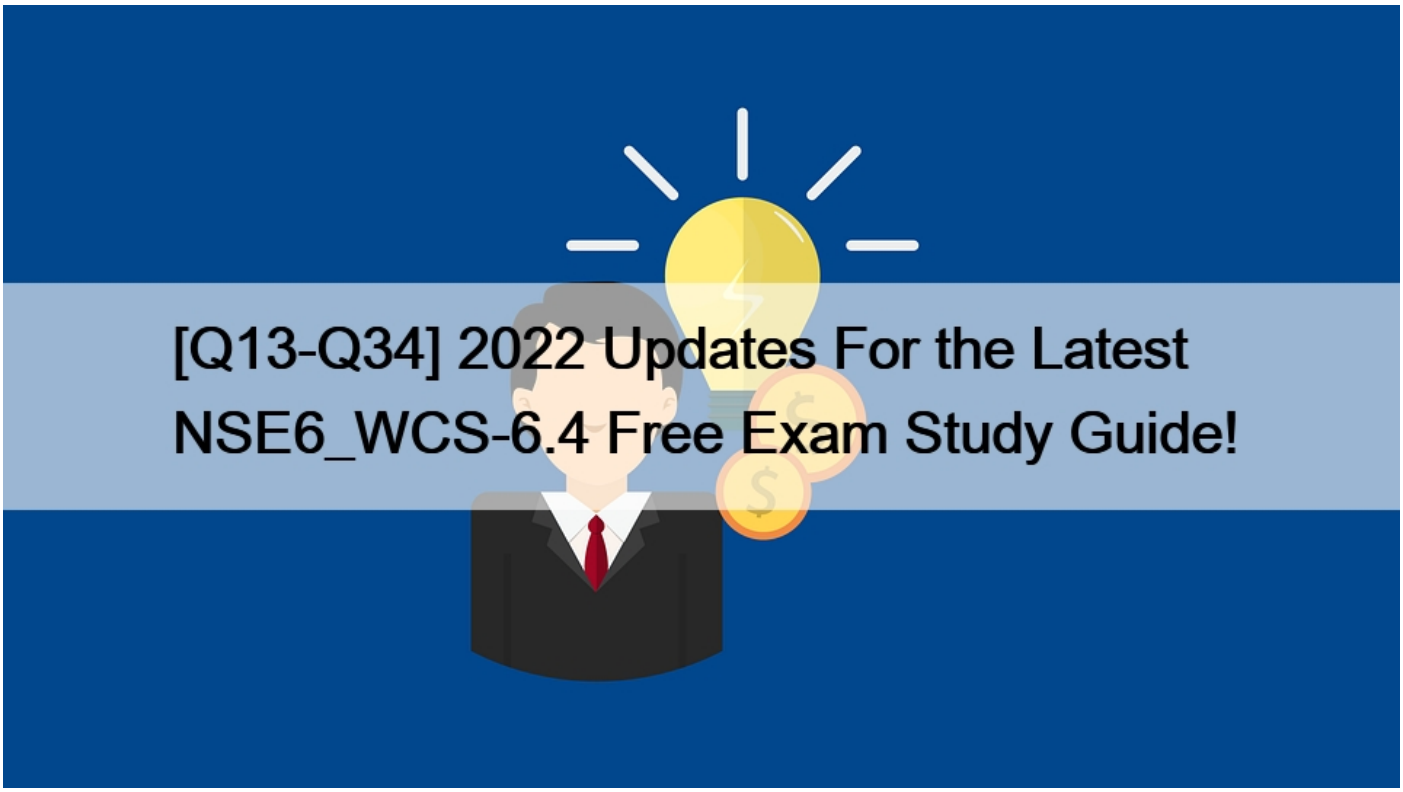
[Q13-Q34 2022 Updates For the Latest NSE6_WCS-6.4 Free Exam Study Guide!



2022 Updates For the Latest NSE6_WCS-6.4 Free Exam Study Guide! Best NSE6_WCS-6.4 Exam Preparation Material with New Dumps Questions

Fortinet NSE6_WCS-6.4 Exam Syllabus Topics:

TopicDetailsTopic 1- Configure HA using Fortinet cloud formation templates- Describe traffic flow in AWSTopic 2- Distinguish between different licenses in AWS Marketplace?PAYG and BYOL- Explain AWS basic concepts and componentsTopic 3- Explain Fortinet solutions for AWS- Deploy Fortinet products in AWS

Q13. Which three statements are correct about VPC flow (Choose three.)

