Download Fortinet NSE7_CDS_AR-7.6 Exam Dumps Free

Shared by Tyson on 17-06-2026

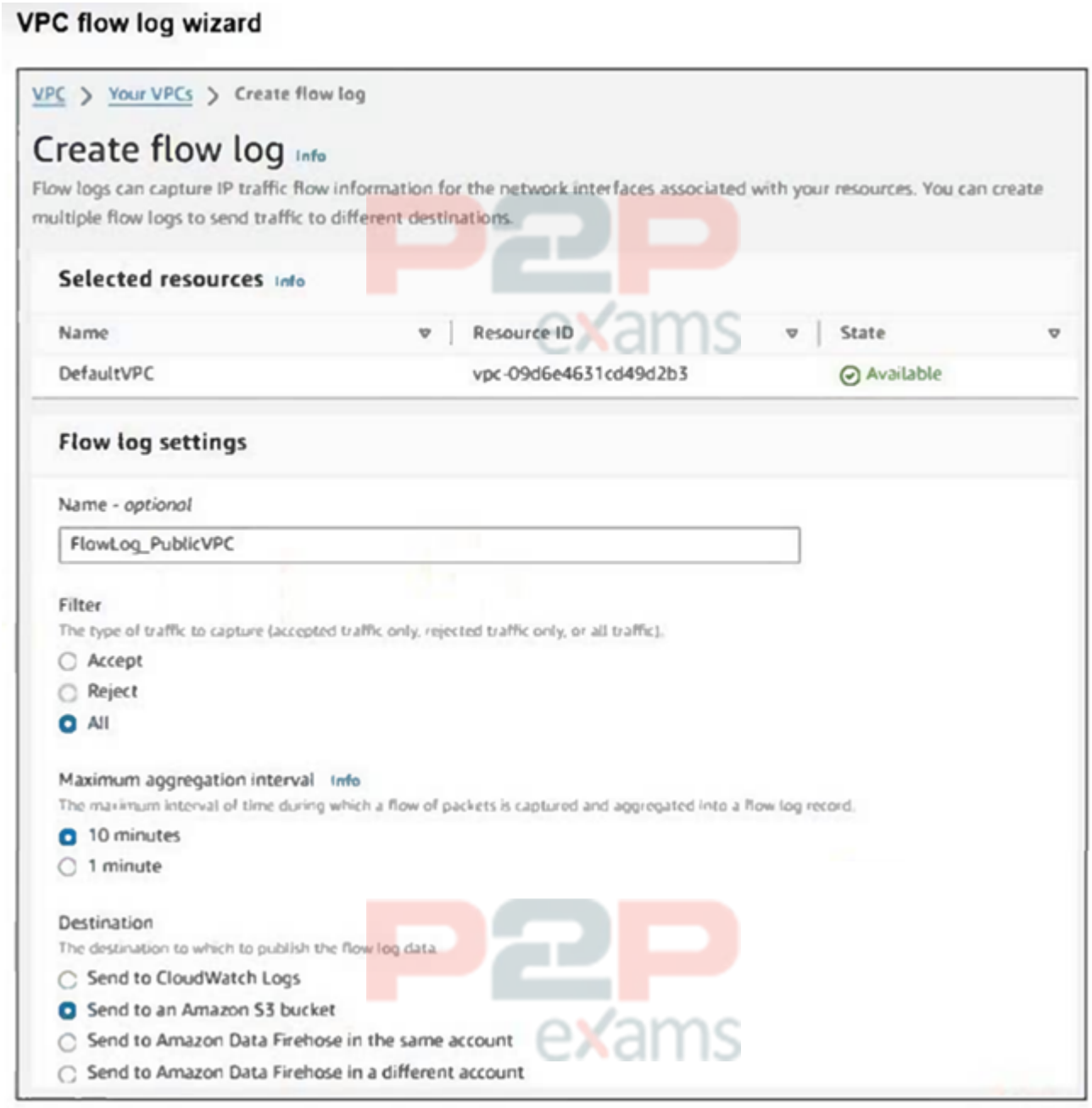
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



Your team notices an unusually high volume of traffic sourced at one of the organizations FortiGate EC2 instances. They create a flow log to obtain and analyze detailed information about this traffic. However, when they checked the log, they found that it included traffic that was not associated with the FortiGate instance in question.

