[20/June/2018 Updated Latest PassLeader 365q 156-915.80 Exam Dumps Collection (Part A)

New Updated 156-915.80 Exam Questions from PassLeader 156-915.80 PDF dumps! Welcome to download the newest PassLeader 156-915.80 VCE dumps: https://www.passleader.com/156-915-80.html (365 Q&As)
Keywords: 156-915.80 exam dumps, 156-915.80 exam questions, 156-915.80 VCE dumps, 156-915.80 PDF dumps, 156-915.80 practice tests, 156-915.80 study guide, 156-915.80 braindumps, Check Point Certified Security Expert Update - R80 Exam
P.S. New 156-915.80 dumps PDF: https://drive.google.com/open?id=1HMGEPKVBag2Bm5dUy2POfhbnpk-1-vCT
NEW QUESTION 266
Which is the correct order of a log flow processed by SmartEvents components?
A. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client
B. Firewall > SmartEvent Server Database > Correlation unit > Log Server > SmartEvent Client
C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client
D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client

Answer: D
NEW QUESTION 267
In SmartEvent, what are the different types of automatic reactions that the administrator can configure?
A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
B. Mail, Block Source, Block Destination, Block Services, SNMP Trap
C. Mail, Block Source, Block Destination, External Script, SNMP Trap
D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap
Answer: A
NEW QUESTION 268
Which components allow you to reset a VPN tunnel?
A. vpn command or SmartView monitor
B. delete or vpn shell command:
vpn ike sa
C. vpn or delete vpn command:
tunnelutil ike sa
D. SmartView monitor only
Answer: D
NEW QUESTION 269
When synchronizing clusters, which of the following statements is FALSE?
A. The state of connections using resources is maintained in a Security Server, so their connections cannot be synchronized.
B. Only cluster members running on the same OS platform can be synchronized.
C. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization.
D. Client Authentication or Session Authentication connections through a cluster member will be lost if the cluster member fails.
Answer: D
NEW QUESTION 270
Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?
A. The rule base can be built of layers, each containing a set of the security rules.
Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
B. Limits the upload and download throughout for streaming media in the company to 1 Gbps.
C. Time object to a rule to make the rule active only during specified times.
D. Sub Policies are sets of rules that can be created and attached to specific rules.
If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.
Answer: A

NEW QUESTION 271
In R80.10, how do you manage your Mobile Access Policy?
A. Through the Unified Policy
B. Through the Mobile Console
C. From SmartDashboard
D. From the Dedicated Mobility Tab
Answer: C
NEW QUESTION 272
You find one of your cluster gateways showing "Down" when you run the "cphaprob stat" command. You then run the "clusterXL_admin up" on the down member but unfortunately the member continues to show down. What command do you run to determine the case?
A. cphaprob -f register
B. cphaprob -d-s report
C. cpstat -f-all
D. cphaprob -a list
Answer: D
NEW QUESTION 273
SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?
A. Smart Cloud Services
B. Load Sharing Mode Services
C. Threat Agent Solution
D. Public Cloud Services
Answer: C
NEW QUESTION 274
Which of the following is NOT a valid way to view interface's IP address settings in Gaia?
A. Using the command sthtool in Expert Mode
B. Viewing the file /config/active
C. Via the Gaia WebUl
D. Via the command show in CLISH:
configuration
Answer: A
NEW QUESTION 275
Check Point recommends configuring Disk Space Management parameters to delete old log entities when available disk space is less than or equal to?
A. 50%
B. 75%
C. 80%
D. 15%
Answer: D
NEW QUESTION 276
What API command below creates a new host with the name "New Host" and IP address of "192.168.0.10"?
A. new host name "New Host" ip-address "192.168.0.10"
B. set host name "New Host" ip-address "192.168.0.10"
C. create host name "New Host" ip-address "192.168.0.10"
D. add host name "New Host" ip-address "192.168.0.10"
Answer: D
NEW QUESTION 277
What are types of Check Point APIs available currently as part of R80.10 code?
A. Security Gateway API, Management API, Threat Prevention API and Identity Awareness Web Services API

B. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
C. OSE API, OPSEC SDK API, Threat Extraction API and Policy Editor API
D. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API
Answer: B
NEW QUESTION 278
Which of the following is NOT an internal/native Check Point command?
A. fwaccel
on
B. fw
ct1 debug
C. tcpdump
D. cphaprob
Answer: C
NEW QUESTION 279
What is the SandBlast Agent designed to do?
A. Performs OS-level sandboxing for SandBlast Cloud architecture.
B. Ensure the Check Point SandBlast services is running on the end user's system.
C. If malware enters an end user's system, the SandBlast Agent prevents the malware form spreading with the network.
D. Clean up email sent with malicious attachments.
Answer: C
NEW QUESTION 280
The SmartEvent R80 Web application for real-time event monitoring is called what?
A. SmartView Monitor
B. SmartEventWeb
C. There is no Web application for SmartEvent
D. SmartView
Answer: A
NEW QUESTION 281
What Shell is required in Gaia to use WinSCP?
A. UNIX
B. CPShell
C. CLISH
D. Bash
Answer: D
NEW QUESTION 282
Which one of the following is true about Threat Emulation?
A. Takes less than a second to complete
B. Works on MS Office and PDF files only
C. Always delivers a file
D. Takes minutes to complete (less than 3 minutes)
Answer: D
NEW QUESTION 283
What are the minimum open server hardware requirements for a Security Management Server/Standalone in R80.10?
A. 2 CPU cores, 4GB of RAM and 15GB of disk space
B. 8 CPU cores, 16GB of RAM and 500GB of disk space
C. 4 CPU cores, 8GB of RAM and 500GB of disk space
D. 8 CPU cores, 32GB of RAM and 1TB of disk space
Answer: C
NEW QUESTION 284
The "MAC magic" value must be modified under which of the following condition?

