

Vendor: Check Point

Exam Code: 156-315.13

Exam Name: Check Point Certified Security Expert R76

Version: DEMO

QUESTION 1
The process _____ is responsible for Policy compilation.

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

Answer: A

QUESTION 2
The process _____ is responsible for Management High Availability synchronization.

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

Answer: B

QUESTION 3
_____ is the called process that starts when opening SmartView Tracker application.

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

Answer: C

QUESTION 4
Anytime a client initiates a connection to a server, the firewall kernel signals the FWD process using a trap. FWD spawns the _____ child service, which runs the security server.

A. FWD
B. FWSD
C. In.httpd
D. FWSSD

Answer: D

QUESTION 5
Security server configuration settings are stored in _____ .

A. $FWDIR/conf/AMT.conf
B. $FWDIR/conf/fwrl.conf
C. $FWDIR/conf/fwauthd.conf
D. $FWDIR/conf/fwopsec.conf

Answer: C

QUESTION 6
User definitions are stored in _____ .

A. $FWDIR/conf/fwmuser
B. $FWDIR/conf/users.NDB
C. $FWDIR/conf/fwauth.NDB
D. $FWDIR/conf/fwusers.conf

Answer: C

QUESTION 7
Jon is explaining how the inspection module works to a colleague. If a new connection passes through the inspection module and the packet matches the rule, what is the next step in the process?

A. Verify if the packet should be moved through the TCP/IP stack.
B. Verify if any logging or alerts are defined.
C. Verify if the packet should be rejected.
D. Verify if another rule exists.

Answer: B

QUESTION 8
Which of the following statements accurately describes the upgrade_export command?

A. Used primarily when upgrading the Security Management Server, upgrade_export stores all object databases and the conf directories for importing to a newer version of the Security Gateway.
B. Used when upgrading the Security Gateway, upgrade_export includes modified files, such as in the directories /lib and /conf.
C. upgrade_export is used when upgrading the Security Gateway, and allows certain files to be included or excluded before exporting.
D. upgrade_export stores network-configuration data, objects, global properties, and the database revisions prior to upgrading the Security Management Server.

Answer: A

QUESTION 9
What are you required to do before running upgrade_export?

A. Run a cpstop on the Security Gateway.
B. Run cpconfig and set yourself up as a GUI client.
C. Run a cpstop on the Security Management Server.
D. Close all GUI clients.

Answer: D

QUESTION 10
A snapshot delivers a complete backup of SecurePlatform. The resulting file can be stored on servers or as a local file in /var/CPsnapshot/snapshots. How do you restore a local snapshot named MySnapshot.tgz?

A. As Expert user, type command snapshot - R to restore from a local file.
Then, provide the correct file name.
B. As Expert user, type command revert --file MySnapshot.tgz.
C. As Expert user, type command snapshot -r MySnapshot.tgz.
D. Reboot the system and call the start menu.
Select option Snapshot Management, provide the Expert password and select [L] for a restore from a local file.
Then, provide the correct file name.

Answer: B

QUESTION 11
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 12
Your R7x-series Enterprise Security Management Server is running abnormally on Windows Server 2003 R2. 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. Run `cpstop` on one member, and configure the new interface via `sysconfig`.
2. Run `cpstart` on the cluster member. Repeat the same steps on another member.
3. Update the new topology in the cluster object from SmartDashboard.
4. Install the Security Policy.

B. 1. Use the `ifconfig` command to configure and enable the new interface on both members.
2. Run `cprestart` on both members.
3. Update the topology in the cluster object for the cluster and both members.
4. Install the Security Policy.

C. 1. Use `sysconfig` to configure the new interfaces on both members.
2. Update the topology in the cluster object.
3. Install the Security Policy.

D. 1. Disable "Cluster membership" from one gateway via `cpconfig`.
2. Configure the new interface via `sysconfig` from the "non-member" Gateway.
3. Re-enable "Cluster membership" on the Gateway.
4. Perform the same steps on the other Gateway.
5. Update the topology in the cluster object.
6. Install the Security Policy.

Answer: B

QUESTION 13
Your primary Security Management Server runs on GAiA . What is the easiest way to back up your Security Gateway R76 configuration, including routing and network configuration files?

A. Using the native GAiA back up utility from command line or in the Web-based user interface.
B. Using the command upgrade_export.
C. Run the command pre_upgrade_verifier and save the file *.tgz to the directory c:/temp.
D. Copying the directories $FWDIR/conf and $FWDIR/lib to another location.

Answer: A

QUESTION 14
You need to back up the routing, interface, and DNS configuration information from your R76 SecurePlatform Security Gateway. Which backup-and-restore solution do you use?

A. SecurePlatform back up utilities
B. Manual copies of the directory $FWDIR/conf
C. Database Revision Control
D. Commands upgrade_export and upgrade_import

Answer: A

QUESTION 15
Which of the following methods will provide the most complete backup of an R76 configuration?

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 16
Which of the following commands can provide the most complete restore of an R76 configuration?

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

D. cpinfo -recover

Answer: A

QUESTION 17
When restoring R76 using the command upgrade_import, which of the following items are NOT restored?

A. Global properties
B. Route tables
C. Licenses
D. SIC Certificates

Answer: B

QUESTION 18
Your organization's disaster recovery plan needs an update to the backup and restore section to reap the benefits of the new distributed R76 installation. Your plan must meet the following required and desired objectives:

Required Objective: The Security Policy repository must be backed up no less frequently than every 24 hours.

Desired Objective: The R76; components that enforce the Security Policies should be backed up at least once a week.

Desired Objective: Back up R76 logs at least once a week.

Your disaster recovery plan is as follows:

- Use the utility `cron` to run the command `upgrade_export` each night on the Security Management Servers.
- Configure the organization's routine back up software to back up the files created by the command `upgrade_export`.
- Configure the SecurePlatform back up utility to back up the Security Gateways every Saturday night.
- Use the utility `cron` to run the command `upgrade_export` each Saturday night on the log servers.
- Configure an automatic, nightly `logswitch`.
- Configure the organization's routine back up software to back up the switched logs every night.

Upon evaluation, your plan:

A. Meets the required objective and only one desired objective
B. Meets the required objective and both desired objectives
C. Meets the required objective but does not meet either desired objective
D. Does not meet the required objective

Answer: B

QUESTION 19
You are running a R76 Security 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 20
Before upgrading SecurePlatform, you should create a backup. To save time, many administrators use the command backup. This creates a backup of the Check Point configuration as well as the system configuration. An administrator has installed the latest HFA on the system for fixing traffic problems after creating a backup file. There is a mistake in the very complex static routing configuration. The Check Point configuration has not been changed. Can the administrator use a restore to fix the errors in static routing?

A. The restore is not possible because the backup file does not have the same build number (version).
B. The restore is done by selecting Snapshot Management from the SecurePlatform boot menu.
C. The restore can be done easily by the command restore and selecting the appropriate backup file.
D. A back up cannot be restored, because the binary files are missing.

Answer: C

Thank You for Trying Our Product

Lead2pass Certification Exam Features:



★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.



★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**