Checkpoint

Exam 156-315.13

Check Point Security Expert R76(GAiA)

Version: 5.0

[Total Questions: 639]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	100
Topic 4: Volume D	100
Topic 5: Volume E	100
Topic 6: Volume F	100
Topic 7: Volume G	39

Topic 1, Volume A

Question No : 1 - (Topic 1)

Which of the following commands can provide the most complete restore of an R76configuration?

A. upgrade_import
B. fwm dbimport -p <export file>
C. cpconfig
D. cpinfo -recover

Answer: A

Question No : 2 - (Topic 1)

What is the primary benefit of using upgrade_export over either backup or snapshot?

A. The commands backup and snapshot can take a long time to run whereas upgrade_export will take a much shorter amount of time.
B. upgrade_export will back up routing tables, hosts files, and manual ARP configurations, where backup and snapshot will not.
C. upgrade_export has an option to backup the system and SmartView Tracker logs while backup and snapshot will not.
D. upgrade_export is operating system independent and can be used when backup or snapshot is not available.

Answer: D

Question No : 3 - (Topic 1)

Which of the following methods will provide the most complete backup of an R76configuration?

A. Database Revision Control
B. Policy Package Management
C. Copying the directories $FWDIR\conf and $CPDIR\conf to another server
D. upgrade_export command

Answer: D

Question No : 4 - (Topic 1)

How does Check Point recommend that you secure the sync interface between gateways?

A. Configure the sync network to operate within the DMZ.
B. Secure each sync interface in a cluster with Endpoint.
C. Use a dedicated sync network.
D. Encrypt all sync traffic between cluster members.

Answer: C

Question No : 5 - (Topic 1)

If using AD Query for seamless identity data reception from Microsoft Active Directory (AD), which of the following methods is NOT Check Point recommended?

A. Leveraging identity in Internet application control
B. Identity-based auditing and logging
C. Basic identity enforcement in the internal network
D. Identity-based enforcement for non-AD users (non-Windows and guest users)

Answer: D

Question No : 6 - (Topic 1)

When, during policy installation, does the atomic load task run?

A. It is the first task during policy installation.
B. It is the last task during policy installation.
C. Before CPD runs on the Gateway.
D. Immediately after fwm load runs on the SmartCenter.

Answer: B

Question No : 7 - (Topic 1)

During a Security Management Server migrate export, the system:

A. Creates a backup file that includes the SmartEvent database.
B. Creates a backup file that includes the SmartReporter database.
C. Creates a backup archive for all the Check Point configuration settings.
D. Saves all system settings and Check Point product configuration settings to a file.

Answer: C

Question No : 8 - (Topic 1)

Identity Agent is a lightweight endpoint agent that authenticates securely with Single Sign-On (SSO). Which of the following is NOT a recommended use for this method?

A. When accuracy in detecting identity is crucial
B. Identity based enforcement for non-AD users (non-Windows and guest users)
C. Protecting highly sensitive servers
D. Leveraging identity for Data Center protection

Answer: B

Question No : 9 - (Topic 1)

What process is responsible for transferring the policy file from SmartCenter to the Gateway?

A. FWD
B. FWM
C. CPRID
D. CPD

Answer: D

Question No : 10 - (Topic 1)

The process _____ is responsible for all other security server processes run on the Gateway.

A. FWD
B. CPLMD
C. FWM
D. CPD

Answer: A

Question No : 11 - (Topic 1)

The process _____ is responsible for GUIClient communication with the SmartCenter.

A. FWD
B. FWM
C. CPD
D. CPLMD

Answer: B

Question No : 12 - (Topic 1)

When upgrading a cluster in Full Connectivity Mode, the first thing you must do is see if all cluster members have the same products installed. Which command should you run?

A. fw fcu
B. cphaprob fcustat
C. cpconfig
D. fw ctl conn –a

Answer: D

Question No : 13 - (Topic 1)

Your users are defined in a Windows 2008 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client

Authentication rule inR76?

