Question 1

You have an Azure subscription that is linked to an Azure AD tenant named contoso.onmicrosoft.com. The subscription contains the following resources:

* A virtual network named Vnet1

* An App Service plan named ASPI

* An Azure App Service named webapp1

* An Azure private DNS zone named private.contoso.com

* Virtual machines on Vnet1 that cannot communicate outside the virtual network

You need to ensure that the virtual machines on Vnet1 can access webapp1 by using a URL of https:/Avwwprivate.contosocom.

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

NOTE: Each correct selection is worth one point.

Options:

A- Create a private endpoint for webapp1.

B- Create a service endpoint for webapp1.

C- Create a CNAME record that maps www.pnvate.contoso.com to webapp1.privatelink.azurewebsites.net.

D- Create a CNAME record that maps wwwprivatemntoso.com to webapp1.contoso.onmicrosoft.com.

E- Register an enterprise application in Azure AD for webapp1.

F- Create a CNAME record that maps wow.private.contoso.com to webapp 1 private@ntoso.com.

Answer:

A, D

Question 2

Question Type: MultipleChoice

You need to use Traffic Analytics to monitor the usage of applications deployed to Azure virtual machines.

Which Azure Network Watcher feature should you implement first?

Options:

A- Connection monitor

B- Packet capture

C- NSG flow logs

D- IP flow verify

Answer:

A

Question 3

Question Type: MultipleChoice

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

RG1 contains an Azure Network Watcher instance named NW1.

You need to ensure that Admin1 can place a lock on NW1. The solution must use the principle of least privilege.

Which role should you assign to Admin1?

Options:

A- User Access Administrator

B- Network Contributor

C- Resource Policy Contributor

D- Monitoring Contributor

Answer:

B

Question 4

Question Type: MultipleChoice

You have an Azure virtual network that contains a subnet named Subnet1. Subnet1 is associated to a network security group (NSG) named NSG1. NSG1 blocks all outbound traffic that is not allowed explicitly.

Subnet1 contains virtual machines that must communicate with the Azure Cosmos DB service.

You need to create an outbound security rule in NSG1 to enable the virtual machines to connect to Azure Cosmos DB.

What should you include in the solution?

Options:

A- a service tag

B- a private endpoint

C- a subnet delegation

D- an application security group

Answer:

A

Explanation:

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

Question 5

Question Type: **MultipleChoice**

You have an Azure subscription that contains the following resources:

A virtual network named Vnet1

Two subnets named subnet1 and AzureFirewallSubnet

A public Azure Firewall named FW1

A route table named RT1 that is associated to Subnet1

A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machines were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

Options:

A- On FW1, create an outbound service tag rule for AzureCloud.

B- On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).

C- Deploy a NAT gateway.

D- To Subnetl, associate a network security group (NSG) that allows outbound access to port 1688.

Answer:

B

Explanation:

https://ryanmangansitblog.com/2020/05/11/firewall-considerations-windows-virtual-desktop-wvd/

Question 6

Question Type: **MultipleChoice**

You have a hybrid environment that uses ExpressRoute to connect an on-premises network and Azure.

You need to log the uptime and the latency of the connection periodically by using an Azure virtual machine and an on-premises virtual machine.

What should you use?

Options:

A- Azure Monitor

B- IP flow verify

C- Connection Monitor

D- Azure Internet Analyzer

Answer:

C

Explanation:

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

Question 7

Question Type: MultipleChoice

You have an Azure subscription that contains multiple virtual machines in the West US Azure region.

You need to use Traffic Analytics.

Which two resources should you create? Each correct answer presents part of the solution. (Choose two.)

NOTE: Each correct answer selection is worth one point.

Options:

A- an Azure Monitor workbook

B- a Log Analytics workspace

C- a storage account

D- an Azure Sentinel workspace

E- an Azure Monitor data collection rule

Answer:

B, C

Explanation:

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics

A storage acccount is used to store network security group flow logs.

A Log Analytics workspace is used by Traffic Analytics to store the aggregated and indexed data that is then used to generate the analytics.

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics#enable-flow-log-settings