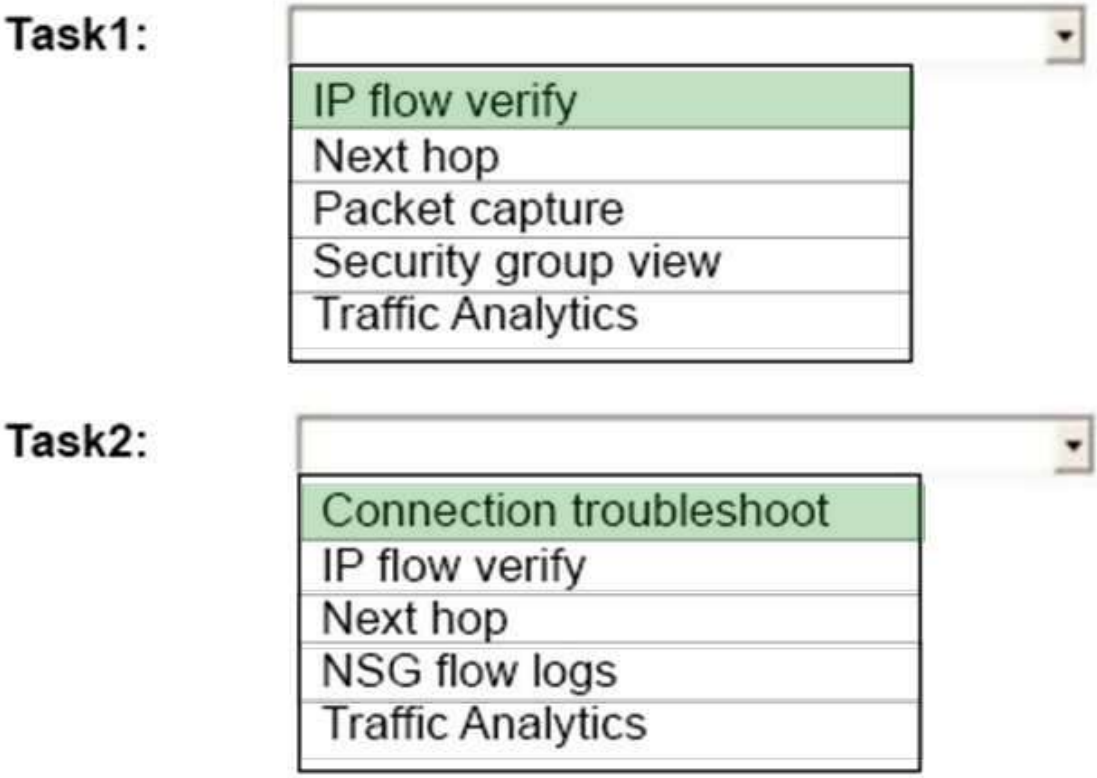
Task1:

- IP flow verify
- Next hop
- Packet capture
- Security group view
- Traffic Analytics

Task2:

- Connection troubleshoot
- IP flow verify
- Next hop
- NSG flow logs
- Traffic Analytics

Answer:



Explanation:
Task 1: IP flow verify
IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.
Task 2:
With the addition of Connection Troubleshoot, Network Watcher will see an incremental increase in its capabilities and ways for you to utilize it in your day to day operations. You can now, for example, check connectivity between source (VM) and destination (VM, URI, FQDN, IP Address).
References:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview
https://azure.microsoft.com/en-us/blog/network-watcher-connection-troubleshoot-now-generally-available/