What can they do to obtain the correct logs? (Choose one answer)

Options:

A- Create a new flow log at the interface level.
B- Change the maximum aggregation time to 1 minute.
C- Ensure that the flow log data is not mixed with the rest of the traffic.
D- Send the logs to Amazon Data Firehose instead to get more granular information.

Answer:

A

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

According to the FortiOS 7.6 AWS Administration Guide and the Public Cloud Security documentation regarding AWS VPC Flow Logs, the level at which a flow log is created determines the scope of the data collected:

Flow Log Scope and Hierarchy (Option A): AWS VPC Flow Logs can be created at three different levels: VPC, Subnet, or Network Interface (ENI).

As seen in the exhibit (VPC flow log wizard), the flow log is being created for the resource vpc-09d6e4631cd49d2b3. When a flow log is created at the VPC level, it captures IP traffic for all network interfaces within that VPC.

To isolate traffic specifically for a single FortiGate EC2 instance and avoid seeing traffic from other instances in the same VPC or subnet, the administrator must create a flow log at the Network Interface level. This provides the most granular visibility and ensures the logs only contain traffic associated with the specific ENIs of that FortiGate instance.

Why other options are incorrect:

Option B: Changing the maximum aggregation interval from 10 minutes to 1 minute increases the frequency of log delivery and captures shorter-lived flows more accurately, but it does not change the scope of the resources being monitored.

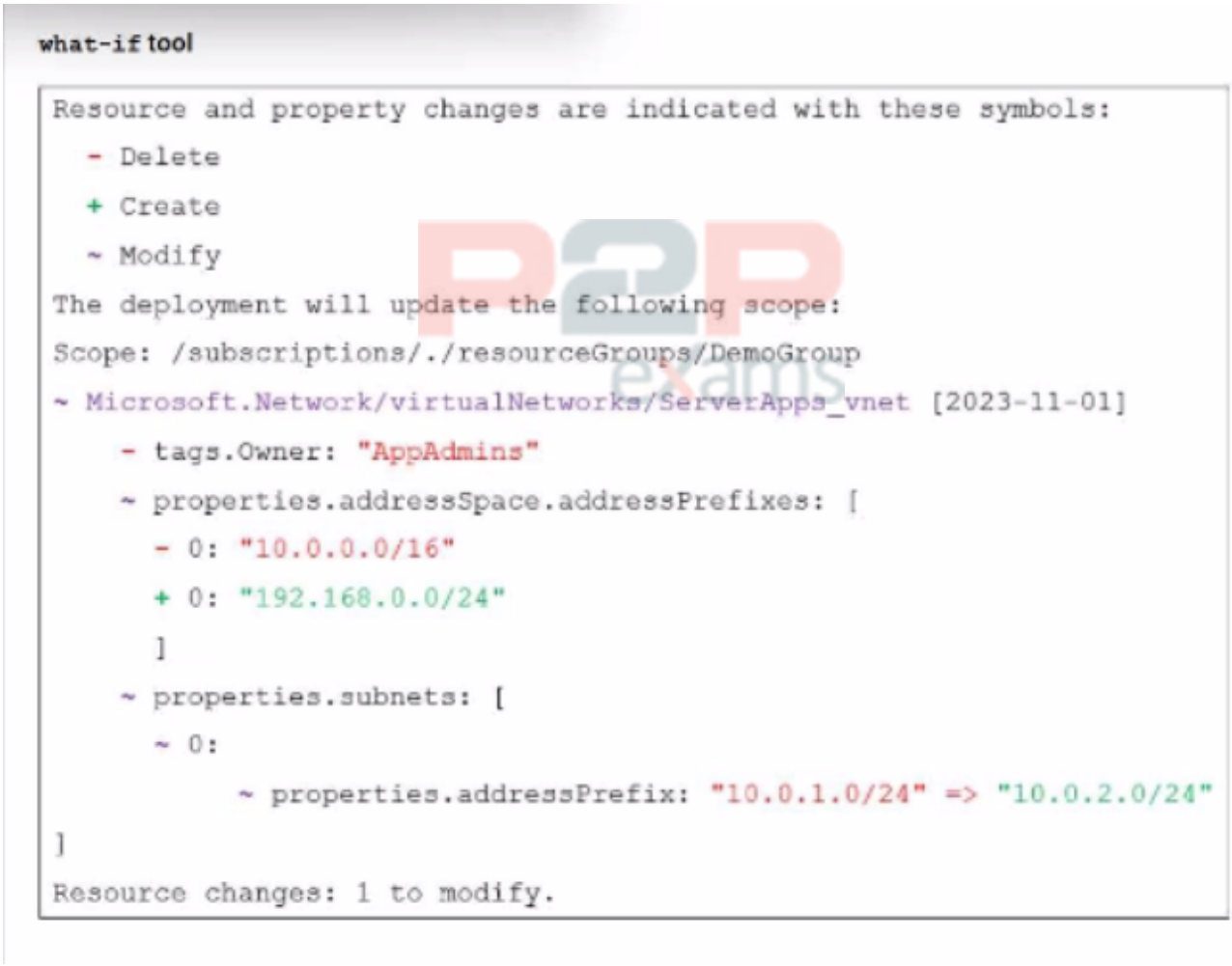
Option C: This is a general troubleshooting statement and not a configuration action within the AWS Flow Log wizard that would filter the traffic by instance.

