



Free Questions for [NSE7_PBC-7.2](#) by [dumpshq](#)

Shared by [Conner](#) on [24-05-2024](#)

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

Question Type: MultipleChoice

An administrator would like to keep track of sensitive data files located in the Amazon Web Services (AWS) S3 bucket and protect it from malware. Which Fortinet product or feature should the administrator use?

Options:

- A- FortiCNP application control policies
- B- FortiCNP web sensitive polices
- C- FortiCNP DLP policies
- D- FortiCNP compliance scanning policies

Answer:

C

Explanation:

To keep track of sensitive data files located in AWS S3 buckets and protect them from malware, the administrator should use:

C) FortiCNP DLP policies.

Data Loss Prevention (DLP): DLP policies are designed to detect and prevent unauthorized access or sharing of sensitive data. In the context of AWS S3, DLP policies can be used to scan for sensitive information stored in S3 objects and enforce protective measures to prevent data exfiltration or compromise.

FortiCNP Integration: FortiCNP is Fortinet's cloud-native protection platform that offers security and compliance solutions across cloud environments. By applying DLP policies within FortiCNP, the administrator can ensure sensitive data within S3 is monitored and protected consistently.

Question 2

Question Type: MultipleChoice

You are configuring the failover settings on a FortiGate active-passive SDN connector solution in Microsoft Azure. Which two mandatory settings are required after the initial deployment? (Choose two)

Options:

A- Subscription-id

- B-** FortiGate license file
- C-** Active FortiGate serial number
- D-** Resource group name

Answer:

A, D

Explanation:

For configuring the failover settings on a FortiGate active-passive SDN connector solution in Microsoft Azure, the two mandatory settings required after the initial deployment are:

A) Subscription-id

D) Resource group name

Subscription ID: This is a unique identifier for your Azure subscription under which all resources are created and billed. FortiGate needs this to interact with the Azure resources associated with that subscription.

Resource Group Name: A resource group in Azure is a container that holds related resources for an Azure solution. The SDN connector requires the resource group name to correctly identify and manage the resources it should control, especially in a failover scenario.

Question 3

Question Type: MultipleChoice

An administrator decides to use the Use managed identity option on the FortiGate SDN connector with Microsoft Azure. However, the SDN connector is failing on the connection. What must the administrator do to correct this issue?

Options:

- A- Make sure to add the Tenant ID on FortiGate side of the configuration
- B- Make sure to set the type to system managed identity on FortiGate SDN connector settings
- C- Make sure to enable the system assigned managed identity on Azure
- D- Make sure to add the Client secret on FortiGate side of the configuration

Answer:

C

Explanation:

When an administrator decides to use the 'Use managed identity' option for the FortiGate SDN connector with Microsoft Azure and faces a connection failure, the correct action to take is:

C) Make sure to enable the system assigned managed identity on Azure.

Managed Identity Configuration: The system assigned managed identity is a feature in Azure that provides an identity for the Azure service instance (in this case, the FortiGate SDN connector) within Azure Active Directory and eliminates the need for credentials to be stored in the configuration.

Troubleshooting Connection Issues: If the SDN connector is failing to connect, it could be because the system assigned managed identity has not been enabled or configured properly in Azure for the FortiGate service.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.

EC2 > Instances > i-09913d2891249b13a > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-09913d2891249b13a (Staging-svr) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID


 i-09913d2891249b13a (Staging-svr)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is Staging-key.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
4. Connect to your instance using its Public IP:

 3.130.6.23

 Command copied

 `ssh -i "Staging-key.pem" ec2-user@3.130.6.23`

 **Note:** In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Users

```
Command Prompt
C:\Users\Fernando> ssh -i "Staging-key.pem" ec2-user@3.130.6.23
Warning: Identity file Staging-key.pem not accessible: No such file or direc
ec2-user@3.130.6.23: Permission denied (publickey,gssapi-keyex,gssapi-with-m
C:\Users\Fernando>
```

What could be the reason that the administrator cannot access the EC2 instance?