A. There is more than one cluster connected to the same VLAN.
B. A firewall cluster is configured to use Multicast for CCP traffic.
C. There are more than two members in a firewall cluster.
D. A firewall cluster is configured to use Broadcast for CCP traffic.
Answer: D
NEW QUESTION 285
The Correlation Unit performs all but which of the following actions?
A. Marks logs that individually are not events, but may be part of a larger pattern to be identified later.
B. Generates an event based on the Event policy.
C. Assigns a severity level to the event.
D. Takes a new log entry that is part of a group of items that together make up an event, and adds it to an ongoing event.
Answer: C
NEW QUESTION 286
Which of the following command is used to verify the CPUSE version?
A. HostName:0>show installer status build
B. [Expert@HostName:0]#show installer status
C. [Expert@HostName:0]#show installer status build
D. HostName:0>show installer build
Answer: A
NEW QUESTION 287
Which statement is true regarding redundancy?
A. System Administrator know when their cluster has failed over and can also see why it failed over by using the cphaprob -f it command.
B. ClusterXL offers three different Load Sharing solutions: Unicast, Broadcast, and Multicast.
C. Machines in a Cluster XL High Availability configuration must be synchronized.
D. Both Cluster XL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments.
Answer: D
NEW QUESTION 288
Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via e-mail. An e-mail with Security_ report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links. Which component of SandBlast protection is her company using on a Gateway?
A. SandBlast Threat Emulation
B. SandBlast Agent
C. Check Point Protect
D. SandBlast Threat Extraction
Answer: D
NEW QUESTION 289
Which command collects diagnostic data for analyzing customer setup remotely?
A. cpinfo
B. migrate export
C. sysinfo
D. cpview
Answer: A
NEW QUESTION 290
When deploying multiple clustered firewalls on the same subnet, what does the firewall administrator need to configure to prevent CCP broadcasts being sent to the wrong cluster?
A. Set the fwha_mac_magic_forward parameter in the $CPDIR/boot/modules/ha_boot. conf
B. Set the fwha_mac_magic parameter in the $FWDIR/boot/fwkern.conf file

C. Set the cluster global ID using the command "cphaconf cluster_id set <value>"
D. Set the cluster global ID using the command "fw ctt set cluster_id <value>"
Answer: C
NEW QUESTION 291
Which of these options is an implicit MEP option?
A. Primary-backup
B. Source address based
C. Round robin
D. Load Sharing
Answer: A
NEW QUESTION 292
John detected high load on sync interface. Which is most recommended solution?
A. For short connections like http service, delay sync for 2 seconds.
B. Add a second interface to handle sync traffic.
C. For short connections like http service, do not sync.
D. For short connections like icmp service, delay sync for 2 seconds.
Answer: A
NEW QUESTION 293
What is the SOLR database for?
A. Used for full text search and enables powerful matching capabilities.
B. Writes data to the database and full text search.
C. Serves GUI responsible to transfer request to the DLEserver.
D. Enables powerful matching capabilities and writes data to the database.
Answer: A
NEW QUESTION 294
What is a feature that enables VPN connections to successfully maintain a private and secure VPN session without employing Stateful Inspection?
A. Stateful Mode
B. VPN Routing Mode
C. Wire Mode
D. Stateless Mode
Answer: C
NEW QUESTION 295
On R80.10 the IPS Blade is managed by ____.
A. Threat Protection Policy
B. Anti-Bot Blade
C. Threat Prevention Policy
D. Layers on Firewall Policy
Answer: A
NEW QUESTION 296
Which packet info is ignored with Session Rate Acceleration?
A. source port ranges
B. source ip
C. source port
D. same info from Packet Acceleration is used
Answer: C
NEW QUESTION 297
What is the purpose of Priority Delta in VRRP?
A. When a box is up, Effective Priority = Priority + Priority Delta.
B. When an Interface is up, Effective Priority = Priority + Priority Delta.