Option D: Changing the destination to Amazon Data Firehose changes how the logs are processed and delivered (e.g., for streaming to a SIEM), but the source data is still determined by the resource level selected (VPC vs. Interface).

Question 2

Question Type: MultipleChoice

Refer to the exhibit.



An administrator used the what-if tool to preview changes to an Azure Bicep file.

What will happen if the administrator decides to apply these changes in Azure?

Options:

A- Subnet 10.0.1.0/24 will replace subnet 10.0.2.0/24.
B- This deployment will fail and no changes will be applied.
C- A new subnet will be added to ServerApps.
D- The ServerApps VNet will be renamed.

Answer:

B

Explanation:

Based on the Fortinet NSE 7 - Public Cloud Security 7.4/7.6 curriculum and Azure Resource Manager (ARM) deployment logic, the what-if tool provides a predictive analysis of infrastructure changes.

Analyzing the Modification Symbols (Option B): The exhibit shows several critical changes being attempted simultaneously on the ServerApps_vnet.

VNet Address Space Change: The symbol - (Delete) is next to the address space 10.0.0.0/16, and + (Create) is next to 192.168.0.0/24.

Subnet Modification: Further down, the symbol ~ (Modify) indicates an attempt to change the prefix of an existing subnet from 10.0.1.0/24 to 10.0.2.0/24.

Azure Deployment Constraints: According to the FortiOS 7.6 Azure Administration Guide, Azure networking has strict dependencies. You cannot delete or modify an address space that contains active subnets or resources.

Why the deployment fails: The what-if output shows the administrator is trying to remove the 10.0.0.0/16 address range. However, the existing subnet 10.0.1.0/24 is still 'resident' within that range during the transaction. Because the subnet is currently attached to the address space being deleted, Azure Resource Manager will reject the deployment as an invalid operation. The attempt to add a new 192.168.0.0/24 range does not resolve the conflict of removing the active range.

Why other options are incorrect:

Option A: The tool shows that 10.0.1.0/24 is being changed to 10.0.2.0/24, not that one is replacing the other as a new entity.

