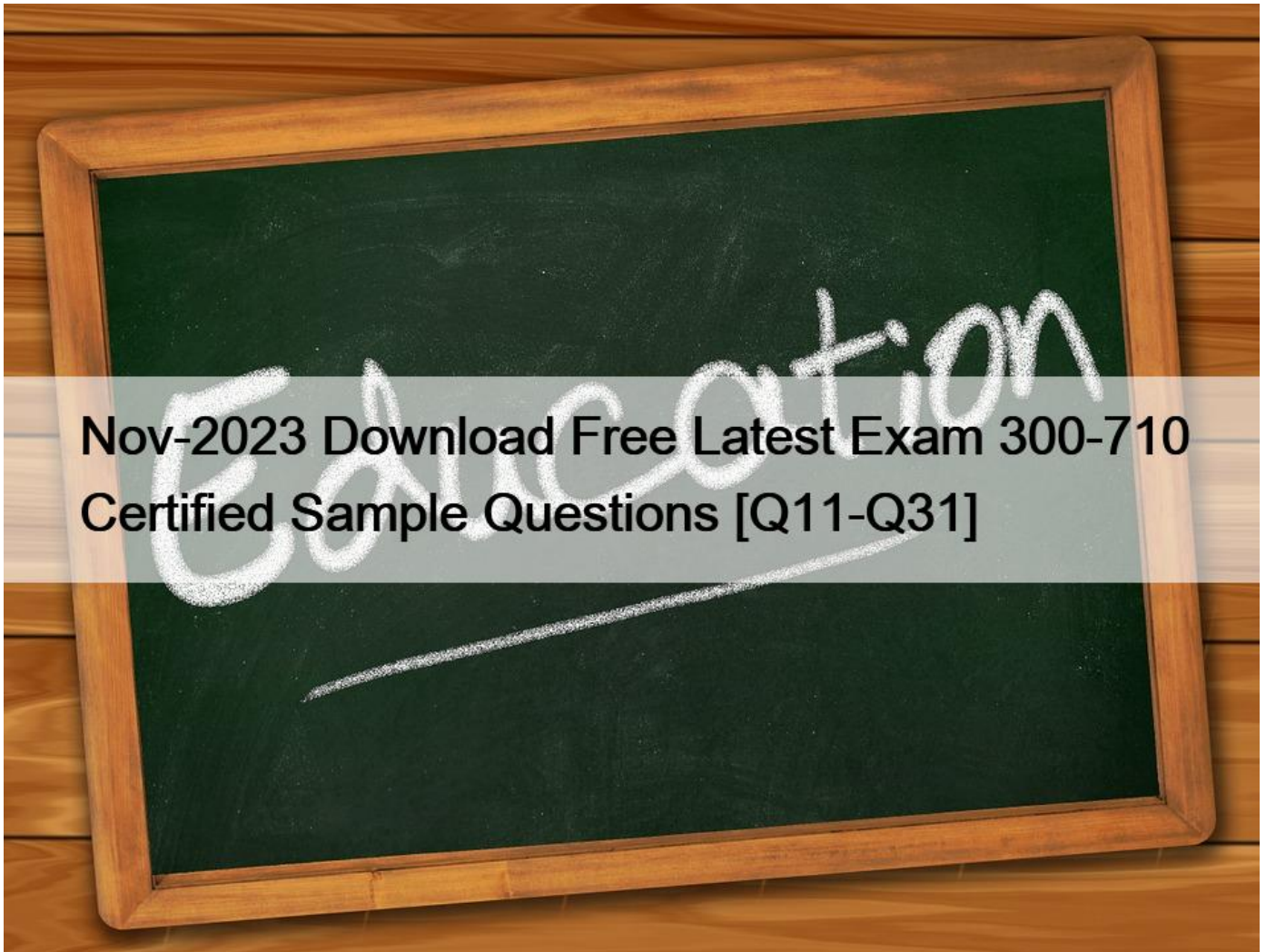


Nov-2023 Download Free Latest Exam 300-710 Certified Sample Questions [Q11-Q31]



Nov-2023 Download Free Latest Exam 300-710 Certified Sample Questions Prepare for your exam certification with our 300-710 Certified Cisco NEW QUESTION 11

An administrator is setting up a Cisco PMC and must provide expert mode access for a security engineer. The engineer is permitted to use only a secured out-of-band network workstation with a static IP address to access the Cisco FMC. What must be configured to enable this access?

- * Enable SSH and define an access list.
- * Enable HTTP and define an access list.
- * Enable SCP under the Access List section.
- * Enable HTTPS and SNMP under the Access List section.

NEW QUESTION 12

When do you need the file-size command option during troubleshooting with packet capture?

