Free Questions for FCP_WCS_AD-7.4 by certscare

Shared by Cobb on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You need to deploy a new Windows server in AWS to offload web traffic from an existing web server in a different availability zone.

According to the AWS shared responsibility model, what three actions must you take to secure the new EC2 instance? (Choose three.)

Options:

A- Update software on the instance.

B- Change the existing elastic load balancer (ELB) to a gateway load balancer

C- Configure security groups.

D- Manage the operating system on the instance.

E- Move all web servers into the same availability zone.

Answer:

A, C, D

Explanation:

Update Software:

As part of the AWS shared responsibility model, it is the customer's responsibility to update and maintain the software running on the EC2 instance, including applying security patches and updates (Option A).

Configure Security Groups:

Security groups act as virtual firewalls for instances to control inbound and outbound traffic. Configuring them correctly is essential for securing the EC2 instance and ensuring only legitimate traffic can reach the server (Option C).

Manage Operating System:

Managing the operating system, including user accounts, permissions, and operating system patches, is the responsibility of the customer under the shared responsibility model (Option D).

Other Options Analysis:

Option B is incorrect as changing the existing ELB to a gateway load balancer is not necessary for securing the new EC2 instance.

Option E is incorrect because it is not required to move all web servers into the same availability zone for security purposes.

AWS Shared Responsibility Model: AWS Shared Responsibility

EC2 Security Best Practices: AWS EC2 Security

Question 2

Question Type: MultipleChoice

Your organization is deciding between deploying FortiWeb VM or Fortinet Managed Rules for AWS WAF.

What are two benefits of choosing FortiWeb VM? (Choose two.)

Options:

A- Only pay for what is used.

B- Up-to-date WAF signatures powered by FortiGuard.

C- Zero-day protection.

D- Advanced WAF functionality.

Answer:

C, D

Explanation:

Zero-day Protection:

FortiWeb VM provides robust protection against zero-day vulnerabilities through advanced security mechanisms and frequent updates from FortiGuard. This ensures that web applications are protected from newly discovered threats that have not yet been patched or

recognized by other security systems (Option C).

Advanced WAF Functionality:

FortiWeb VM offers a range of advanced WAF features that go beyond what is typically provided by managed rules for AWS WAF. These include more detailed traffic analysis, customizable rules, machine learning-based threat detection, and comprehensive logging and reporting capabilities (Option D).

Other Options Analysis:

Option A is more relevant to a consumption-based pricing model but not a specific benefit unique to FortiWeb VM over AWS WAF.

Option B is incorrect because both FortiWeb VM and Fortinet Managed Rules for AWS WAF are powered by FortiGuard updates.

FortiWeb Overview: FortiWeb VM

AWS WAF and Fortinet Managed Rules: AWS WAF

Question 3

Question Type: MultipleChoice

Refer to the exhibit.

FortiGate debug output

```
FortiGate-VM64-AWS # diagnose debug enable

FortiGate-VM64-AWS # diagnose debug application awsd -1
Debug messages will be on for 24 minutes.

FortiGate-VM64-AWS # awsd sd connector AWS Lab prepare to update
awsd sdn connector AWS Lab start updating
aws curl response err, 401
<?xml version="1.0" encoding="UTF-8"?>
<Response><Errors><Error><Code>AuthFailure</Code><Message>AWS was not able to validate
the provided access credentials</Message></Error></Errors><RequestID>b3c08dfe-8
97d-4307-b039-ece48519f1b8</RequestID></Response>
aws access/secret key invalid
awsd sdn connector AWS Lab failed to get instance list
awsd reap child pid: 14257
sdn AWS Lab firewall addr change
awsd sdn connector AWS Lab prepare to update
awsd sdn connector AWS Lab start updating
aws curl response err, 401
<?xml version="1.0" encoding="UTF-8"?>
<Response><Errors><Error><Code>AuthFailure</Code><Message>AWS was not able to validate
the provided access credentials</Message></Error></Errors><RequestID>befa40a0-
17d-4819-a281-5daa7dd63a7c</RequestID></Response>
aws access/secret key invalid
awsd sdn connector AWS Lab failed to get instance list
awsd reap child pid: 14259
sdn AWS Lab firewall addr change
awsd sdn connector AWS Lab prepare to update
awsd sdn connector AWS Lab start updating
aws curl response err, 401
<?xml version="1.0" encoding= "UTF-8"?>
<Response><Errors><Error><Code>AuthFailure‹/Code><Message>AWS was not able to validate
the provided access credentials</Message></Error></Errors><RequestID>8e82eecd-
290-4e05-8c6b-85e7004ee48a</RequestID></Response>
aws access/secret key invalid
```

An administrator configured a FortiGate device to connect to the AWS API to retrieve resource values from the AWS console to create dynamic objects for the FortiGate policies. The administrator is unable to retrieve AWS dynamic objects on FortiGate.

Which two reasons can explain why? (Choose two.)

Options:

A- The AWS API call is not supported on XML version 1.0.

B- AWS was not able to validate credentials provided by the AWS Lab SDN connector because of a clock skew between FortiGate and AWS.

C- The AWS Lab SDN connector is configured with an invalid AWS access or secret key.

D- The AWS Lab SDN connector failed to connect on port 401.

E- The AWS Lab SDN did not find any instances in the configured VPC.