* Flow logs can capture real-time log streams for the network interfaces.
* Flow logs do not capture DHCP traffic.
* Flow logs can capture traffic to the reserved IP address for the default VPC router.
* Flow logs can be used as a security tool to monitor the traffic that is reaching the instance.
* Flow logs do not capture traffic to andfrom169.2 54 .169.254 for instance metadata.

Q14. An organization has created a VPC and deployed a FortiGate-VM (VM04 /c4.xlarge) in AWS, FortiGate-VM is initially configured With two Elastic Network Interfaces (ENIs). The primary ENI of FortiGate-VM is configured for a public subnet. and the second ENI is configured for a private subnet. In order to provide internet access. they now want to add an EIP to the primary ENI of FortiGate, but the EIP assignment is failing.

Which action would allow the EIP assignment to be successful?
* Shut down the FortiGate VM. if it is running. assign the EIP to the primary ENI. and then power it on.
* Create and associate a public subnet With the primary ENI Of FortiGate, and then assign the EIP to the primary ENI.
* Create and attach a public routing table to the public subnet, associate the public subnet With the primary ENI Of FortiGate. and then assign the EP to the primary ENI.
* Create and attach an Internet gateway to the VPC. and then assign the EIP to the primary ENI Of FortiGate.

Q15. An MSSP deployed 16 FortiGate VMS With the default AWS security groups and network access lists using an on-demand license from Amazon Web Services (AWS) Marketplace. They are using a third-party configuration backup application to back up and track changes for the FortiGate configurations. It can connect to the FortiGatedevices using only the SSH protocol, A customer is using the correct username and password configured on the FortiGate devices. but they are unable to log in using theSSH protocol.

What can be the reason Why this authentication is failing?
* The default AWS network access list for FortiGate does not allow SSH.
* The AWS key is required to log in to FortiGate using SSH
* AWS uses non-standard SSH port1025, and the default AWS security groups and NACL for FortiGate are not configured for the port.
* The default AWS Security group for FortiGate does not allow SSH.

Q16. A customer deployed Fortinet Managed Rules for Amazon Web Services (AWS) Web-Application Firewall (WAF) to protect web application servers from attacks.

Which statement about Fortinet Managed Rules for AWS WAF is correct?
* It offers a negative security model.
* It can provide Layer 7 DOS protection.
* It can provide IP Reputation (WAF subscription FortiGuard).
* It can perform bot and known search engine identification and protection

Q17. A customer deployed an HA Cloud formation to Stage and bootstrap the FortiGate configuration.

Which AWS functions are used by FortiGate HA to call the HA failover?
* AWS Lambda functions
* AWS Mapping functions
* AWS S3 functions
* AWS DynamoDB functions

Q18. Which three Fortinet products are available in Amazon Web Services in both on-demand and bring your own license (BYOL) formats? (Choose three.)
* FortiGate
* FortiWeb
* FortiADC
* FortiSlEM
* FortiSOAR

Q19. Refer to the exhibit.

```
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 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>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
```

blog.examslabs.com

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

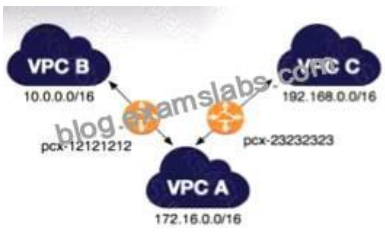
Which three reasons can explain btw? (Choose three.)
* AWS was not able to validate credentials provided by the AWS Lab SON connector.
* The AWS Lab SON connector failed to connect on port 401.
* The AWS Lab SON connector failed to retrieve the instance list.
* The AWS API call is not supported on XML version I . O.
* The AWS Lab SON connector is configured with an invalid AWS access or secret key

Q20. You connected to the AWS Management Console at 10:00 AM and verified that there are two FortiGate VMS running, You receive a call from a user reporting about a temporary slow Internet connection that lasted only a few minutes. When you go back to the AWS portal. you notice there are now two additional FortiGate VMS that you did not create. Later that day, the number of VMS returns to two without your intervention. A similar situation occurs several times during the week.

