



Vendor: Fortinet

Exam Code: FCP_FSA_AD-5.0

Exam Name: Fortinet NSE 5 - FortiSandbox 5.0
Administrator

Version: DEMO

QUESTION 1

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?

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

Answer: D

Explanation:

Malware that attempts to replace or modify vital system executables is characteristic of a rootkit, which is designed to gain persistent, stealthy control over the system by altering core operating system components.

QUESTION 2

A manufacturing facility wants to enhance security for their OT environment by enabling the OT capabilities of FortiSandbox. After installing the LinuxOT VM, which two conditions must be met to complete this objective? (Choose two.)

- A. FortiSandbox must have at least one Windows VM clone.
- B. You must have a valid industrial security service license.
- C. There must be at least one ICAP adapter configured for OT network input.
- D. The LinuxOT VM must have the desired file types selected in the scan profile.

Answer: BD

Explanation:

OT capabilities require a valid industrial security service license to enable analysis features for industrial environments. The LinuxOT VM must also be configured in the scan profile with the appropriate file types so it can process and analyze OT-related files.

QUESTION 3

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?

- A. `hc-settings -sc -tN -nPrimaryNode -cFSAGrp -p<password> -iport4`
- B. `hc-settings -sc -tR -nPrimaryNode -cFSAGrp -p<password> -iport4`
- C. `hc-settings -sc -tP -nPrimaryNode -cFSAGrp -p<password> -iport4`
- D. `hc-settings -sc -tM -nPrimaryNode -cFSAGrp -p<password> -iport4`

Answer: C

Explanation:

The primary node in a FortiSandbox HA cluster is configured using the cluster setup command with the type parameter set to primary, along with the HA interface specified for cluster communication.

QUESTION 4

What is the default timeout value on FortiGate for inline scanning mode?

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

Answer: B

Explanation:

In inline scanning mode, FortiGate waits a limited time for a verdict from FortiSandbox before allowing or blocking the file. The default timeout is 50 seconds, ensuring timely traffic handling without excessive delay.

QUESTION 5

You notice a recent file downloaded by some end stations is exhibiting malware behavior, however, on the sandbox the file is rated clean. After further investigation you determine that only end stations using the Opera browser are being affected. What must you do to prevent these infections?

- A. Enable the STIX/TAXII Integration setting on FortiSandbox.
- B. Configure a custom VM to use the same browser as the exploited end stations.
- C. Modify the scan profile to include the malware file type.
- D. Change the job queue priority to process web-based files first.

Answer: B

Explanation:

Sandbox analysis accuracy depends on how closely the VM environment matches the real endpoint. Since the malware only affects systems using the Opera browser, creating a custom VM with the same browser allows FortiSandbox to properly replicate the behavior and detect the threat.

QUESTION 6

An organization has an existing FortiGate provisioned as a data center firewall (DCFV) that submits inbound files to FortiSandbox for inline scanning. As a result of a network redesign, traffic between the FortiSandbox and the DCFV 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?

- 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: B

Explanation:

For FortiGate inline scanning integration, FortiGate must be able to communicate with FortiSandbox over TCP/8890. If an intermediate firewall blocks that port, file submission and verdict exchange for inline scanning will fail.

QUESTION 7

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

- 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.

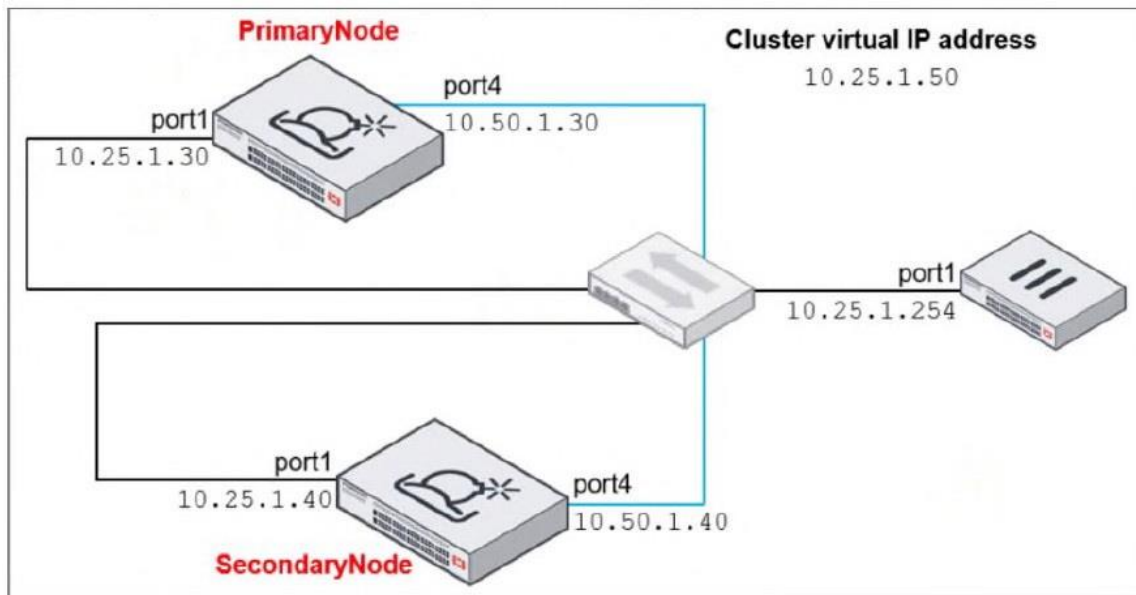
Answer: B

Explanation:

In an HA cluster, the primary node acts as the coordinator and distributes incoming jobs, including MTA jobs, across available resources such as itself and any connected worker nodes to balance the load and optimize processing.

QUESTION 8

Refer to the exhibit. Which command must you use to configure the FortiSandbox device as the primary node?



- 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: A

Explanation:

The primary node is configured using its own interface IP address. The diagram shows the primary node using port1 with IP address 10.25.1.30, which is the correct value for configuring it as the primary node.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14