A. LDAP group
B. External-user group
C. A group with a generic user
D. All Users

Answer: A

Question No : 14 - (Topic 1)

YourR76enterprise Security Management Server is running abnormally on Windows 2008 Server. You decide to try reinstalling the Security Management Server, but you want to try keeping the critical Security Management Server configuration settings intact (i.e., all Security Policies, databases, SIC, licensing etc.) What is the BEST method to reinstall the Server and keep its critical configuration?

A. 1. Create a database revision control backup using the SmartDashboard
2. Create a compressed archive of the *FWDlR*\ conf and »FWDiR8\lib directories and copy them to another networked machine.
3. Uninstall all R70 packages via Add/Remove Programs and reboot.
4. Install again as a primary Security Management Server using the R70 CD.
5. Reboot and restore the two archived directories over the top of the new installation, choosing to overwrite existing files.
B. 1. Download the latest upgrade_export utility and run it from a c; \temp directory to export the configuration into a . tgz file
2. Skip any upgarde__verification warnings since you are not upgrading
3. Transfer the . tgz file to another networked machine
4. Download and run the cpclean utility and reboot
5. Use the R70 CD-ROM to select the uuarade import ootion to import the confiauration
C. 1. Download the latest upqrade_expoct utility and run it from a \temp directory to export the configuration into a . tgz file
2. Perform any requested upgcade_veri£ic«tion suggested steps
3. Uninstall all R70 packages via Add/Remove Programs and reboot
4. Use SmartUpdate to reinstall the Security Management Server and reboot
5. Transfer the tgz file back to the local \temp
6. Run upgrade__import to import the configuration
D. 1. Insert the F70 CD-ROM, and select the option to export the configuration using the latest upgrade utilities
2. Perform any requested upgrade_verification suggested steps and re-export the configuration if needed
3. Save the export " tgz file to a local c: \temp directory

4. Uninstall all R70 packages via Add/Remove Programs and reboot
5. Install again using the R70 CD-ROM as a primary Security Management Server and reboot
6. Run upgrade_import to import the configuration

Answer: C

Question No : 15 - (Topic 1)

With the User Directory Software Blade, you can createR76user definitions on a(n) _____ Server.

A. SecureID
B. LDAP
C. NT Domain
D. Radius

Answer: B

Question No : 16 - (Topic 1)

David wants to manage hundreds of gateways using a central management tool.

What tool would David use to accomplish his goal?

A. SmartProvisioning
B. SmartBlade
C. SmartDashboard
D. SmartLSM

Answer: B

Question No : 17 - (Topic 1)

Which of the following is NOT a feature of ClusterXL?

A. Enhanced throughput in all ClusterXL modes (2 gateway cluster compared with 1

gateway)
B. Transparent failover in case of device failures
C. Zero downtime for mission-critical environments with State Synchronization
D. Transparent upgrades

Answer: C

Question No : 18 - (Topic 1)

A Fast Path Upgrade of a cluster:

A. Upgrades all cluster members except one at the same time.
B. Treats each individual cluster member as an individual gateway.
C. Is not a valid upgrade method inR76.
D. Is only supported in major releases (R70 to R71, R75toR76).

Answer: C

Question No : 19 - (Topic 1)

Remote clients are using SSL VPN to authenticate via LDAP server to connect to the organization. Which gateway process is responsible for the authentication?

A. vpnd
B. cpvpnd
C. fwm
D. fwd

Answer: B

Question No : 20 - (Topic 1)

You are running aR76Security Gateway on SecurePlatform. In case of a hardware failure, you have a server with the exact same hardware and firewall version installed. What backup method could be used to quickly put the secondary firewall into production?

A. upgrade_export
B. manual backup
C. snapshot
D. backup

Answer: C

Question No : 21 - (Topic 1)

The process _____ is responsible for Policy compilation.

A. FWM
B. Fwcmp
C. CPLMD
D. CPD

Answer: A

Question No : 22 - (Topic 1)

_____ is the called process that starts when opening SmartView Tracker application.

A. logtrackerd
B. fwlogd
C. CPLMD
D. FWM

Answer: C

Question No : 23 - (Topic 1)

How would you set the debug buffer size to 1024?

A. Run fw ctl set buf 1024
B. Run fw ctl kdebug 1024
C. Run fw ctl debug -buf 1024
D. Run fw ctl set int print_cons 1024