TestInsides

Quality and Value

TestInsides Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all vce.

Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

Easy to Pass

If you prepare for the exams using our TestInsides testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

Try Before Buy

TestInsides offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

Try before you buy

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

Choose an exam to sample

Select a vendor...

Select an exam...

Your email address

Download Now

About Full Refund

Candidates have own unqualified certificate scanned and then sent to our mailbox. After confirmation, we will refund. (**Contact now**)

Refund Policy

1. Questions must be purchased before the exam.
2. The transcript's subject must be the same subject when you bought the questions.

http://www.testinsides.top/

Testinsides offers the best valid test dumps and test questions

Exam : **156-315.82**

Title : Check Point Certified Security Expert - R82

Vendor : CheckPoint

Version : DEMO

NO.1 What feature is provided by the SMO?
A. The SMO can automatically add or remove the node out of the ClusterXL cluster without administrator intervention.
B. The SMO provides a range of IP addresses which are dynamically assigned to the Cluster nodes.
C. The SMO provides a single IP address for use in management communication and policy installation, simplifying the management process.
D. The SMO maintains a list of ports dynamically assigned to the Cluster nodes to communicate with the Management Server.
Answer: C
Explanation:
The correct answer isC. In ElasticXL, theSingle Management Object, SMO, represents the ElasticXL Cluster as one managed Security Gateway object in SmartConsole. This simplifies management communication and policy installation because the administrator manages and installs policy to the ElasticXL Cluster through a single management identity rather than treating every member as a separately managed gateway. Check Point' s ElasticXL Getting Started procedure instructs administrators to configure a single Security Gateway object in SmartConsole to represent the ElasticXL Cluster and then install policy on that object. Option A is wrong because SMO does not mean automatic uncontrolled member removal; member addition and removal are managed through Gaia Portal or gClish workflows. Option B is wrong because SMO is not a dynamic IP range allocator. Option D is fabricated; SMO is not a port-assignment database. The tested feature is simple:
one management object/IP path for management and policy installation. Reference topic:ElasticXL Getting Started / Single Management Object in SmartConsole.
========

NO.2 When using SmartEvent, what feature can be used to analyze previously generated log files for Event Policy analysis?
A. An Offline Job
B. Correlation Unit > Add > Historical Log Analysis
C. SmartEvent can only analyze new incoming logs or logs less than 24 hours old.
D. The command CPLogInvestigator -f < log file name >
Answer: A

NO.3 What should be upgraded first in Advanced Upgrade Method?
A. Primary Management Server
B. Security Gateway
C. Secondary Management Server
D. Dedicated Log Server
Answer: A

NO.4 Which of these commands will show the availability of a new ElasticXL Cluster member?
A. show cluster info overview
B. show elasticxl members
C. show provision info available
D. show provision members new

Answer: A
Explanation:
The best answer from the provided options isA, although the more precise command for detected/pending members isshow cluster info provision. Check Point's ElasticXL Getting Started guide states that, in Gaia gClish, administrators get the list of ElasticXL Cluster Members and detected Security Appliances with show cluster info provision. The R82 show cluster info reference confirms that the provision parameter shows the provisioning state of new Security Group Members and lets administrators see the progress when new members are joining. Because the exact official command is not present in the answer choices, option A is the only valid command family listed: show cluster info .... Options B, C, and D are not the documented R82 Gaia gClish commands. A clean, corrected version of the answer should be:show cluster info provision. The uploaded question's options are weak here, so do not memorize option C or D. Reference topic:ElasticXL Getting Started / Adding members in Gaia gClish.
========

NO.5 In the Management HA environment, how many synchronization methods are supported?
A. 1
B. 4
C. 3
D. 2
Answer: D
Explanation:
The correct answer isD. Management High Availability supportstwo synchronization methods: synchronization manually and synchronization on a schedule/automatic interval. Check Point's R82 Installation and Upgrade Guide states that Management HA databases are synchronized "manually or on a schedule." The Security Management Administration Guide also explains that the Active server synchronizes with Standby servers at intervals and when the SmartConsole session is published. Option A is too narrow because synchronization is not only manual. Option B and C overstate the number of supported synchronization methods. For exam purposes, reduce it to the clean model:manual synchronizationandscheduled/automatic synchronization.
========