- * when capture packets are less than 16 MB
- * when capture packets are restricted from the secondary memory
- * when capture packets exceed 10 GB
- * when capture packets exceed 32 MB

NEW QUESTION 13

Drag and drop the steps to restore an automatic device registration failure on the standby Cisco FMC from the left into the correct order on the right. Not all options are used.

Enter the "configure manager add" command at the CLI of the affected device.	Step 1
Unregister the device from the standby Cisco FMC.	Step 2
Register the affected device on the active Cisco FMC.	Step 3
Enter the "configure manager delete" command at the CLI of the affected device.	Step 4
Register the affected device on the standby Cisco FMC.	
Unregister the device from the active Cisco FMC.	

Enter the "configure manager add" command at the CLI of the affected device.	Unregister the device from the active Cisco FMC.
Unregister the device from the standby Cisco FMC.	Enter the "configure manager delete" command at the CLI of the affected device.
Register the affected device on the active Cisco FMC.	Enter the "configure manager add" command at the CLI of the affected device.
Enter the "configure manager delete" command at the CLI of the affected device.	Register the affected device on the active Cisco FMC.
Register the affected device on the standby Cisco FMC.	
Unregister the device from the active Cisco FMC.	

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html#id_32288

NEW QUESTION 14

The event dashboard within the Cisco FMC has been inundated with low priority intrusion drop events, which are overshadowing high priority events. An engineer has been tasked with reviewing the policies and reducing the low priority events. Which action should be configured to accomplish this task?

- * generate events
- * drop packet
- * drop connection
- * drop and generate

NEW QUESTION 15

Drag and drop the steps to restore an automatic device registration failure on the standby Cisco FMC from the left into the correct order on the right. Not all options are used.

Enter the "configure manager add" command at the CLI of the affected device.	Step 1
Unregister the device from the standby Cisco FMC.	Step 2
Register the affected device on the active Cisco FMC.	Step 3
Enter the "configure manager delete" command at the CLI of the affected device.	Step 4
Register the affected device on the standby Cisco FMC.	
Unregister the device from the active Cisco FMC.	

Enter the "configure manager add" command at the CLI of the affected device.	Unregister the device from the standby Cisco FMC.
Unregister the device from the standby Cisco FMC.	Enter the "configure manager delete" command at the CLI of the affected device.
Register the affected device on the active Cisco FMC.	Enter the "configure manager add" command at the CLI of the affected device.
Enter the "configure manager delete" command at the CLI of the affected device.	Register the affected device on the active Cisco FMC.
Register the affected device on the standby Cisco FMC.	
Unregister the device from the active Cisco FMC.	

Explanation

Unregister the device from the active Cisco FMC.

Enter the "configure manager delete" command at the CLI of the affected device.

Enter the "configure manager add" command at the CLI of the affected device.

Register the affected device on the active Cisco FMC.

Explanation

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html#id_32288

NEW QUESTION 16

In a Cisco AMP for Networks deployment, which disposition is returned if the cloud cannot be reached?

- * unavailable
- * unknown
- * clean
- * disconnected

NEW QUESTION 17

administrator is configuring SNORT inspection policies and is seeing failed deployment messages in Cisco FMC . What information should the administrator generate for Cisco TAC to help troubleshoot?

- * A Troubleshoot” file for the device in question.
- * A “show tech” file for the device in question
- * A “show tech” for the Cisco FMC.
- * A “troubleshoot” file for the Cisco FMC

NEW QUESTION 18

How many report templates does the Cisco Firepower Management Center support?

- * 20
- * 10
- * 5
- * unlimited

Section: Management and Troubleshooting

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

NEW QUESTION 19

A network administrator notices that SI events are not being updated The Cisco FTD device is unable to load all of the SI event

entries and traffic is not being blocked as expected. What must be done to correct this issue?

- * Restart the affected devices in order to reset the configurations
- * Manually update the SI event entries to that the appropriate traffic is blocked
- * Replace the affected devices with devices that provide more memory
- * Redeploy configurations to affected devices so that additional memory is allocated to the SI module

NEW QUESTION 20

When do you need the file-size command option during troubleshooting with packet capture?

- * when capture packets are less than 16 MB
- * when capture packets are restricted from the secondary memory
- * when capture packets exceed 10 GB
- * when capture packets exceed 32 MB

Section: Management and Troubleshooting

Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.html

NEW QUESTION 21

A Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface. What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace?

- * The destination MAC address is optional if a VLAN ID value is entered
- * Only the UDP packet type is supported
- * The output format option for the packet logs is unavailable
- * The VLAN ID and destination MAC address are optional

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.html

NEW QUESTION 22

Which license type is required on Cisco ISE to integrate with Cisco FMC pxGrid?