Options:

- A- You must elevate the permissions to access the EC2 instance
- B- You must run the `chmod 400 Staging-key.pem` command before accessing the instance.

C- There is no .pem key created on in Amazon Web Services (AWS)

D- The directory location of the .pem file is incorrect.

Answer:

D

Explanation:

The reason the administrator cannot access the EC2 instance could be:

D) The directory location of the .pem file is incorrect.

SSH Key Location: When initiating an SSH connection to an AWS EC2 instance, you must specify the private key file (.pem file) location that corresponds to the public key used when the instance was launched. The error 'Warning: Identity file Staging-key.pem not accessible: No such file or directory' indicates that the SSH client cannot find the .pem file at the specified location.

Correct File Path: The administrator needs to ensure that the path to the Staging-key.pem file is correctly specified when running the SSH command. If the file is not in the current directory from which the command is executed, the full or relative path to the file must be provided.

Question 5

Question Type: MultipleChoice

Refer to the exhibit.

The screenshot shows the 'Network settings' section of an AWS console. It includes a dropdown for VPC (vpc-0832884e2cfba2440), a dropdown for Subnet (subnet-0afdedac6fea5a8b8), a dropdown for Auto-assign public IP (Disable), and radio buttons for Firewall (security groups) (Create security group selected). To the right, a 'Summary' panel shows 'Number of instances' (1), 'Software Image (AMI)' (Amazon Linux 2023 AMI), 'Virtual server type (instance type)' (t2.micro), and 'Storage (volumes)' (1 volume(s) - 8 GiB).

Network settings [Info](#)

VPC - required [Info](#)

vpc-0832884e2cfba2440 (Terraform-VPC) 10.0.0.0/24

Subnet [Info](#)

subnet-0afdedac6fea5a8b8 terraform-subnet [Create new subnet](#)

VPC: vpc-0832884e2cfba2440 Owner: 845513257411 Availability Zone: us-east-2a
IP addresses available: 251 CIDR: 10.0.0.0/24

Auto-assign public IP [Info](#)

Disable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Summary

Number of instances

[Software Image \(AMI\)](#)

Amazon Linux 2023 AMI
ami-00c6c849418b7612c

[Virtual server type \(instance type\)](#)

t2.micro

[Firewall \(security groups\)](#)

New security group

[Storage \(volumes\)](#)

1 volume(s) - 8 GiB

You have deployed a Linux EC2 instance in Amazon Web Services (AWS) with the settings shown on the exhibit

What next step must the administrator take to access this instance from the internet?

Options:

- A- Configure the user name and password.
- B- Enable source and destination checks on the instance
- C- Enable SSH and allocate it to the device
- D- Allocate an Elastic IP address and assign it to the instance

Answer:

D

Explanation:

The next step the administrator must take to access the Linux EC2 instance from the internet is:

D) Allocate an Elastic IP address and assign it to the instance.

Elastic IP (EIP) Requirement: By default, when an EC2 instance is launched in AWS, it receives a public IP address from Amazon's pool, which is not static. This IP address can change, for example, if the instance is stopped and started again. To have a static IP address,

you need to allocate an Elastic IP (EIP), which is a persistent public IP address, and then associate it with the instance.

Public Accessibility: Without an Elastic IP, the instance may not be accessible over the internet after a reboot or stop/start sequence.

Assigning an Elastic IP ensures the instance can be accessed consistently using the same IP address.

Question 6

Question Type: MultipleChoice

Refer to the exhibit.

```
FGT-AP-SDN-Active #  
FGT-AP-SDN-Active # diagnose sniffer packet any "host 76.64.1[REDACTED].32 and p  
Using Original Sniffing Mode  
interfaces=[any]  
filters=[host 76.64.1[REDACTED].32 and port 443]  
[
```

An administrator has deployed a FortiGate VM in Amazon Web Services (AWS) and is trying to access it using its public IP address from their local computer. However, the connection is not successful and at the same time FortiGate is not receiving any HTTPS or SSH traffic.

to its external interface

What should the administrator check for possible issue?