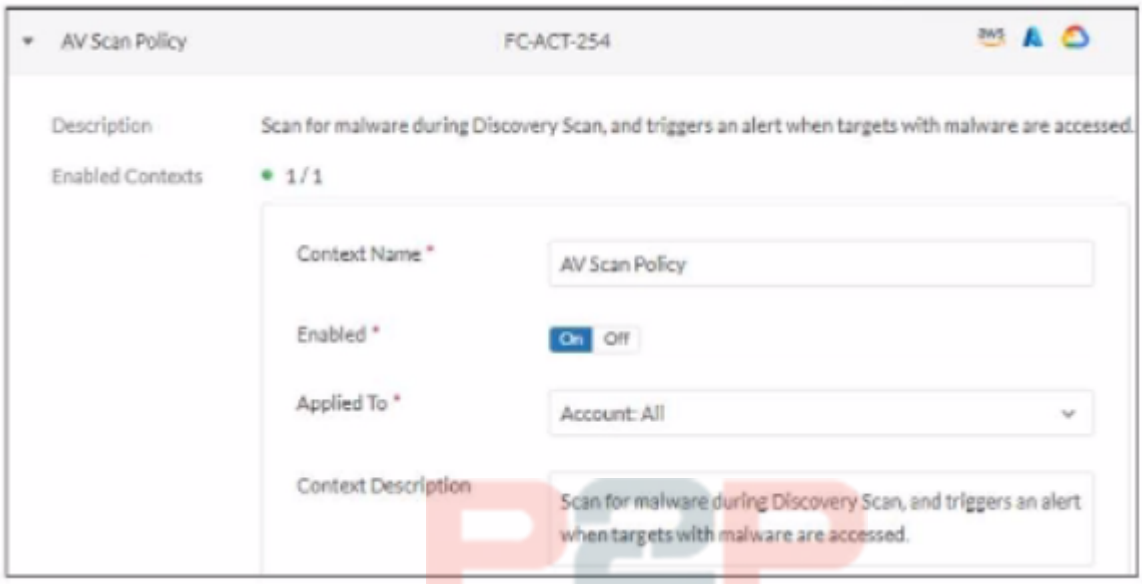
Option C: The symbols show a modification (~) of an existing subnet (index 0:), not the creation (+) of an entirely new subnet.

Option D: The VNet name ServerApps_vnet is not being changed; only its internal properties (tags, address space, and subnets) are being modified.

Question 3

Question Type: MultipleChoice

Exhibit.



In which type of FortiCNP insights can an administrator examine the findings triggered by this policy?

Options:

A- Data
B- Threat
C- Risk
D- User activity

Answer:

C

Question 4

Question Type: MultipleChoice

How does an administrator secure container environments in Amazon AWS from newly emerged security threats? (Choose one answer)

Options:

A- Using Docker-related application control signatures.
B- Using Amazon AWS-related application control signatures.
C- Using distributed network-related application control signatures.
D- Using Amazon AWS_S3-related application control signatures.

Answer:

A

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

According to the FortiOS 7.6 Docker Administration Guide and the Public Cloud Security study materials, container security is addressed through granular visibility into container-specific protocols.

Application Control for Containers (Option A): FortiOS includes a dedicated set of application control signatures specifically for Docker traffic. These signatures allow the FortiGate-VM to identify and control specific actions within a container environment, such as:

Docker_Pull.Blob / Docker_Pull.Manifest: Identifying when a container image is being pulled from a registry.

Docker_Push.Blob / Docker_Push.Manifest: Monitoring when images are uploaded to a registry.

Enforcing Security Policies: By using these Docker-related signatures, an administrator can create firewall policies that only allow container pulls from known clean, private registries while blocking traffic from unauthorized or public registries that may contain vulnerable or malicious images.5

Defense-in-Depth: While traditional network-related signatures (Option C) or AWS-specific infrastructure signatures (Option B) protect the underlying network and cloud services, they do not provide the necessary visibility into the Docker API calls and manifest transfers required to secure the container lifecycle itself. FortiGate further enhances this by scanning the actual payload of these transfers using the Intrusion Prevention Service (IPS) and Advanced Malware Protection (AMP).

