300-710 Q&As

Securing Networks with Cisco Firepower (SNCF)

Pass Cisco 300-710 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/300-710.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

An engineer is using the configure manager add Cisc404225383 command to add a new Cisco FTD device to the Cisco FMC; however, the device is not being added. Why is this occurring?

A. DONOTRESOLVE must be added to the command

B. The IP address used should be that of the Cisco FTD, not the Cisco FMC

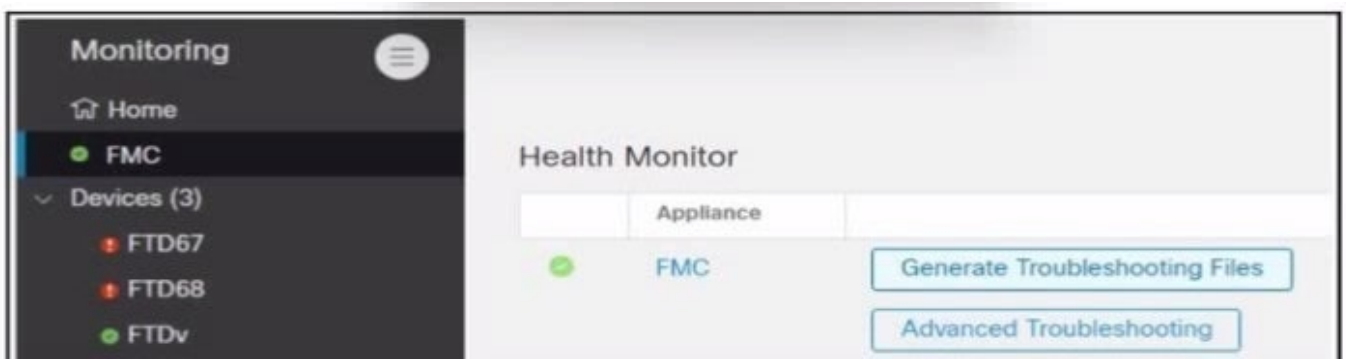
C. The registration key is missing from the command

D. The NAT ID is required since the Cisco FMC is behind a NAT device

Correct Answer: C

QUESTION 2

Refer to the exhibit.



An engineer generates troubleshooting files in Cisco Secure Firewall Management Center (FMC).

A successfully completed task Is removed before the files are downloaded.

Which two actions must be taken to determine the filename and obtain the generated troubleshooting files without regenerating them? (Choose two.)

A. Use an FTP client Hi expert mode on Secure FMC lo upload the files to the FTP server.

B. Go to the same screen as shown in the exhibit, click Advanced Troubleshooting, enter the rile name, and then start the download

C. Connect to CU on the FTD67 and FTD66 devices and copy the tiles from flash to the PIP server.

D. Go to expert mode on Secure FMC. list the contents of/Var/common, and determine the correct filename from the output

E. Click System Monitoring, men Audit to determine the correct filename from the line containing the Generate Troubleshooting Files string.

Correct Answer: DE

If a task to generate troubleshooting files in Cisco Secure Firewall Management Center (FMC) is completed successfully but removed before the files are downloaded, the following steps can be taken to determine the filename and obtain the

generated troubleshooting files without regenerating them:

Go to expert mode on Secure FMC:

Use the System Monitoring Audit logs:

These actions help identify and retrieve the generated troubleshooting files without the need to regenerate them, saving time and resources. References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on

Troubleshooting and File Management.

QUESTION 3

An engineer is configuring a Cisco Secure Firewall Threat Defense device managed by Cisco Secure Firewall Management Center. The device must have SSH enabled and be accessible from the inside interface for remote administration. Which type of policy must the engineer configure to accomplish this?

A. platform settings

B. access control

C. prefilter

D. identity

Correct Answer: A

To enable SSH access to a Cisco Secure Firewall Threat Defense (FTD) device from the inside interface for remote administration, the engineer needs to configure a Platform Settings policy in Cisco Secure Firewall Management Center

(FMC). The Platform Settings policy allows the configuration of various system-related settings, including enabling SSH, specifying the allowed interfaces, and defining the SSH access parameters.

Steps:

In FMC, navigate to Policies > Access Control > Platform Settings. Create a new Platform Settings policy or edit an existing one.

In the policy settings, go to the SSH section.

Enable SSH and specify the inside interface as the allowed interface for SSH access.

Define the SSH parameters such as allowed IP addresses, user credentials, and other security settings.

Save and deploy the policy to the FTD device.

This configuration ensures that SSH access is enabled on the specified interface, allowing secure remote administration.

References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Platform Settings.

QUESTION 4

An analyst is reviewing the Cisco FMC reports for the week. They notice that some peer-to- peer applications are being used on the network and they must identify which poses the greatest risk to the environment.

Which report gives the analyst this information?

A. Attacks Risk Report

B. User Risk Report

C. Network Risk Report

D. Advanced Malware Risk Report

Correct Answer: C

QUESTION 5

Which object type supports object overrides?

A. time range

B. security group tag

C. network object

D. DNS server group

Correct Answer: C

Object Overrides supported are: Network Port VLAN tag URL

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053