Options:

- A- Run a debug flow to check any network ACLs
- B- Check the FortiGate firewall policies
- C- Check the FortiGate instance ID
- D- Check the inbound network security group rules

Answer:

D

Explanation:

Considering the situation where the administrator is unable to access the FortiGate VM using its public IP address and no traffic is reaching the FortiGate's external interface, the administrator should check:

D) Check the inbound network security group rules.

Network Security Group Rules: AWS uses security groups as a virtual firewall that controls inbound and outbound traffic to AWS resources such as EC2 instances. If the FortiGate VM's public interface is not receiving HTTPS or SSH traffic, it's likely because the inbound security group rules associated with that interface are not allowing access on the necessary ports (HTTPS - port 443, SSH - port 22).

Troubleshooting: The administrator should verify that the security group rules for the FortiGate VM's network interface allow inbound traffic on the specific ports used for management access. If these rules are absent or misconfigured, the intended traffic will be blocked, resulting in the inability to connect.

Question 7

Question Type: MultipleChoice

Refer to the exhibit.

```
Do you really want to destroy all resources?  
Terraform will destroy all your managed infrastructure, as shown above.  
There is no undo. Only 'yes' will be accepted to confirm.  
  
Enter a value:   
  
aws_network_interface_sg_attachment.publicattachment: Destroying... [id=sg-0  
aws_route.externalroute: Destroying... [id=r-rtb-07301520ef1fd3c5c1080289494  
aws_route_table_association.publicassociate: Destroying... [id=rtbassoc-014  
aws_network_interface_sg_attachment.internalattachment: Destroying... [id=sg  
aws_eip.FGTPublicIP: Destroying... [id=eipalloc-089e0464d18c2324d]  
aws_route_table_association.internalassociate: Destroying... [id=rtbassoc-02  
aws_route.internalroute: Destroying... [id=r-rtb-0a3d10220e4ed7b221080289494  
aws_route_table_association.publicassociate: Destruction complete after 0s  
aws_route_table_association.internalassociate: Destruction complete after 0s
```

What would be the impact of confirming to delete all the resources in Terraform?

Options:

- A- It destroys all the resources in the . tfvars file
- B- It destroys all the resources tied to the AWS Identity and Access Management (IAM) user.

C- It destroys all the resources in the resource group

D- It destroys all the resources in the state file.

Answer:

D

Explanation:

Confirming to delete all the resources in Terraform will have the following impact:

D) It destroys all the resources in the state file.

Terraform State File Role: The terraform.tfstate file contains a real-time mapping of the resources that Terraform manages, including their current configuration and relationships. This file tracks the actual state of resources provisioned by Terraform.

Impact of Destruction: When Terraform prompts for confirmation to destroy resources, and 'yes' is entered, Terraform reads the state file and systematically removes all the resources that are managed as part of that state. This is not limited to a specific .tfvars file, IAM user, or resource group---it is a global action that affects all resources tracked by the state file associated with the current Terraform workspace and configuration.

Question 8

Question Type: MultipleChoice

Refer to the exhibit.

