Prepare Smart for Success Free Fortinet NSE7_CDS_AR-7.6 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 7 - Public Cloud Security 7.6.4 Architect exam PDF questions now. Get authentic NSE7_CDS_AR-7.6 dumps packed with verified answers and secure your certification success with PrepBolt NSE7_CDS_AR-7.6 exam pdf questions and answers.

Thank you for Downloading NSE7_CDS_AR-7.6 exam PDF Demo

https://prepbolt.com/NSE7_CDS_AR-7.6.html

Question 1

Question Type: MultipleChoice

A customer would like to use FortiGate fabric integration with FortiCNP. When adding a FortiGate VM to FortiCNP, which three mandatory configuration steps must you follow on FortiGate? (Choose three answers)

Options:

A- Enable pre-shared key on both sides.
B- Import the FortiGate certificate into FortiCNP.
C- Configure FortiGate to send logs to FortiCNP.
D- Create an IPS sensor and a firewall policy.
E- Create an SSL/SSH inspection profile.

Answer:

C, D, E

Explanation:

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

According to the FortiCNP 24.x Administration Guide and the FortiOS 7.6 Security Fabric Integration documentation, integrating a FortiGate-VM with FortiCNP requires specific local configurations on the FortiGate to ensure the cloud security platform can ingest and analyze traffic data.

Configuring Logging (Option C): Before adding the FortiGate VM to FortiCNP, the administrator must Enable Send Logs on the FortiGate. This allows the FortiGate to forward the necessary security telemetry and traffic logs to the FortiCNP cloud endpoint for threat correlation and risk analysis.

Policy and Inspection Setup (Option D): The integration relies on the FortiGate's ability to identify and block threats at the network layer. Specifically, the administrator must Create a FortiGate IPS Sensor and Create a FortiGate Firewall Policy. The IPS sensor detects malicious patterns, while the firewall policy dictates which traffic is subjected to this inspection.

Deep Packet Inspection (Option E): To provide visibility into encrypted traffic---which is critical for identifying threats hidden in HTTPS flows---the administrator must Create an SSL/SSH Inspection Profile on the FortiGate. Without this profile, FortiCNP would lose significant visibility into potential attack vectors utilizing encrypted channels.

Why other options are incorrect:

Option A: While pre-shared keys are used in VPN and some Fabric setups, they are not listed as one of the specific mandatory steps for the initial FortiGate-to-FortiCNP fabric integration workflow.

Option B: While certificate exchange is part of the overall trust relationship, the primary 'mandatory configuration steps on FortiGate' defined in the official setup guide focus on the logging and security profile components required to generate the data FortiCNP needs.

Question 2

Question Type: MultipleChoice

You have onboarded the organization's Microsoft Azure account on FortiCNAPP using the automated configuration approach. However, FortiCNAPP does not appear to be receiving any workload scanning data. How can you remedy this? (Choose one answer)

Options:

A- Add a new Azure App Registration.
B- Add a service principal in the Azure Cloud Shell.
C- Add a FortiCNAPP threat policy to monitor Azure workloads.
D- Add the appropriate integration type using the guided configuration.

Answer:

D

Explanation:

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

Based on the FortiCNAPP 24.x Administration Guide regarding Microsoft Azure onboarding and feature activation:

Separation of Integration Types (Option D): In FortiCNAPP, onboarding a cloud account via the automated configuration approach often initializes the Cloud Security Posture Management (CSPM) and Cloud Infrastructure Entitlement Management (CIEM) features. However, Workload Scanning (specifically Agentless Scanning) is treated as a distinct integration type within the platform.

Guided Configuration Requirement: Even after the account is onboarded, the administrator must navigate to the Integrations or Onboarding section and specifically add the Workload Scanning integration for that Azure account. This 'Guided Configuration' ensures that the necessary additional permissions (such as those required to create snapshots of disks and scan them) and resources (like the scanner VNet or regional scanners) are properly deployed within the Azure environment.

Why other options are incorrect:

