156-315.81 Q&As

Check Point Certified Security Expert R81

Pass CheckPoint 156-315.81 Exam with 100% Guarantee

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

https://www.geekcert.com/156-315-81.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Bob needs to know if Alice was configuring the new virtual cluster interface correctly. Which of the following Check Point commands is true?

A. cphaprob-aif

B. cp hap rob state

C. cphaprob list

D. probcpha -a if

Correct Answer: A

You can use the cphaprob -a if command to check the status of the virtual cluster interface1. This command displays the state, virtual IP address, and physical IP address of each cluster interface2. It also shows the load balancing method,

the load on each interface, and the active member for each interface2. This command can help you verify that Alice configured the virtual cluster interface correctly and that it is working properly. To run this command, you need to access the

cluster member in Clish and run cphaprob -a if1.

References: How to configure ClusterXL in Load Sharing Unicast mode - Check Point Software, cphaprob -a if - Check Point Software

QUESTION 2

Please choose correct command to add an "emailserver1" host with IP address 10.50.23.90 using GAiA management CLI?

A. host name myHost12 ip-address 10.50.23.90

B. mgmt: add host name ip-address 10.50.23.90

C. add host name emailserver1 ip-address 10.50.23.90

D. mgmt: add host name emailserver1 ip-address 10.50.23.90

Correct Answer: D

The correct command to add an "emailserver1" host with IP address 10.50.23.90 using GAiA management CLI is mgmt: add host name emailserver1 ip-address 10.50.23.90. This command will create a new host object in the Security Management Server database, with the specified name and IP address. The mgmt: prefix indicates that the command is executed on the Security Management Server, and not on the local GAiA machine. The other commands are either missing the mgmt: prefix, or have incorrect syntax or parameters.

QUESTION 3

Which of the following Check Point processes within the Security Management Server is responsible for the receiving of log records from Security Gateway?

A. logd

B. fwd

C. fwm

D. cpd

Correct Answer: B

The fwd process within the Security Management Server is responsible for the receiving of log records from Security Gateway. The fwd process handles the communication with the Security Gateways and log servers via TCP port 2571. The other processes have different roles, such as logd for writing logs to the database, fwm for handling GUI clients, and cpd for infrastructure tasks2. References: Check Point Ports Used for Communication by Various Check Point Modules, Check Point Processes Cheat Sheet ?LazyAdmins

QUESTION 4

Please choose the path to monitor the compliance status of the Check Point R81.20 based management.

A. Gateways and Servers --> Compliance View

B. Compliance blade not available under R81.20

C. Logs and Monitor --> New Tab --> Open compliance View

D. Security and Policies --> New Tab --> Compliance View

Correct Answer: C

The path to monitor the compliance status of the Check Point R81.20 based management is Logs and Monitor > New Tab > Open compliance View. Compliance View is a feature that allows administrators to monitor and assess the compliance level of their Check Point products and security policies based on best practices and industry standards. Compliance View provides a dashboard that shows the overall compliance status, compliance score, compliance trends, compliance issues, compliance reports, and compliance blades for different security aspects, such as data protection, threat prevention, identity awareness, etc. To access Compliance View in R81.20 SmartConsole, administrators need to go to Logs and Monitor > New Tab > Open compliance View. The other options are either incorrect or not available in R81.20.

QUESTION 5

What makes Anti-Bot unique compared to other Threat Prevention mechanisms, such as URL Filtering, Anti-Virus, IPS, and Threat Emulation?

A. Anti-Bot is the only countermeasure against unknown malware

B. Anti-Bot is the only protection mechanism which starts a counter-attack against known Command and Control Centers

C. Anti-Bot is the only signature-based method of malware protection.

D. Anti-Bot is a post-infection malware protection to prevent a host from establishing a connection to a Command and Control Center.

Correct Answer: D

Anti-Bot is a post-infection malware protection that detects and blocks botnet communications from infected hosts to Command and Control servers. It is different from other Threat Prevention mechanisms that prevent malware from entering the network or executing on the hosts. References: Anti-Bot Software Blade