Question 1

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Services (AWS) account.

You need to add the AWS account to Defender for Cloud.

What should you do first?

Options:

A- From the Azure portal, add the AWS enterprise application.

B- From the AWS account, enable a security hub.

C- From Defender for Cloud, configure the Security solutions settings.

D- From Defender for Cloud, configure the Environment settings.

Answer:

D

Question 2

You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.

Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 20.04.

You create a service endpoint for Microsoft. Storage in Subnet1.

You need to ensure that when you deploy Docker containers to VM1, the containers can access Azure Storage resources by using the service endpoint.

What should you do on VM1 before you deploy the container?

Options:

A- Create an application security group and a network security group (NSG).

B- Install the container network interface (CNI) plug-in.

C- Edit the docker-compose.ym1 file.

Answer:

B

Question 3

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.

You need to use the automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.

What should you create?

Options:

A- an Azure AD user

B- a secret in Azure Key Vault

C- an Azure AD group

D- a role assignment

Answer:

D

Question 4

You have an Azure subscription that is linked to an Azure AD tenant and contains the resources shown in the following table.

Name	Location	Description
Group1	Not applicable	Dynamic device security group in Azure AD
Managed1	East US	Managed identity
VM1	West US	Virtual machine that has a system-assigned managed identity
VM2	Central US	Virtual machine
App1	Not applicable	Enterprise application in Azure AD

Which resources can be assigned the Contributor role for VM1?

Options:

A- Managed1 and App1 only

B- Group1 and Managed1 only

C- Group1. Managed1, and VM2only

D- Group1, Managed1, VM1. and App1 only

Answer:

A

Question 5

Question Type: MultipleChoice

You have an Azure subscription that contains an Azure Data Lake Storage account named sa1.

You plan to deploy an app named Appl that will access sa1 and perform operations, including Read. List, Create Directory, and Delete Directory.

You need to ensure that Appl can connect securely to sa1 by using a private endpoint

What is the minimum number of private endpoints required for sa1 ?

Options:

A- 1

B- 2

C- 3

D- 4

E- 5

Answer:

A

Explanation:

A private endpoint is a network interface that connects you privately and securely to a service that's powered by Azure Private Link. By enabling a private endpoint, you're bringing the service into your virtual network. You only need one private endpoint for each service that you want to access privately, such as Azure Data Lake Storage. You can create a private endpoint for your Azure Data Lake Storage account named sa1 by following the steps inthis article.

What is a private endpoint? - Azure Private Link

Private Endpoints for Azure Storage are now Generally Available

Step-by-Step: How to Configure a Private Endpoint to Secure Azure ...

Question 6

Question Type: MultipleChoice

You have an Azure subscription that contains an Azure Key Vault Standard key vault named Vault1. Vault1 hosts a 2048-bit RSA key named key1.

You need to ensure that key1 is rotated every 90 days.

What should you do first?

Options:

A- Create a key rotation policy.

B- Modify the Access policies settings of Vault1.

C- Upgrade Vault1 to Key Vault Premium.

D- Recreate key1 as an EC key.

Answer:

A