- * mobility
- * plus
- * base
- * apex

NEW QUESTION 23

Which two routing options are valid with Cisco Firepower Threat Defense? (Choose two.)

- * BGPv6
- * ECMP with up to three equal cost paths across multiple interfaces
- * ECMP with up to three equal cost paths across a single interface
- * BGPv4 in transparent firewall mode
- * BGPv4 with nonstop forwarding

Section: Configuration

Explanation/Reference: <https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config->

guide-v601/fpmc-config-guide-v60_chapter_01100011.html#ID-2101-0000000e

NEW QUESTION 24

What is the maximum SHA level of filtering that Threat Intelligence Director supports?

- * SHA-1024
- * SHA-4096
- * SHA-512
- * SHA-256

NEW QUESTION 25

Which interface type allows packets to be dropped?

- * passive
- * inline
- * ERSPAN
- * TAP

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring-firepower-threat-defense-int.html>

NEW QUESTION 26

An engineer is configuring a cisco FTD appliance in IPS-only mode and needs to utilize fail-to-wire interfaces. Which interface mode should be used to meet these requirements?

- * transparent
- * routed
- * passive
- * inline set


NEW QUESTION 27

Drag and drop the steps to restore an automatic device registration failure on the standby Cisco FMC from the left into the correct order on the right. Not all options are used.

Enter the "configure manager add" command at the CLI of the affected device.	Step 1
Unregister the device from the standby Cisco FMC.	Step 2
Register the affected device on the active Cisco FMC.	Step 3
Enter the "configure manager delete" command at the CLI of the affected device.	Step 4
Register the affected device on the standby Cisco FMC.	
Unregister the device from the active Cisco FMC.	

Enter the "configure manager add" command at the CLI of the affected device.	Unregister the device from the active Cisco FMC.
Unregister the device from the standby Cisco FMC.	Enter the "configure manager delete" command at the CLI of the affected device.
Register the affected device on the active Cisco FMC.	Enter the "configure manager add" command at the CLI of the affected device.
Enter the "configure manager delete" command at the CLI of the affected device.	Register the affected device on the active Cisco FMC.
Register the affected device on the standby Cisco FMC.	
Unregister the device from the active Cisco FMC.	

NEW QUESTION 28



II. ASSESSMENT RESULTS

AUTOMATING THE TUNING EFFORT

During the assessment period, the following changes to your network were observed.

NETWORK CHANGE TYPE	NUMBER OF CHANGES
A new operating system was found	310
A new host was added to the network	366
A device started using a new transport protocol	381
A device started using a new network protocol	373

Refer to the exhibit. An engineer is analyzing the Attacks Risk Report and finds that there are over 300 instances of new operating systems being seen on the network. How is the Firepower configuration updated to protect these new operating systems?

- * The administrator manually updates the policies.
- * The administrator requests a Remediation Recommendation Report from Cisco Firepower.
- * Cisco Firepower gives recommendations to update the policies.
- * Cisco Firepower automatically updates the policies.

Section: Management and Troubleshooting

NEW QUESTION 29

What is the result of specifying of QoS rule that has a rate limit that is greater than the maximum throughput of an interface?

- * The rate-limiting rule is disabled.
- * Matching traffic is not rate limited.
- * The system rate-limits all traffic.
- * The system repeatedly generates warnings.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/quality_of_service_qos.pdf

NEW QUESTION 30

What is the maximum bit size that Cisco FMC supports for HTTPS certificates?

- * 1024
- * 8192
- * 4096
- * 2048

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/system_configuration.html

NEW QUESTION 31

In a Cisco AMP for Networks deployment, which disposition is returned if the cloud cannot be reached?

- * unavailable
- * unknown
- * clean
- * disconnected

Section: Integration

Explanation/Reference:

Cisco 300-710 (Securing Networks with Cisco Firepower) certification exam is designed to test the knowledge and skills of network security professionals who use Cisco Firepower Next-Generation Firewall (NGFW), web security, and email security appliances. 300-710 exam focuses on the deployment, configuration, and management of Cisco Firepower NGFW, including its integration with other Cisco security solutions. Securing Networks with Cisco Firepower certification is intended for security engineers, network designers, and administrators who want to enhance their knowledge and skills in network security.

Obtaining the Cisco 300-710 certification validates the skills and knowledge of network security professionals in deploying and managing Cisco Firepower NGFW and its associated security solutions. Securing Networks with Cisco Firepower certification can increase job opportunities and enhance career growth for professionals in the network security field. It also helps organizations ensure that their network security professionals have the necessary skills to secure their networks against modern security threats.

Free Cisco 300-710 Exam 2023 Practice Materials Collection: <https://www.topexamcollection.com/300-710-vce-collection.html>