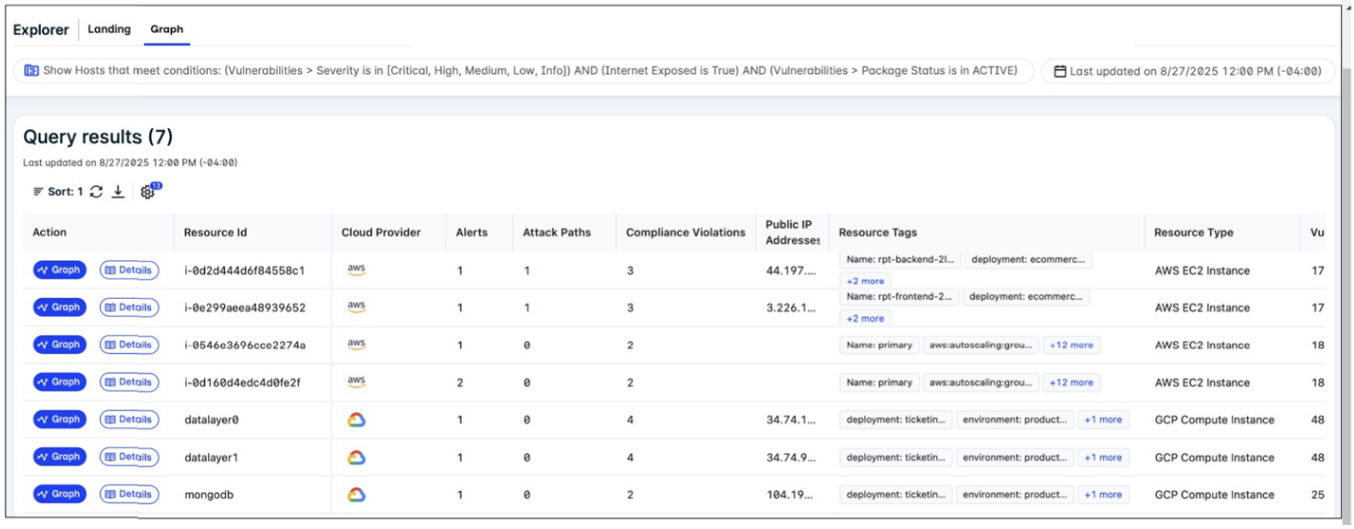
Option A & B: Automated onboarding already handles the creation of necessary App Registrations and Service Principals. Manually adding more without following the specific integration workflow will not activate the workload scanning engine.

Option C: Threat policies are used to generate alerts based on existing data. If the raw workload scanning data is not being received from Azure, a policy will have no data to analyze; the issue is at the ingestion/integration layer, not the policy layer.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



A FortiCNAPP administrator used the FortiCNAPP Explorer to reveal all hosts exposed to the internet that are running active packages with vulnerabilities of all severity levels. Why do only the first two results have an attack path? (Choose one answer)

Options:

A- Attack paths are available only for AWS resources with public IP addresses.
B- Attack paths are available only for AWS resources with high impact scores.
C- Attack paths are available only for resources with potential multi-hop exposure.
D- Attack paths are available only for resources that have critical vulnerabilities.

Answer:

A

Explanation:

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

Based on the FortiCNAPP (formerly Lacework) Cloud Security documentation regarding Attack Path Analysis and Explorer functionality:

Attack Path Generation (Option A): In FortiCNAPP, an 'Attack Path' is a visualized sequence of potential exploit steps that an external attacker could take to reach a sensitive resource. For the platform to generate and display an attack path, the target resource must be externally reachable.

Evidence in the Exhibit: * The exhibit shows a list of EC2 and GCP instances.

The first two results (Resource IDs i-0d2d... and i-0e29...) have values populated in the Public IP Addresses column (44.197.... and 3.226....). Consequently, these are the only two resources showing a value of 1 in the Attack Paths column.

The remaining resources in the list do not have public IP addresses listed in the exhibit's view, and as a result, their Attack Paths count is 0. This confirms that FortiCNAPP specifically calculates these paths for resources that have a direct entry point from the internet via a public IP.

Contextual Risk Assessment: FortiCNAPP prioritizes attack path analysis for internet-exposed assets because they represent the highest immediate risk. While internal resources may have vulnerabilities, the lack of a public-facing network interface means there is no direct external 'path' to visualize in this specific Explorer view.

Question 4

Question Type: MultipleChoice

You are investigating an attack path for a top risky host. You notice that the Common Vulnerability Scoring System (CVSS) and the vulnerability impact scores are very high. However, the attack path severity for the top risky host itself is low. Which two pieces of contextualized information can help you understand why? (Choose two answers)

Options:

A- The FortiCNAPP risk score
B- The package status
C- The vulnerability score
D- The fix version

Answer:

A, B

Question 5

Question Type: MultipleChoice

Refer to the exhibit.

An administrator installed a FortiWeb ingress controller to protect a containerized web application. What is the reason for the status shown in FortiView? (Choose one answer)

Options:

A- The SDN connector is not authenticated correctly.
B- The FortiWeb VM is missing a route to the node subnet.
C- The manifest file deployed is configured with the wrong node IP addresses.
D- The load balancing type is not set to round-robin.

