Prepare Smart for Success Free Fortinet FCP_FSA_AD-5.0 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 5 - FortiSandbox 5.0 Administrator exam PDF questions now. Get authentic FCP_FSA_AD-5.0 dumps packed with verified answers and secure your certification success with PrepBolt FCP_FSA_AD-5.0 exam pdf questions and answers.

Thank you for Downloading FCP_FSA_AD-5.0 exam PDF Demo

https://prepbolt.com/FCP_FSA_AD-5.0.html

Question 1

Question Type: MultipleChoice

An organization has an existing FortiGate provisioned as a data center firewall (DCFW) that submits inbound files to FortiSandbox for inline scanning. As a result of a network redesign, traffic between the FortiSandbox and the DCFW now passes through an intermediate firewall. Inline scanning is no longer working. While examining the configuration of the intermediate firewall you notice that it is configured to allow traffic on ports TCP/3389, UDP/53, and TCP/443. What must you change for the integration to work? (Choose one answer)

Options:

A- FortiGate must be able to access FortiSandbox on TCP/4443.
B- FortiGate must be able to access FortiSandbox on TCP/8890.
C- FortiGate must be able to access FortiSandbox on UDP/8888.
D- FortiGate must be able to access FortiSandbox on UDP/1344.

Answer:

A

Explanation:

The FortiSandbox 5.0 Administrator Lab Guide explicitly states during the inline scanning configuration: ''FortiGate and FortiSandbox communicate through port 4443. Management or API ports grant access through port 4443.'' In the same exercise, the guide has you enable API access on port2 specifically so inline scanning can function, which confirms that the integration depends on FortiGate reaching FortiSandbox over TCP/4443.

In this scenario, the intermediate firewall currently allows TCP/3389, UDP/53, and TCP/443, but not TCP/4443. That is why inline scanning stopped working after the redesign. TCP/443 is not sufficient here because the documented FortiGate-to-FortiSandbox inline communication port is 4443, not standard HTTPS 443. The other ports in the options do not match the inline-scanning communication requirement described in the uploaded lab materials. Therefore, the required fix is to allow FortiGate access to FortiSandbox on TCP/4443.

Question 2

Question Type: MultipleChoice

A FortiSandbox HA cluster is configured with the MTA adapter. What does the primary node do when it receives MTA jobs? (Choose one answer)

Options:

A- It distributes the MTA jobs to secondary members.
B- It distributes the MTA jobs to itself or to worker nodes.
C- It assigns the MTA jobs to itself
D- It assigns the MTA jobs only to worker members.

Answer:

B

Explanation:

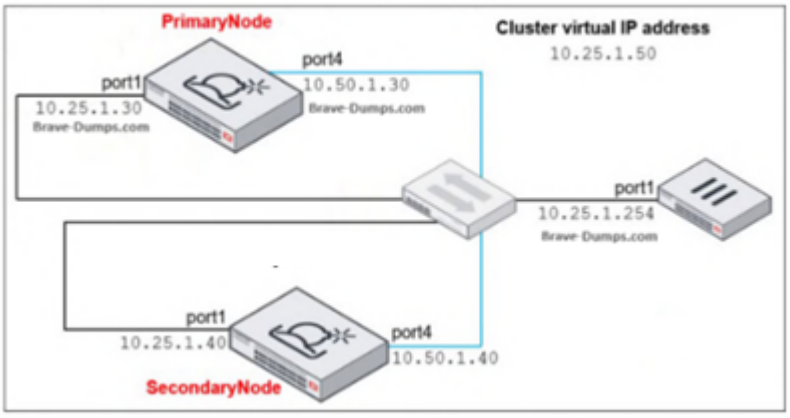
The Study Guide states that in an HA cluster, ''As well as normal scanning duties, the primary node also manages the cluster, distributes jobs, and gathers the verdicts.'' It also says that ''The worker nodes provide load balancing. The primary node distributes scan jobs to the worker nodes.''