NO.6 What are the key components of an Access Role object?
A. Name, Subnet, Mask-length, User Group, LDAP Account Unit
B. Name, IP Address, Mask-Length, LDAP Account Unit, Remote Access Client
C. Name, LDAP Account Unit, Remote Access Client, Subnet, Host Object Type
D. Name, Networks, Users, Machines, Remote Access Clients
Answer: D
Explanation:
The correct answer isD. In Check Point Identity Awareness and Access Control policy, anAccess Roleobject combines identity and location attributes into one reusable policy object. The R82 Security Management Administration Guide states that Access Role objects let administrators configure network access according toNetworks,Users and user groups,Computers and computer groups, andRemote Access VPN clients. That maps directly to option D: Name, Networks, Users, Machines, and Remote Access Clients. Option A is too narrow and incorrectly reduces the object to subnet and

LDAP fields. Option B mixes IP address and LDAP account unit fields but misses the real policy dimensions. Option C also mixes back-end directory and object- type terminology rather than the functional Access Role components. The purpose of an Access Role is not merely to identify a subnet or LDAP unit; it is to define who, from which machines, on which networks, and through which remote-access context can match a rule. Reference topic:Access Roles / Identity Awareness.
========

NO.7 VTI in Site-to-Site VPN stands for:
A. Virtual Tunnel Interface
B. VPN Transfer Interface
C. Virtual Transfer Interface
D. VPN Tunnel Interface
Answer: A
Explanation:
The correct answer isA. VTI stands forVirtual Tunnel Interface. In Check Point Site-to-Site VPN, a VTI is used for route-based VPN. Instead of identifying VPN traffic only through encryption domains, the gateway can route traffic through a virtual interface that represents the VPN tunnel. Check Point's R82 Site-to-Site VPN guide defines a Virtual Tunnel Interface as a virtual interface that is a member of an existing route-based VPN tunnel. This makes routing behavior more similar to routing through a physical interface, which allows the use of static or dynamic routing over the VPN. Option B, "VPN Transfer Interface," is not a Check Point term. Option C incorrectly replaces "Tunnel" with "Transfer." Option D sounds plausible, but the official expansion isVirtual Tunnel Interface, not VPN Tunnel Interface. The practical CCSE concept is that VTI belongs toRoute-Based VPN, while encryption-domain matching belongs toDomain-Based VPN. Reference topic:Route-Based VPN / VPN Tunnel Interfaces.
========

NO.8 Any VPN Gateway that can establish a direct VPN tunnel with any peer Gateway is a member of which VPN Community?
A. Direct Community
B. Any Community
C. Star Community
D. Mesh Community
Answer: D
Explanation:
The correct answer isD. AMesh VPN Communityallows every member Security Gateway to establish VPN tunnels directly with every other member Security Gateway in that community. Check Point's R82 Site-to- Site VPN guide describes VPN communities as being based on Star and Meshed topologies. In a Star VPN Community, each satellite gateway has a VPN tunnel to the central gateway, but not directly to other satellite gateways. In a Meshed VPN Community, there are VPN tunnels between each pair of Security Gateways.
Option A, "Direct Community," is not a formal Check Point VPN Community type. Option B is also not a Check Point community type. Option C is wrong because Star topology is hub-and-spoke; satellites communicate through or with the center depending on routing configuration, not automatically with every other peer directly. The phrase "any gateway can establish a direct VPN tunnel with any peer

gateway" is the defining behavior of aMesh Community. Reference topic:VPN Communities / Star and Meshed Topologies.
========

NO.9 Choose the correct names for the bonding interfaces that are present by default in an ElasticXL configuration.
A. Mgmt, eth1-Sync
B. magg1, Sync
C. magg1, eth1
D. Mgmtagg1, Syncagg1
Answer: B
Explanation:
The correct answer isB. In ElasticXL, the default bond interfaces aremagg1andSync. Check Point's ElasticXL documentation states that the physical Mgmt interface becomes a subordinate interface in the bond called magg1. It also states that the physical Sync interface is renamed to eth1-Sync and becomes a subordinate interface in the bond called Sync. Therefore, Mgmt and eth1-Sync are physical/subordinate interface names, not the final default bond-interface names. Option A confuses subordinate interfaces with bond names. Option C is wrong because eth1 is not the documented default Sync bond name. Option D is fabricated and not used in ElasticXL. This distinction matters because administrators must understand what they are seeing in Gaia, gClish, monitoring commands, and licensing workflows. The default management bond ismagg1, and the default sync bond isSync. Reference topic:ElasticXL Important Notes / Interface renaming and bonding.
========

