156-115.80^{Q&As}

Check Point Certified Security Master - R80

Pass CheckPoint 156-115.80 Exam with 100% Guarantee

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

https://www.pass4itsure.com/156-115-80.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

Which of the following commands can be used to see the list of processes monitored by the Watch Dog process?

A. cpwd_admin list

B. ps –ef | grep watchd

C. cpstat fw –f watchdog

D. fw ctl get str watchdog

Correct Answer: A

Reference: https://community.checkpoint.com/thread/8054-cpwdadmin-list-overview-sms

QUESTION 2

Which command will register the host_monitor device and checks end-to-end connectivity to routers and other network devices?

A. clusterXL_monitor_ips

B. clusterXL_monitor_admin

C. clusterXL_monitor_process

D. clusterXL_admin

Correct Answer: A

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_ClusterXL_WebAdminGuide/ html_frameset.htm?topic=documents/R77/CP_R77_ClusterXL_WebAdminGuide/7298

QUESTION 3

What is the recommended command to manually initiate a failover on a cluster member in HA?

A. Perform a cpstop on the standby member

B. Perform a clusterXL_admin down on the standby member

C. Perform a cpstop on the active member

D. Perform a clusterXL_admin down on the active member

Correct Answer: D

Reference: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/ CP_R81_CLI_ReferenceGuide/Topics-CLIG/CXLG/Initiating-Manual-Cluster-Failover.htm

QUESTION 4

What ClusterXL mechanism is used to verify that the interfaces of other cluster members are UP and communicates the status of cluster members?

A. PING

B. CCP

C. PPP

D. HELLO

Correct Answer: B

QUESTION 5

The maximum number of critical devices or pnotes on a cluster member is what?

A. 8

B. 24

C. 32

D. 16

Correct Answer: D

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7298.htm

QUESTION 6

Which Threat Prevention daemon is the core Threat Emulation engine and responsible for emulation files and communications with Threat Cloud?

A. ctasd

B. in.msd

C. ted

D. scrub

Correct Answer: C

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?
eventSubmit_doGoviewsolutiondetails=andsolutionid=sk97638

QUESTION 7

What file extension should be used with fw monitor to allow the output file to be imported and read in Wireshark?

A. .cap

B. .exe

C. .tgz

D. .pcap

Correct Answer: A

QUESTION 8

URL Filtering is an essential part of Web Security in the Gateway. For the Security Gateway to perform a URL lookup when a client makes a URL request, where is the sync-request forwarded from if a sync-request is required?

A. RAD Kernel Space

B. URLF Kernel Client

C. URLF Online Service

D. RAD User Space

Correct Answer: B

Reference: https://community.checkpoint.com/thread/9034-url-filtering-using-dns

QUESTION 9

In a high traffic network, which feature allows for more than one traffic path on an interface so that more than one CPU can be used for acceleration?

A. interface bonding

B. vlan

C. asic

D. multi queue

Correct Answer: D

Reference: https://sc1.checkpoint.com/documents/R76/ CP_R76_PerformanceTuning_WebAdmin/93689.htm

QUESTION 10

Where do Protocol parsers register themselves for IPS?

A. Passive Streaming Library

B. Other handlers register to Protocol parser

C. Protections database

D. Context Management Infrastructure

Correct Answer: A

Reference: http://www.nwtechusa.com/pdf/checkpoint_blade_ips.pdf

QUESTION 11

An administrator is creating a new site-to-site VPN connection. The agreed settings are AES256 and SHA256. If Elliptic Curve type transforms are required then what can be specifically configured to achieve this level of security?

A. Protocol 50 with AES

B. Diffie-Hellman Group 20

C. Perfect Forward Secrecy

D. AH should replace ESP

Correct Answer: B

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?
eventSubmit_doGoviewsolutiondetails=andsolutionid=sk27054

QUESTION 12

IPS detection incorporates 4 layers. Which of the following is NOT a layer in IPS detection?

A. Context Management

B. Protocol Parsers

C. Protections

D. Detections

Correct Answer: D

QUESTION 13

Which one of following commands should you run to display HTTPS packet content together with kernel debug?

A. fw ctl get int https_inspection_show_decrypted_data_in_debug=1 fw ctl get int ssl_inspection_extra_debug=1

B. fw set int https_inspection_get_encrypted_data_in_debug 1 fw set int https_inspection_show_debug 1

C. fw ctl set int https_inspection_show_decrypted_data_in_debug 1 fw ctl set int ssl_inspection_extra_debug 1

D. fw ctl set int http_inspection_display_encrypted_data_in_debug=1 fw ctl set int http_inspection_extra_debug=1

Correct Answer: C

QUESTION 14

For organizations with existing IPv4 networks who wish to move to IPv6, which of the following is a Transition Mechanism that can be used?

A. ipv4 to ipv6 Triple Stack

B. Hex to Dec translation

C. 6 in 4 Tunneling

D. NAT-T to NAT6sec

Correct Answer: C

QUESTION 15

Which of the following is correct in a Threat Prevention policy?

A. Threat Prevention inspects traffic to all objects specified in the Protected Scope

B. Threat Prevention inspects traffic to and/or from all objects specified in the Protected Scope

C. Threat Prevention is applied based on the profile. Protection Scope does not have any relevance

D. Threat Prevention inspects traffic from all objects specified in the protected Scope

Correct Answer: B

Reference: https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/ CP_R80.10_ThreatPrevention_AdminGuide/html_frameset.htm?topic=documents/R80.10/ WebAdminGuides/EN/ CP_R80.10_ThreatPrevention_AdminGuide/136933

[Latest 156-115.80 Dumps](#)   [156-115.80 PDF Dumps](#)   [156-115.80 Braindumps](#)