What is the most likely reason for this to happen?
* The VMS are in an availability group with dynamic membership.
* Autoscaling is configured to act as described in the scenario.
* The user ran a script to create the extra VMS to get faster connectivity.
* The AWS portal is not refreshed automatically. and another administrator is creating and removing the VMS as needed.

Q21. Which two statements are correct about AWS Network Access Control Lists (NACLS)? (Choose two.)
* NACLs are stateless: responses to allowed inbound traffic are subject to the rules for outbound traffic.
* An NACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
* By default. each custom NACL allows all inbound and outbound traffic unless you add new rules,
* VPC automatically comes with a modifiable default NACL, and by default it denies all inbound and outbound IPv4 traffic.

Q22. Refer to the exhibit.



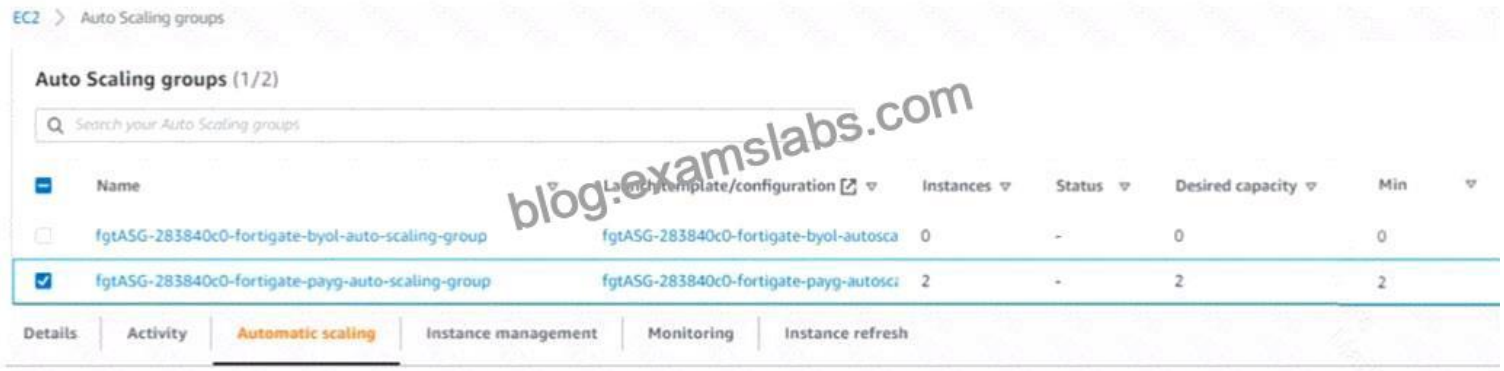
blog.examslabs.com

Which statement is correct about the VPC peering connections shown in the exhibit?
* You can associate VPC ID pcx-23232323 with VPC B to form a VPC

peering connection between VPC B and VPC C.
* You cannot route packets directly from VPC B to VPC C through VPC A.
* TO route packets directly from VPC B to VPC C through VPC A, you must add a route for network 192.168.0.0/16 in the VPC A routing table.
* You cannot create a VPC peering connection between VPC B

and VPC C to route packets directly.

Q23. Refer to the exhibit.



An administrator configured two auto-scaling polices that they now want to test, What Will be the impact on payg-auto-scaling-group for the FortiGate devices if the administrator executes a scale-in policy?
* The scale-in policy will decrease instances from two to one.
* The scale-in policy will decrease the desired capacity from two to one
* The scale-in policy will decrease the number of maximum instances from four to three.

Q24. Refer to the exhibit.

You have created an autoscale configuration using a FortiGate HA Cloud

Formation template. You want to examine the autoscale FortiOS configuration to confirm that FortiGate autoscale is configured to synchronize primary and secondary devices. On one of the FortiGate devices, you execute the command shown in the exhibit Which statement is correct about the output of the command?

* The device is the primary in the HA configuration. with the IP address

10.0.0.173.

* The device is the secondary in the HA configuration, and the IP address Of the primary device is 10.0.0.173.
* The device is the primary in the HA configurationand the IP address of the secondary device is10.0.0.173.
* The device is the secondary in the HA configuration. with the IP address

10.0.0.173.

Free NSE6_WCS-6.4 Exam Files Verified & Correct Answers Downloaded Instantly:
https://www.examslabs.com/Fortinet/Fortinet-Certification/best-NSE6_WCS-6.4-exam-dumps.html]