Question 5

Question Type: MultipleChoice

You are using Ansible to modify the configuration of several FortiGate VMs. What is the minimum number of files you need to create, and in which file should you configure the target FortiGate IP addresses?

Options:

A- One playbook file for each target and the required tasks, and one inventory file.
B- One .yaml file with the targets IP addresses, and one playbook file with the tasks.
C- One inventory file for each target device, and one playbook file.
D- One text file for all target devices, and one playbook file.

Answer:

D

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

Based on the FortiOS 7.6 Automation Guide and the provided documentation for Ansible workflows, the following structure is required for managing multiple FortiGate nodes:

Inventory File (The Target List): The inventory is a single file that defines the list of managed nodes. It specifies critical information such as hostnames, connection details, and specifically the IP addresses of the target devices. According to the study guide, this inventory is a text file that lists all the systems you want to manage.

Playbook File (The Task List): You create and edit a separate file that acts as the playbook. This file is written in YAML format and contains the series of tasks that Ansible performs on the managed nodes to reach a desired state.

Minimum File Count: A basic Ansible workflow consists of exactly two files: one inventory file (text) and one playbook file (YAML). By listing the target IP address (e.g., 10.0.206.131) within the inventory text file, the administrator can manage the FortiGate device without needing individual files for every target.

Why other options are incorrect:

Option A & C: Creating a separate playbook or inventory file for each target is inefficient and contradicts the core Ansible workflow, which uses a single inventory to manage multiple hosts.

Option B: While the playbook is a .yaml file, the study guide specifically defines the inventory (where IP addresses are configured) as a text file in the context of the basic workflow.

Question 6

Question Type: MultipleChoice

In an SD-WAN TGW Connect topology, which three initial steps are mandatory when routing

traffic from a spoke VPC to a security VPC through a Transit Gateway? (Choose three.)

Options:

A- From the security VPC TGW subnet routing table, point 0.0.0.0/0 traffic to the FortiGate internal port.
B- From the security VPC TGW subnet routing table, point 0.0.0.0/0 traffic to the TGW.
C- From both spoke VPCs, and the security VPC, point 0.0.0.0/0 traffic to the Internet Gateway.
D- From the security VPC FortiGate internal subnet routing table, point 0.0.0.0/0 traffic to the TGW.
E- From the spoke VPC internal routing table, point 0.0.0.0/0 traffic to the TGW.

Answer:

A, D, E

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

In an AWS SD-WAN Transit Gateway (TGW) Connect topology, traffic flow must be meticulously orchestrated through VPC route tables to ensure that the FortiGate-VM (Security VPC) can inspect traffic transitioning between spokes.

Spoke to TGW Redirection (Option E): For traffic to leave a Spoke VPC and reach the inspection hub, the Spoke VPC internal routing table must be configured to send all non-local traffic (0.0.0.0/0) to the Transit Gateway (TGW). This is the first step in the traffic chain.

TGW to FortiGate Redirection (Option A): Once the traffic arrives at the TGW and is forwarded to the Security VPC via a TGW attachment, it lands in the TGW subnet (or attachment subnet). To ensure this traffic is inspected, the Security VPC TGW subnet routing table must point the default route (0.0.0.0/0) to the FortiGate's internal network interface (ENI).

FortiGate Return/Egress Path (Option D): After the FortiGate processes the packet, it must be sent back to the TGW to reach its final destination in a different spoke or to exit via a different gateway. Therefore, the Security VPC FortiGate internal subnet routing table (the subnet where the FortiGate's internal leg resides) must have a default route (0.0.0.0/0) pointing back to the TGW.

Why other options are incorrect:

Option B: If the Security VPC TGW subnet routing table points to the TGW as the next hop, it creates a routing loop where traffic arrives from the TGW and is immediately sent back without being inspected by the FortiGate.