Answer:

B

Explanation:

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

According to the FortiWeb 7.4 Administration Guide and the FortiWeb Ingress Controller Installation Guide, the status of backend servers in the FortiView Topology dashboard is a direct reflection of the health check results.

Interpreting the Status Icon (Orange): In the FortiView Topology view, a green circle indicates that the

server is up and responding to health checks, while an orange circle indicates that the server is not running or is unreachable.

Connectivity and Routing (Option B): For the FortiWeb ingress controller to accurately monitor and protect a containerized application, it must have a valid network path to the Kubernetes (K8s) worker nodes. If the FortiWeb VM is missing a route to the specific subnet where the K8s nodes reside, the health check packets will fail to reach their destination. As a result, FortiWeb identifies the backend servers (192.168.0.1, 192.168.0.2, and 192.168.0.3) as 'Down,' leading to the orange status shown in the exhibit.

Health Check Failures: When the status is orange, it implies that the Server Health Check (configured in the server pool) is detecting that the web servers are not responsive to connections. While this could be caused by an application-level failure, in a fresh cloud deployment of an ingress controller, the most common underlying cause is a network routing misconfiguration preventing the FortiWeb appliance from reaching the node IPs.12

Why other options are incorrect:34

Option A: If the SDN connector were not authenticated correctly, FortiWeb would likely fail to discover the containerized resources entirely, rather than discovering them and repor5ting them as 'Down'.6

Option C: While wron7g IP addresses would cause a failure, the Ingress Controller's job is to dynamically sync these addresses from the K8s API; a manual configuration error in a manifest file regarding IP addresses is less likely in an automated ingress environment.

Option D: The load balancing algorithm (Round Robin, Least Connections, etc.) affects how traffic is distributed, but it does not influence the up/down health status of the individual backend servers.

Question 6

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? (Choose 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 7

Question Type: MultipleChoice

You are experiencing intermittent connectivity issues in a FortiGate HA cluster deployed with Azure gateway load balancer. Traffic is being dropped when it passes through the cluster. What is the cause of the issue? (Choose one answer)1

Options:

A- The FortiGate firewalls are using the default maximum transmission unit (M2TU) size supported by Azure.
B- The Azure gateway load balancer is configured with an incorrect health probe port.
C- The Azure gateway load balancer is blocking large packets, causing traffic failures.

D- The protected VMs are running an application that fragments packets.

Answer:

A

Explanation:

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

According to the FortiOS 7.6 Azure Administration Guide and the Public Cloud Security documentation regarding Azure Gateway Load Balancer (GWLB) integration:

Encapsulation Overhead: Azure Gateway Load Balancer uses VXLAN (Virtual eXtensible LAN) to encapsulate the traffic before sending it to the FortiGate-VM HA cluster. This encapsulation adds a header that typically consists of 50 bytes for regular IPv4 traffic (Ethernet, IP, UDP, and VXLAN headers).

MTU Mismatch (Option A): The default maximum transmission unit (MTU) in Azure is 1500 bytes. If a protected VM sends a packet at the maximum default size (1500 bytes), and the GWLB then adds the 50-byte VXLAN header, the resulting encapsulated packet becomes 1550 bytes.

Packet Drops: If the FortiGate-VM's network interfaces are left at the default MTU of 1500 bytes, they will not be able to process the 1550-byte encapsulated frames without fragmentation. Because many network paths or configurations (including Azure's fabric for certain flows) may drop packets that require fragmentation or have the Don't Fragment (DF) flag set, this results in the observed intermittent connectivity issues and dropped traffic.

Required Resolution: To resolve this issue, administrators must increase the MTU on the FortiGate-VM interfaces (specifically the one receiving GWLB traffic) to at least 1570 bytes to accommodate both IPv4 and IPv6 VXLAN overhead.

Why other options are incorrect:

Option B: While an incorrect health probe port would cause the GWLB to mark the FortiGate as down, it would typically lead to a complete loss of traffic flow through that instance rather than intermittent packet drops within an active flow.

Option C: The GWLB itself is the component adding the overhead; it is the FortiGate's inability to receive the larger resulting frame (due to its own default MTU setting) that causes the failure.

Option D: Packet fragmentation by the application is a secondary effect. The primary 'intermittent' issue described in GWLB deployments is almost always related to the tunneling overhead exceeding the receiving interface's MTU.

Thank You for trying NSE7_CDS_AR-7.6 PDF Demo

To try our NSE7_CDS_AR-7.6 practice exam software visit link below

https://prepbolt.com/NSE7_CDS_AR-7.6.html

Start Your NSE7_CDS_AR-7.6 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your NSE7_CDS_AR-7.6 preparation with actual exam questions.