From those official statements, the primary node is not just a coordinator. It also performs normal scanning duties itself, while distributing scan jobs across worker nodes for load balancing. That rules out A, because the secondary node is for failover, not normal job distribution. It rules out C, because the primary is not restricted to itself only. It also rules out D, because the primary can still perform scanning duties and is not limited to sending all jobs only to workers. Therefore, when the primary receives MTA jobs, the correct behavior is that it distributes the MTA jobs to itself or to worker nodes.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



Which command must you use to configure the FortiSandbox device as the primary node? (Choose one answer)

Options:

A- hc-settings -si iport1 -a10.25.1.30
B- hc-settings -si iport1 -a10.25.1.40
C- hc-settings -si iport1 -a10.25.1.254
D- hc-settings -si iport1 -a10.25.1.50

Answer:

D

Explanation:

The exhibit labels 10.25.1.50 as the cluster virtual IP address. The Study Guide explains that in HA configuration, ''You must configure the HA group name, password, and the virtual IP only on the primary node.'' It also says: ''You must also configure an external interface for external communication and an IP address that will be used as a virtual IP for the whole cluster. Devices will interact with the cluster using this virtual IP.''

That is why the command for the primary node must point to the cluster virtual IP, not to the individual port1 addresses of the primary, secondary, or upstream firewall. In the exhibit, 10.25.1.30 is the primary node's own port1 IP, 10.25.1.40 is the secondary node's port1 IP, and 10.25.1.254 is the network device. The only address that matches the required cluster virtual IP is 10.25.1.50, so the correct command is hc-settings -si iport1 -a10.25.1.50.

Question 4

Question Type: MultipleChoice

You are troubleshooting long delays between FortiMail file submissions to FortiSandbox and verdicts being returned form FortiSandbox. Which FortiMail debug tool must you use to troubleshoot this issue further? (Choose one answer)

Options:

A- diagnose debug application hoststatd
B- diagnose debug application deferd
C- diagnose debug application oftpd
D- diagnose debug application mailfilterd

Answer:

B

Explanation:

The FortiSandbox 5.0 Administrator Lab Guide shows that, when diagnosing FortiMail submission issues, the required FortiMail debugs are sandboxclid and deferd. It explicitly instructs: ''Enter the following commands to enable both deferd and sandboxclid debugging'' and then shows that the deferd daemon spools the email and later releases the email from the queue folder after FortiSandbox processing.

Because sandboxclid is not one of the answer choices, the best answer among the listed FortiMail debug tools is deferd. It is the FortiMail daemon directly shown in the official lab workflow for troubleshooting submission-and-verdict handling. The other options in the answer list are not the ones the lab uses for FortiMail-to-FortiSandbox submission troubleshooting. So, based on the uploaded guide, diagnose debug application deferd is the correct choice.

Question 5

Question Type: MultipleChoice

On a FortiClient EMS integrated with FortiSandbox, how can you apply FortiSandbox profile configurations to endpoints even if they are off fabric? (Choose one answer)

Options:

A- As part of the fabric connectors configuration
B- As part of an endpoint workgroup configuration

C- As part of the endpoint policy configuration
D- As part of the sandbox profile configuration

Answer:

C

Explanation:

The FortiClient EMS Integration section is explicit on this point. It says: ''You must include the sandbox profile in the active endpoint policy.'' It then explains how off-fabric handling works: ''FortiClient on-fabric detection rules configured within the policy will classify endpoints as on-fabric or off-fabric. The Profile (Off-Fabric) setting allows you to select a second profile to be applied to endpoints when they are determined to be off-fabric.''

This means the control point for applying FortiSandbox-related behavior to off-fabric endpoints is the endpoint policy, not the fabric connector, not a workgroup, and not the sandbox profile by itself. The sandbox profile defines FortiSandbox behavior, but it must be attached through the active endpoint policy, where the Off-Fabric profile selection is made. Therefore, the correct answer is C. As part of the endpoint policy configuration.