Option C: Pointing all traffic to an Internet Gateway (IGW) would bypass the Transit Gateway entirely and send traffic to the public internet rather than through the internal security fabric.

Question 7

Question Type: MultipleChoice

Refer to the exhibit.

Terraform configuration

```
@Azure:~/FCSS/terraform/Troubleshooting$ terraform plan

Error: building account: getting authenticated object ID: listing Service Principals: ServicePrincipalsClient.BaseClient.Get():
clientCredentialsToken: received HTTP status 400 with response: {"error":"invalid_request","error_description":"AADSTS90002: Tenant
'942b80cd-1b14-42a1-8dcf-4b21dece61bb' not found. Check to make sure y ou have the correct tenant ID and are signing into the correct cloud.
Check with your subscription administrator, this may happen if there are no active subscriptions for the tenant.\r\nTrace ID:
fb39a7b9-1dc9-4d3f-a6c8-7f0569cf5600\r\nCorrelation ID: 81872e60-4daf-472a-967b-69960d36b66e\r\nTimestamp: 2022-09-14 19:53:26Z",
"error_ codes":[90002],"timestamp":"2022-09-14 19:53:26Z","trace_id":"fb39a7b9-1dc9-4d3f-a6c8-7f0569cf5600",
"correlation_id":"81872e60-4daf-472a-967b-69960d36b66e","error_uri " :"https ://login.mic rosoftonline.com/error?code=90002")

    with provider["registry.terraform.io/hashicorp/azurerm"],
    on provider.tf line 1, in provider "azurerm":
    1: provider "azurerm" {


@Azure:~/FCSS/terraform/Troubleshooting$
```

After the initial Terraform configuration in Microsoft Azure, the terraform plan command is run.

Which two statements about running the terraform plan command are true? (Choose two.)

Options:

A- The terraform plan command will deploy the rest of the resources except the service principle details.
B- You cannot run the terraform apply command before the terraform plan command.
C- The terraform plan command makes terraform do a dry run.
D- You must run the terraform init command once, before the terraform plan command.

Answer:

C, D

Question 8

Question Type: MultipleChoice

Exhibit.

```
[ec2-user@ip-10-0-0-200 ~]$ sudo yum -y install unzip
Last metadata expiration check: 0:02:31 ago on Sun Jul 21 22:12:44 2024.
Package unzip-6.0-57.amzn2023.0.2.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-10-0-0-200 ~]$ unzip terraform_${TERRAFORM_VER}_linux_amd64.zip
Archive: terraform_1.5.3_linux_amd64.zip
inflating: terraform
[ec2-user@ip-10-0-0-200 ~]$ terraform version
-bash: terraform: command not found
[ec2-user@ip-10-0-0-200 ~]$
```

You are tasked with deploying FortiGate using Terraform. When you run the terraform version command during the Terraform installation, you get an error message.

What could you do to resolve the command not found error?

Options:

A- You must move the binary file to the bin directory.
B- You must reinstall Terraform.
C- You must change the directory location to the root directory.
D- You must assign correct permissions to the ec2-user.

Answer:

A

Explanation:

https://github.com/fortinet/fortigate-terraform-deploy

According to the Terraform documentation for installing Terraform on Linux, you need to download a zip archive that contains a single binary file called terraform. You need to unzip the archive and move the binary file to a directory that is included in your system's PATH environment variable, such as /usr/local/bin. This way, you can run the terraform command from any directory without specifying the full path. If you do not move the binary file to the bin directory, you will get a command not found error when you try to run the terraform version command, as shown in the screenshot. To fix this error, you need to move the binary file to the bin directory or specify the full path of the binary file when running the command.

Question 9

Question Type: MultipleChoice

As part of your organization's monitoring plan, you have been tasked with obtaining and analyzing detailed information about the traffic sourced at one of your FortiGate EC2 instances.

What can you do to achieve this goal?