Variables

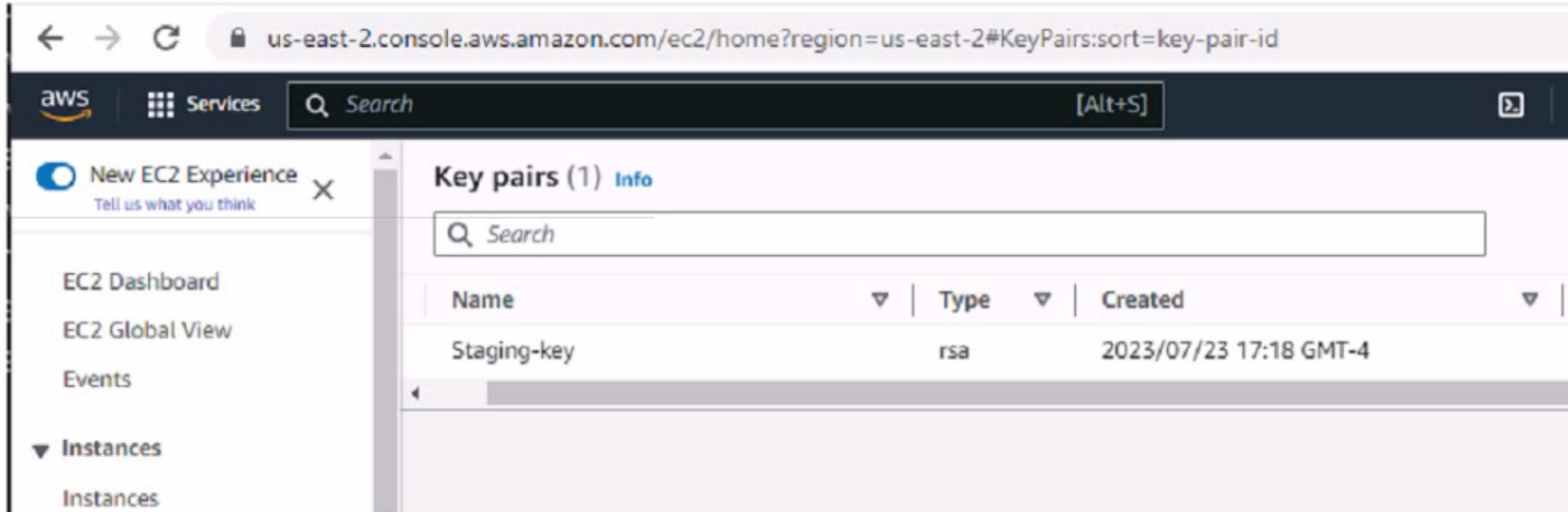
```
variable "size" {
  default = "c5n.xlarge"
}

// Existing SSH Key on the AWS
variable "keyname" {
  default = "<AWS SSH KEY>"
}

variable "adminsport" {
  default = "8443"
}

variable "bootstrap-fgtvm" {
  // Change to your own path
  type      = string
  default = "fgtvm.conf"
}
```

Dashboard-Key Pairs



The screenshot shows the AWS Management Console interface for Key Pairs in the us-east-2 region. The breadcrumb trail is "us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#KeyPairs:sort=key-pair-id". The navigation bar includes the AWS logo, "Services", a search bar, and a keyboard shortcut "[Alt+S]". A "New EC2 Experience" notification is present. The left-hand navigation menu lists "EC2 Dashboard", "EC2 Global View", "Events", "Instances", and "Instances". The main content area is titled "Key pairs (1) Info" and features a search bar. Below the search bar is a table with the following data:

Name	Type	Created
Staging-key	rsa	2023/07/23 17:18 GMT-4

What value or values must the administrator use in the SSH Key section to deploy a FortiGate VM using Terraform in Amazon Web Services (AWS)?

Options:

- A- Use the Name and ID values of the key pair
- B- Use the Name of the key pair
- C- Use the ID value of the key pair.
- D- Use the Fingerprint value of the key pair

Answer:

B

Explanation:

For deploying a FortiGate VM using Terraform in AWS, the administrator must use:

B) Use the Name of the key pair.

Terraform and AWS SSH Keys: When deploying instances in AWS using Terraform, it is required to specify the name of the SSH key pair to enable key-based authentication to the instance post-deployment.

Configuration Syntax: The variable keyname within the Terraform configuration should match the exact name of the SSH key pair as it is stored in AWS. This ensures that Terraform can reference the correct key during the deployment process to set up SSH access to the FortiGate VM.

Terraform Variables: The variable 'keyname' block in the Terraform configuration will look for the key pair name as it should be declared in the terraform.tfvars file or passed as a variable during execution. This does not require the key pair's ID or fingerprint, just its name.

To Get Premium Files for NSE7_PBC-7.2 Visit

https://www.p2pexams.com/products/nse7_pbc-7.2

For More Free Questions Visit

<https://www.p2pexams.com/fortinet/pdf/nse7-pbc-7.2>