Answer:

B, C

Explanation:

Invalid Credentials:

The debug output shows an 'AuthFailure' error, indicating that AWS was not able to validate the provided access credentials. This usually points to incorrect or invalid AWS access or secret keys configured in the AWS Lab SDN connector (Option C).

Clock Skew:

Another common reason for authentication failures in AWS API calls is a clock skew between the FortiGate device and AWS. AWS requires that the system time of the client making the API call is synchronized with its own time, within a small margin. If there is a significant time difference, AWS will reject the credentials (Option B).

Other Options Analysis:

Option A is incorrect because the AWS API supports XML version 1.0.

Option D is incorrect as the error message does not indicate an issue with connecting on port 401.

Option E is incorrect because the error is related to authentication, not the absence of instances.

AWS API Authentication: AWS API Security

FortiGate AWS Integration Guide: FortiGate AWS Integration

Question 4

Question Type: **MultipleChoice**

A cloud administrator is tasked with protecting web applications hosted in AWS cloud.

Which three Fortinet cloud offerings can the administrator choose from to accomplish the task? (Choose three.)

Options:

A- AWS WAF

B- FortiEDR

C- FortiGate Cloud-Native Firewall (CNF)

D- Fortinet Managed Rules for AWS WAF

E- FortiWeb Cloud

Answer:

C, D, E

Explanation:

FortiGate Cloud-Native Firewall (CNF):

FortiGate CNF offers cloud-native firewall capabilities designed to provide network security within AWS. It integrates seamlessly with AWS services and offers advanced threat protection and traffic management (Option C).

Fortinet Managed Rules for AWS WAF:

Fortinet Managed Rules for AWS WAF provide pre-configured, updated security rules that protect web applications from common threats such as SQL injection and cross-site scripting. This offering simplifies the protection of web applications hosted on AWS (Option D).

FortiWeb Cloud:

FortiWeb Cloud is a Web Application Firewall (WAF) as a service that provides comprehensive protection for web applications hosted on AWS. It offers features such as bot mitigation, DDoS protection, and deep inspection of HTTP/HTTPS traffic (Option E).

Comparison with Other Options:

Option A (AWS WAF) is a native AWS service, not a Fortinet offering.

Option B (FortiEDR) is focused on endpoint detection and response, which is not specifically aimed at protecting web applications.

FortiGate CNF Documentation: FortiGate CNF

Fortinet Managed Rules for AWS WAF: Fortinet AWS WAF Rules

FortiWeb Cloud Overview: FortiWeb Cloud

Question 5

Question Type: **MultipleChoice**

A customer is attempting to deploy an active-passive high availability (HA) cluster using the software-defined network (SDN) connector in the AWS cloud.

What is an important consideration to ensure a successful formation of HA, failover, and traffic flow?

Options:

A- Both cluster members must be in the same availability zone.

B- VDOM exceptions must be configured.

C- Unicast FortiGate Clustering Protocol (FGCP) must be used.

D- Both cluster members must show as healthy in the elastic load balancer (ELB) configuration.

Answer:

C

Explanation:

HA Cluster in AWS Cloud:

Deploying an active-passive HA cluster in AWS requires careful consideration of the clustering protocol used to ensure seamless failover and traffic flow.

Unicast FortiGate Clustering Protocol (FGCP):

Unicast FGCP is specifically designed for environments where multicast traffic is not feasible or supported, such as in the AWS cloud. Using unicast FGCP ensures that heartbeat and synchronization traffic between the cluster members are managed correctly over unicast communication, which is suitable for AWS's network infrastructure (Option C).

Comparison with Other Options:

Option A is incorrect because while placing both cluster members in the same availability zone might be required for certain configurations, it is not the critical factor for HA formation.

Option B is incorrect as VDOM exceptions are not directly related to the successful formation of HA.

Option D is incorrect because the ELB configuration checks are more about ensuring that the load balancer correctly routes traffic but do not specifically ensure HA formation and failover.

FortiGate HA in AWS Documentation: FortiGate HA

Fortinet FGCP Details: FGCP Documentation

Question 6

Question Type: **MultipleChoice**

An administrator must deploy a web application firewall (WAF) solution to protect the web applications of their organization.

Why would the administrator choose FortiWeb Cloud over AWS WAF with Fortinet managed rules?

Options:

A- WAF signatures must be manually updated by FortiGuard.

B- The solution must meet PCI 6.6 compliance.

C- SSL inspection is a requirement.

D- Traffic must be inspected for malware.

Answer:

C

Explanation:

SSL Inspection Requirement:

FortiWeb Cloud provides comprehensive SSL inspection capabilities, allowing it to decrypt and inspect HTTPS traffic for threats. This is a crucial feature for many organizations that need to ensure all traffic, including encrypted traffic, is thoroughly inspected (Option C).

Comparison with AWS WAF:

While AWS WAF with Fortinet managed rules provides robust protection, it might not offer the same level of SSL inspection capabilities as FortiWeb Cloud.

Other Considerations:

Option A (Manual WAF signature updates) is incorrect because FortiWeb Cloud updates signatures automatically.

Option B (PCI 6.6 compliance) is a general requirement for any WAF solution, not specific to choosing FortiWeb Cloud over AWS WAF.

Option D (Traffic inspection for malware) is a feature provided by both FortiWeb Cloud and AWS WAF with Fortinet managed rules.

FortiWeb Cloud Overview: FortiWeb Cloud

AWS WAF Documentation: AWS WAF