NO.10 Alice knows about the Check Point Management HA installation from Bob and needs to know which Check Point Security Management Server is currently in the "Active" state. Alice uses the Check Point SmartConsole tool. Which Check Point console location is needed to look up the Management High Availability status?
A. SmartView Tracker > Log Search > HA Status
B. SmartUpdate > Package Repository > Management High Availability
C. Gaia Portal > Overall View > Management High Availability
D. Check Point SmartConsole > Menu > Management High Availability
Answer: D
Explanation:
The correct answer isD. The Management High Availability status is checked from SmartConsole, not from SmartView Tracker, SmartUpdate, or the Gaia Portal. In SmartConsole, the administrator opens the main menu and selectsHigh AvailabilityorManagement High Availability, depending on the interface wording. The High Availability Status window displays the Management Servers in the HA configuration, including which server SmartConsole is connected to, whether that server is Active or Standby, and the synchronization status of its peer or peers. Option A is wrong because SmartView Tracker/log search is not the Management HA status interface. Option B is wrong because SmartUpdate package management is not used to view active /standby Management HA status. Option C is wrong because Gaia Portal can show appliance/system information, but Management HA role status is handled from SmartConsole. For CCSE-level accuracy, remember this path:SmartConsole Menu > High Availability / Management High Availability.

Reference topic:Monitoring High Availability.

NO.11 What does the Firewall administrator need to do when Management Servers are in Collision Mode?

A. Reboot both servers.

B. Do nothing; the servers will re-synchronize in the next synchronization interval.

C. Run the cpstop; cpstart command in CLI on both servers.

D. Manually re-synchronize the servers.

Answer: D

Explanation:

The correct answer isD. Collision Mode means more than one Management Server is configured asActive. In this condition, the Active servers donotsynchronize with each other, even if network connectivity exists. The administrator must manually resolve the conflict by changing one Active server back to Standby from SmartConsole's Management High Availability window. When one server becomes Standby, synchronization starts and the data on that Standby server is overwritten by the remaining Active server's data. That is why this must be handled deliberately; blindly rebooting both servers or restarting Check Point services does not resolve the logical HA conflict. Option B is dangerous because Check Point explicitly says two Active servers cannot sync with each other. Option C is also wrong because daemon restarts do not decide which database is authoritative. The operational correction is to manually return the environment to a single-Active model and allow synchronization from the authoritative Active Management Server. Reference topic:High Availability Troubleshooting / Collision or HA Conflict.

========

NO.12 Alice and Bob are concurrently logged in to SmartConsole under Logs & Events to check the IKE "Key Install" between a working Site-to-Site VPN tunnel between site Alpha and site Bravo. Which of the following IKE versions are available?

A. IKE

B. IKEv1 & IKEv3

C. IKEv1 & IKEv2

D. IKEv2 & IKEv4

Answer: C

Explanation:

The correct answer isC. Check Point Site-to-Site VPN uses IKE/IPsec for VPN tunnel negotiation. The supported IKE versions in normal Check Point VPN terminology areIKEv1andIKEv2. IKEv1 includes Phase 1
/Phase 2 behavior such as Main Mode, Aggressive Mode, and Quick Mode, while IKEv2 uses the newer IKE_SA_INIT and IKE_AUTH exchange model. There is no Check Point VPN version called IKEv3 or IKEv4 in this context. Option A is too generic because the question asks which versions are available. Option B and D are wrong because IKEv3 and IKEv4 are not valid Check Point VPN choices. Check Point's R82 Site-to-Site VPN guide describes IKE as the key-management protocol used to create VPN tunnels and shows IKE configuration through VPN Community encryption settings.

========

NO.13 How many interfaces are required as a minimum on each ElasticXL Cluster member?

A. Five
B. Six
C. At least three
D. At least four
Answer: D
Explanation:
The correct answer isD. Each ElasticXL Cluster Member requires at leastfour interfaces. Check Point's R82 ElasticXL documentation states that an ElasticXL Cluster requires at least four interfaces on each member: a dedicated management interface, a dedicated Sync interface, an external interface, and an internal interface.
The Mgmt port is selected automatically for the management interface, and the Sync port is selected automatically for the synchronization interface. The administrator selects and configures the external and internal data interfaces. Option A and Option B overstate the requirement. Option C is wrong because three interfaces would not satisfy the documented minimum: management, synchronization, external, and internal are all required as separate functional interface roles. This is not a design preference; it is an ElasticXL requirement. For CCSE R82, the answer is straightforward:minimum four interfaces per ElasticXL Cluster Member. Reference topic:ElasticXL Important Notes / Minimum interface requirement.
========