Options:

A- Use AWS CloudTrail to capture and then examine traffic from the EC2 instance.
B- Create a virtual public cloud (VPC) flow log at the network interface level for the EC2 instance.
C- Add the EC2 instance as a target in CloudWatch to collect its traffic logs.
D- Configure a network access analyzer scope with the EC2 instance as a match finding.

Answer:

B

Question 10

Question Type: MultipleChoice

Refer to the exhibit.

variable configuration

```
variable access_key {}
variable secret_key {}

variable "region" {
 default = "eu-west-1"
}

// Availability zones for the region
variable "az1" {
 default = "eu-west-1a"
}

variable "vpccidr" {
 default = "10.2.0.0/16"
}

variable "publiccidraz1" {
 default = "10.1.0.0/24"
}

variable "privatecidraz1" {
 default = "10.1.1.0/24"
}

// License Type to create FortiGate-VM
// Provide the license type for FortiGate-VM Instances, either
byol or payg. variable "license_type" {
 default = "byol" "Brave-Dumps.com"
}

// AMIs are for FGTVM-AWS(PAYG) - 7.6.0
variable "fgtvmami" {
```

You are tasked to deploy a FortiGate VM with private and public subnets in Amazon Web Services (AWS). You examined the variables.tf file. Assume that all the other terraform files are in place. What will be the final result after running the terraform init and terraform apply commands? (Select one answer)

Options:

A- Terraform will not deploy a FortiGate VM.

B- Terraform will deploy a FortiGate VM in the eu-West-1a availability zone without any subnets.

C- Terraform will deploy a FortiGate VM in the eu-West-1 region with private and public subnets.

D- Terraform will deploy a FortiGate VM in the eu-West-1a availability zone with two subnets and BYOL license.

Answer:

A

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

Based on the FortiOS 7.6 AWS Administration Guide and the Fortinet 7.4 Public Cloud Security documentation regarding Terraform deployments:

Variable Validation and Logic (Option A): The variables.tf file contains a logic error that prevents a successful deployment.

Specifically, the variable license_type has a default value defined as 'byol' 'Brave-Dumps.com'.

In Terraform HCL (HashiCorp Configuration Language), a variable's default attribute can only hold a single value string (e.g., 'byol'). The inclusion of the secondary string 'Brave-Dumps.com' within the same default assignment is a syntax error.

Impact on Execution: When terraform apply is executed, the Terraform engine performs a validation check on all loaded files. Because of this syntax error in the variable definition, the validation will fail, and Terraform will stop execution with an error message before any resources---including the FortiGate VM---are created in AWS.

Network Mismatch: Additionally, the variable vpccidr is set to 10.2.0.0/16, while the public (10.1.0.0/24) and private (10.1.1.0/24) subnets are defined within a completely different address space (10.1.x.x). Even if the syntax error were fixed, the deployment would likely fail at the infrastructure level because subnets must reside within the CIDR block of their parent VPC.

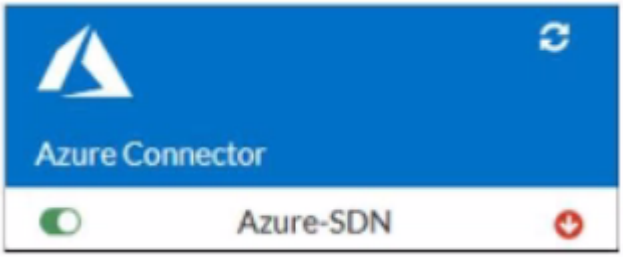
Why other options are incorrect:

Option B, C, & D: None of these successful deployment outcomes can occur because the Terraform parser will identify the invalid syntax in the variables.tf file and abort the process entirely.

Question 11

Question Type: MultipleChoice

Refer to the exhibit.



You are troubleshooting a Microsoft Azure SDN connector issue on your FortiGate VM in Azure.

Which command can you use to examine details about API calls sent by the connector?

Options:

A- diag debug application cloud-connector -1
B- diag test application azd 1
C- diag debug application azd -1
D- get system sdn-connector

Answer:

C