Question 6

Question Type: MultipleChoice

A security analyst is reviewing a scan job report that indicates a true positive match. The job report displays that the malware attempts to replace vital system executables. Which type of malware is the analyst observing? (Choose one answer)

Options:

A- Exploit
B- Trojan
C- Dropper
D- Rootkit

Answer:

D

Explanation:

The Results Analysis section gives direct malware-type definitions. It says: ''A downloader attempts to download malicious content from a remote system'', ''A dropper installs malicious content'', ''A trojan appears to be a legitimate software application'', and most importantly, ''A rootkit attempts to hide its components by replacing valid system files.''

That exact wording matches the question statement about malware attempting to replace vital system executables. Replacing valid system files is classic rootkit behavior because the purpose is concealment and persistence by hiding malicious components behind trusted operating-system files. A dropper's main role is delivering payloads. A trojan is mainly deceptive software that appears legitimate. An exploit takes advantage of a vulnerability. None of those definitions match the described behavior as precisely as the rootkit definition in the Study Guide. Therefore, the malware type being observed is Rootkit.

Question 7

Question Type: MultipleChoice

You are asked to configure a FortiSandbox HA cluster. Port 4 on the primary and secondary nodes is dedicated for HA-specific communication. Which command must you use to configure the primary node? (Choose one answer)

Options:

A- hc-settings -sc -tN -nPrimaryNode -cFSAGrp -p -iport4
B- hc-settings -sc -tR -nPrimaryNode -cFSAGrp -p -iport4
C- hc-settings -sc -tF -nPrimaryNode -cFSAGrp -p -iport4
D- hc-settings -sc -tM -nPrimaryNode -cFSAGrp -p -iport4

Answer:

D

Explanation:

The Study Guide states that HA is configured from the CLI and that ''the main HA cluster CLI commands are hc-settings, hc-slave, and hc-status''. It also explains that ''You use the hc-settings command and options to configure the main HA settings... node alias, group name, group password, and the HA interface.'' The same HA section further says that the primary and secondary nodes must have a dedicated HA communication interface, and specifically notes that ''port4 in this example'' is the HA interface between them.

On the primary-node example configuration shown on page 137 of the uploaded study guide, the command uses -tM for the primary node with -iport4 for the HA interface. That directly matches option D. The other options use different node-type flags and do not correspond to the primary-node example. Therefore, the correct command is hc-settings -sc -tM -nPrimaryNode -cFSAGrp -p -iport4.

Question 8

Question Type: MultipleChoice

What is the default timeout value on FortiGate for inline scanning mode? (Choose one answer)

Options:

A- 300 seconds
B- 50 seconds
C- 40 minutes
D- 30 minutes

Answer:

B

Explanation:

The correct answer is B. 50 seconds. The Study Guide explicitly states: ''FortiGate holds the file while waiting for a verdict from FortiSandbox... The default file inspection timeout, and maximum, is 50 seconds.'' This is the clearest direct statement for the default timeout used with inline scanning mode on FortiGate.

The Lab Guide confirms the same design limit from the operational side. During the inline scanning exercise, it notes: ''Because of the inline scanning time-out limit (maximum of 50 seconds), it's not recommended to submit files for VM inspection.'' That reinforces that inline scanning is designed for quick decision phases such as active content, community cloud, antivirus, and static analysis, not long VM dynamic analysis jobs. Therefore, options A, C, and D are incorrect because they are far above the documented inline inspection limit. The default FortiGate inline scanning timeout is 50 seconds.

Thank You for trying FCP_FSA_AD-5.0 PDF Demo

To try our FCP_FSA_AD-5.0 practice exam software visit link below

https://prepbolt.com/FCP_FSA_AD-5.0.html

Start Your FCP_FSA_AD-5.0 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your FCP_FSA_AD-5.0 preparation with actual exam questions.