C. When an Interface fail, Effective Priority = Priority + Priority Delta.
D. When a box fail, Effective Priority = Priority + Priority Delta.
Answer: C
NEW QUESTION 298
What is the purpose of a SmartEvent Correlation Unit?
A. The SmartEvent Correlation Unit is designed to check the connection reliability from SmartConsole to the SmartEvent Server.
B. The SmartEvent Correlation Unit's task it to assign severity levels to the identified events.
C. The Correlation unit role is to evaluate logs from the log server component to identify patterns/threats and convert them to events.
D. The SmartEvent Correlation Unit is designed to check the availability of the SmartReporter Server.
Answer: C
NEW QUESTION 299
The CDT utility supports which of the following?
A. Major version upgrades to R77.30
B. Only Jumbo HFA's and hotfixes
C. Only major version upgrades to R80.10
D. All upgrades
Answer: D
NEW QUESTION 300
The Firewall kernel is replicated multiple times, therefore ____.
A. the Firewall kernel only touches the packet if the connection is accelerated
B. the Firewall can run different policies per core
C. the Firewall kernel is replicated only with new connections and deletes itself once the connection times out
D. the Firewall can run the same policy on all cores
Answer: D
NEW QUESTION 301
Sticky Decision Function (SDF) is required to prevent which of the following assume you set up an Active-Active cluster?
A. Symmetric routing
B. Failovers
C. Asymmetric routing
D. Anti-Spoofing
Answer: C
NEW QUESTION 302
Which is not a blade option when configuring SmartEvent?
A. Correlation Unit
B. SmartEvent Unit
C. SmartEvent Server
D. Log Server
Answer: B
NEW QUESTION 303
What command would show the API server status?
A. cpm status
B. api restart
C. api status
D. show api status
Answer: C
NEW QUESTION 304
You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

A. fw cti multik dynamic_dispatching on
B. fw cti multik dynamic_dispatching set_mode 9
C. fw cti multik set_mode 9
D. fw cti multik pq enable
Answer: C
NEW QUESTION 305
You have existing dbedit scripts from R77. Can you use them with R80.10?
A. dbedit is not supported in R80.10.
B. dbedit is fully supported in R80.10.
C. You can use dbedit to modify threat prevention or access policies, but not create or modify layers.
D. dbedit scripts are being replaced by mgmt_cli in R80.10.
Answer: D
NEW QUESTION 306
SecureXL improves non-encrypted firewall traffic throughput and encrypted VPN traffic throughput. True or false?
A. This statement is true because SecureXL does improve all traffic.
B. This statement is false because SecureXL does not improve this traffic but CoreXL does.
C. This statement is true because SecureXL does improve this traffic.
D. This statement is false because encrypted traffic cannot be inspected.
Answer: C
NEW QUESTION 307
What are the three components for Check Point Capsule?
A. Capsule Docs, Capsule Cloud, Capsule Connect
B. Capsule Workspace, Capsule Cloud, Capsule Connect
C. Capsule Workspace, Capsule Docs, Capsule Connect
D. Capsule Workspace, Capsule Docs, Capsule Cloud
Answer: D
NEW QUESTION 308
When using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?
A. mgmt_cli add host "Server_1" ip-address "10.15.123.10" -format txt
B. mgmt_cli add host name "Server_1" ip-address "10.15.123.10" -format json
C. mgmt_cli add object host "Server_1" ip-address "10.15.123.10" -format json
D. mgmt_cli add object "Server_1" ip-address "10.15.123.10" -format json
Answer: B
NEW QUESTION 309
When defining QoS global properties, which option below is not valid?
A. Weight
B. Authenticated timeout
C. Schedule
D. Rate
Answer: C
NEW QUESTION 310
Check Point APIs allow system engineers and developers to make changes to their organization's security policy with CLI tools and Web Services for all of the following except?
A. Create new dashboards to manage 3rd party task.
B. Create products that use and enhance 3rd party solutions.
C. Execute automated scripts to perform common tasks.
D. Create products that use and enhance the Check Point Solution.
Answer: A
NEW QUESTION 311
What happen when IPS profile is set in Detect-Only Mode for troubleshooting?

A. It will generate Geo-Protection traffic.
B. Automatically uploads debugging logs to Check Point Support Center.
C. It will not block malicious traffic.
D. Bypass licenses requirement for Geo-Protection control.
Answer: C
NEW QUESTION 312
When simulating a problem on CLusterXL cluster with cphaprob -d STOP -s problem -t 0 register, to initiate a failover on an active cluster member, which command allows you remove the problematic state?
A. cphaprob -d STOP unregister
B. cphaprob STOP unregister
C. cphaprob unregister STOP
D. cphaprob -d unregister STOP
Answer: A
NEW QUESTION 313
You are investigating issues with two gateway cluster members that are not able to establish the first initial cluster synchronization. What service is used by the FWD daemon to do a Full Synchronization?
A. TCP port 443
B. TCP port 257
C. TCP port 256
D. UDP port 8116
Answer: C
NEW QUESTION 314
Which command shows the current connections distributed by CoreXL FW instances?
A. fw ctl multik stat
B. fw ctl affinity -l
C. fw ctl instances -v
D. fw ctl iflist
Answer: A
NEW QUESTION 315
What is the most ideal Synchronization Status for Security Management Server High Availability deployment?
A. Lagging
B. Synchronized
C. Never been synchronized
D. Collision
Answer: B