Free Questions for 300-710 by actualtestdumps

Shared by Dunlap on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which protocol is needed to exchange threat details in rapid threat containment on Cisco FMC?

Options:

A- SGT

B- SNMP v3

C- BFD

D- pxGrid

Answer:

D

Question 2

Question Type: MultipleChoice

An engineer is troubleshooting a file that is being blocked by a Cisco FTD device on the network.

The user is reporting that the file is not malicious.

Which action does the engineer take to identify the file and validate whether or not it is malicious?

Options:

A- identify the file in the intrusion events and submit it to Threat Grid for analysis.

B- Use FMC file analysis to look for the file and select Analyze to determine its disposition.

C- Use the context explorer to find the file and download it to the local machine for investigation.

D- Right click the connection event and send the file to AMP for Endpoints to see if the hash is malicious.

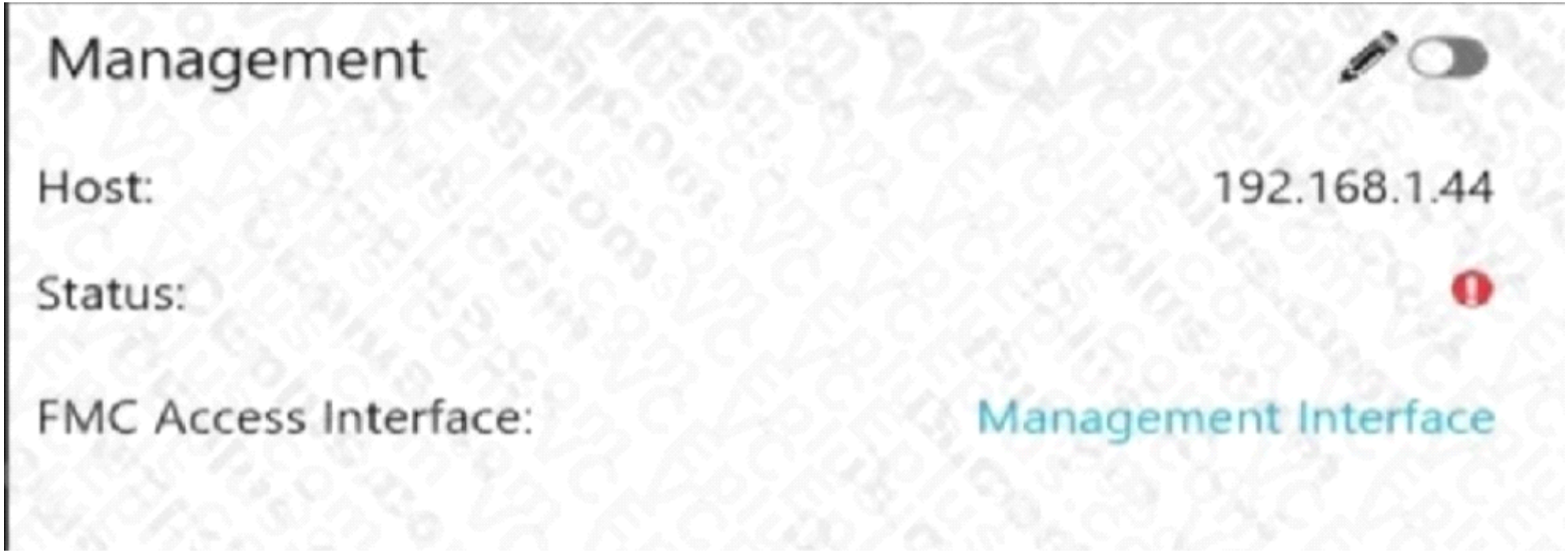
Answer:

A

Question 3

Question Type: **MultipleChoice**

Refer to the exhibit.



What is the effect of the existing Cisco FMC configuration?

Options:

A- The remote management port for communication between the Cisco FMC and the managed device changes to port 8443.

B- The managed device is deleted from the Cisco FMC.

C- The SSL-encrypted communication channel between the Cisco FMC and the managed device becomes plain-text communication

channel.

D- The management connection between the Cisco FMC and the Cisco FTD is disabled.

Answer:

D

Question 4

Question Type: MultipleChoice

An engineer wants to add an additional Cisco FTD Version 6.2.3 device to their current 6.2.3 deployment to create a high availability pair.

The currently deployed Cisco FTD device is using local management and identical hardware including the available port density to enable the failover and stateful links required in a proper high availability deployment. Which action ensures that the environment is ready to pair the new Cisco FTD with the old one?

Options:

A- Change from Cisco FDM management to Cisco FMC management on both devices and register them to FMC.

B- Ensure that the two devices are assigned IP addresses from the 169 254.0.0/16 range for failover interfaces.

C- Factory reset the current Cisco FTD so that it can synchronize configurations with the new Cisco FTD device.

D- Ensure that the configured DNS servers match on the two devices for name resolution.

Answer:

A

Question 5

Question Type: MultipleChoice

A network engineer sets up a secondary Cisco FMC that is integrated with Cisco Security Packet Analyzer What occurs when the secondary Cisco FMC synchronizes with the primary Cisco FMC?

Options:

A- The existing integration configuration is replicated to the primary Cisco FMC

B- The existing configuration for integration of the secondary Cisco FMC the Cisco Security Packet Analyzer is overwritten.

C- The synchronization between the primary and secondary Cisco FMC fails

D- The secondary Cisco FMC must be reintegrated with the Cisco Security Packet Analyzer after the synchronization

Answer:

B

Question 6

Question Type: MultipleChoice

What is the role of the casebook feature in Cisco Threat Response?

Options:

A- sharing threat analysts

B- pulling data via the browser extension

C- triage automaton with alerting

D- alert prioritization

Answer:

A

Explanation:

The casebook and pivot menu are widgets available in Cisco Threat Response. Casebook - It isused to record, organize, and share sets of observables of interest primarily during an investigation and threat analysis. You can use a casebook to get the current verdicts or dispositions on the observables.

https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_13-5-1/b_ESA_Admin_Guide_ces_13-5-1/b_ESA_Admin_Guide_13-0_chapter_0110001.pdf

Question 7

Question Type: MultipleChoice

Refer to the exhibit An engineer is modifying an access control pokey to add a rule to inspect all DNS traffic that passes through the firewall After making the change and deploying the pokey they see that DNS traffic is not bang inspected by the Snort engine What is the problem?

Options:

A- The rule must specify the security zone that originates the traffic

B- The rule must define the source network for inspection as well as the port

C- The action of the rule is set to trust instead of allow.

D- The rule is configured with the wrong setting for the source port

Answer:

C

Question 8

Question Type: MultipleChoice

An engineer is vorlang on a LAN switch and has noticed that its network connection to the mime Cisco IPS has gone down Upon troubleshooting it is determined that the switch is working as expected What must have been implemented for this failure to occur?

Options:

A- The upstream router has a misconfigured routing protocol

B- Link-state propagation is enabled

C- The Cisco IPS has been configured to be in fail-open mode

D- The Cisco IPS is configured in detection mode

Answer:

D