Checkpoint

Exam 156-315.77

Check Point Security Expert R77

Version: 7.0

[Total Questions: 736]

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	95
Topic 6: Volume F	100
Topic 7: Volume G	98
Topic 8: Volume H	43

Topic 1, Volume A

Question No : 1 - (Topic 1)

There are severalSmart Directory(LDAP) features that can be applied to further enhanceSmart Directory(LDAP) functionality, which of the following is NOT one of those features?

A. High Availability, where user information can be duplicated across several servers
B. Support multipleSmart Directory(LDAP) servers on which many user databases are distributed
C. Encrypted or non-encryptedSmart Directory(LDAP) Connections usage
D. Support many Domains under the same account unit

Answer: D

Question No : 2 - (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 theSmart Center.

Answer: B

Question No : 3 - (Topic 1)

The process _____ is responsible for GUIClient communication with theSmart Center.

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

Answer: B

Question No : 4 - (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

Answer: C

Question No : 5 - (Topic 1)

_____ is the called process that starts when openingSmart ViewTracker application.

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

Answer: C

Question No : 6 - (Topic 1)

In a "zero downtime" scenario, which command do you run manually after all cluster members are upgraded?

A. cphaconf set_ccp broadcast
B. cphaconf set clear_subs
C. cphaconf set mc_relod
D. cphaconf set_ccp multicast

Answer: D

Question No : 7 - (Topic 1)

The file snapshot generates is very large, and can only be restored to:

A. The device that created it, after it has been upgraded
B. Individual members of a cluster configuration
C. Windows Server class systems
D. A device having exactly the same Operating System as the device that created the file

Answer: D

Question No : 8 - (Topic 1)

What process is responsible for transferring the policy file fromSmart Centerto the Gateway?

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

Answer: D

Question No : 9 - (Topic 1)

You are running aR76Security Gateway onSecure Platform. 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 : 10 - (Topic 1)

What are you required to do before runningupgrade 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 No : 11 - (Topic 1)

When upgrading Check Point products in a distributed environment, in which order should you upgrade these components?

1 GUI Client

2 Security Management Server

3 Security Gateway

A. 3, 2, 1
B. 1, 2, 3
C. 3, 1, 2
D. 2, 3, 1

Answer: D

Question No : 12 - (Topic 1)

Which of the following access options would you NOT use when configuring Captive Portal?

A. Through the Firewall policy
B. From the Internet
C. Through all interfaces
D. Through internal interfaces

Answer: B

Question No : 13 - (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 : 14 - (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 : 15 - (Topic 1)

You have pushed a policy to your firewall and you are not able to access the firewall. What command will allow you to remove the current policy from the machine?

A. fw purge policy
B. fw fetch policy
C. fw purge active
D. fw unload local

Answer: D

Question No : 16 - (Topic 1)

Which command would you use to save the interface information before upgrading a

Windows Gateway?

A. cp /etc/sysconfig/network.C [location]
B. ipconfig –a > [filename].txt
C. ifconfig > [filename].txt
D. netstat –rn > [filename].txt

Answer: B

Question No : 17 - (Topic 1)

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 No : 18 - (Topic 1)

John is upgrading a cluster from NGX R65 toR76. John knows that you can verify the upgrade process using the pre-upgrade verifier tool. When John is running Pre-Upgrade Verification, he sees the warning message:

Title: Incompatible pattern.

What is happening?

A. R76uses a new pattern matching engine. Incompatible patterns should be deleted before upgrade process to complete it successfully.
B. Pre-Upgrade Verification process detected a problem with actual configuration and upgrade will be aborted.
C. Pre-Upgrade Verification tool only shows that message but it is only informational.
D. The actual configuration contains user defined patterns in IPS that are not supported inR76. If the patterns are not fixed after upgrade, they will not be used withR76Security Gateways.

Answer: D

Question No : 19 - (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 : 20 - (Topic 1)

Choose the BEST sequence for configuring user management inSmart Dashboard, using an LDAP server.

A. Configure a workstation object for the LDAP server, configure a server object for the LDAP Account Unit, and enable LDAP in Global Properties.
B. Configure a server object for the LDAP Account Unit, and create an LDAP resource object.
C. Enable LDAP in Global Properties, configure a host-node object for the LDAP server, and configure a server object for the LDAP Account Unit.
D. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP resource object.

Answer: C

Question No : 21 - (Topic 1)

A Full Connectivity Upgrade of a cluster:

A. Treats each individual cluster member as an individual gateway.
B. Upgrades all cluster members except one at the same time.
C. Is only supported in minor version upgrades (R70 to R71, R71 toR76).

D. Is not a valid upgrade method inR76.

Answer: C

Question No : 22 - (Topic 1)

A Zero Downtime Upgrade of a cluster:

A. Upgrades all cluster members except one at the same time.
B. Is only supported in major releases (R70 to R71, R71 toR76).
C. Treats each individual cluster member as an individual gateway.
D. Is not a valid upgrade method inR76.

Answer: A

Question No : 23 - (Topic 1)

The process _____ is responsible for Policy compilation.

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

Answer: A

Question No : 24 - (Topic 1)

From the following output of cphaprob state, which ClusterXL mode is this?

A. New mode