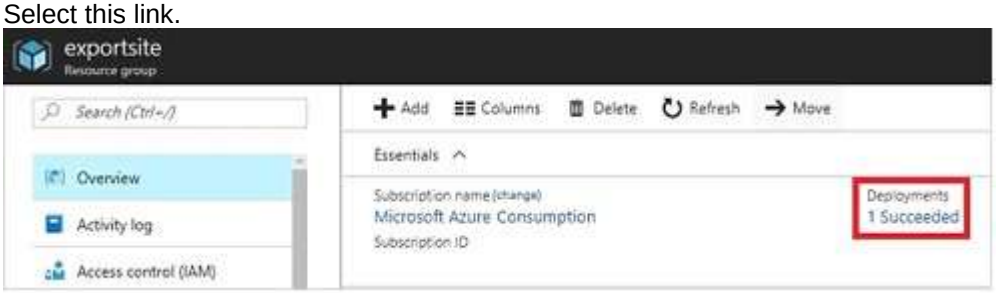
QUESTION 115
You have an Azure subscription named Subscription1 that is used be several departments at your company. Subscription1 contains the resources in the following table:

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

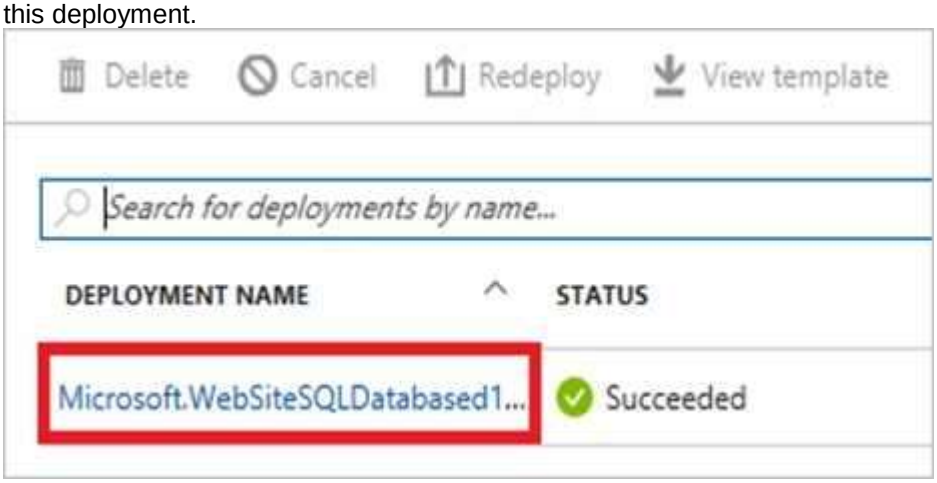
Another administrator deploys a virtual machine named VM1 and an Azure Storage account named Storage2 by using a single Azure Resource Manager template. You need to view the template used for the deployment. From which blade can you view the template that was used for the deployment?

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

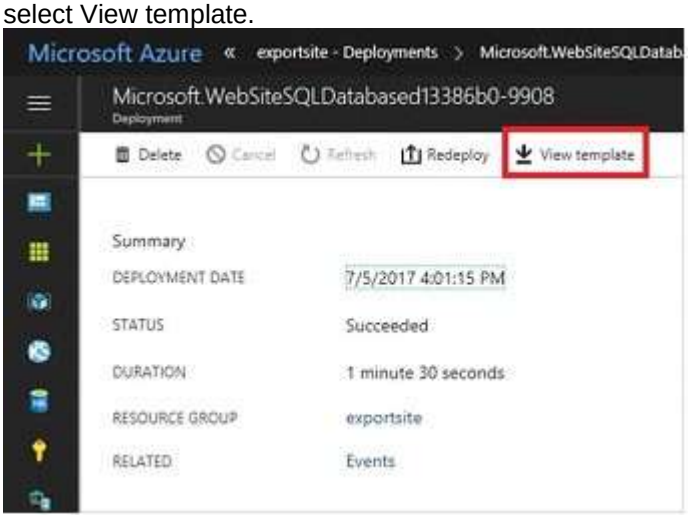
Answer: A
Explanation:
1. View template from deployment history
Go to the resource group for your new resource group. Notice that the portal shows the result of the last deployment. Select this link.



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



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



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