Checkpoint.156-536.by.Janui.36q

Number: 156-536
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: 156-536

Exam Name: Check Point Certified Harmony Endpoint Specialist - R81.20

Exam A

QUESTION 1
By default, Endpoint Security Manager is configured as which kind of server?

A. Network Server
B. Webserver
C. Management Server
D. Log Server

Correct Answer: C
Section:

QUESTION 2
How many security levels can you set when enabling Remote help on pre-boot?

A. Four levels - Low security, Medium security, High security, Very High security
B. Two levels - Low and High security
C. Three levels - Low security, Medium security. High security
D. One and only level - enable or disable security

Correct Answer: C
Section:

QUESTION 3
When is the heartbeat initiated?

A. During the first sync
B. After the last sync
C. Before the first sync.
D. After the first sync

Correct Answer: D
Section:

QUESTION 4
Harmony Endpoint offers Endpoint Security Client packages for which operating systems?

A. Unix, WinLinux and macOS
B. Windows, macOS and Linux operating systems
C. macOS, iPadOS and Windows
D. Windows, AppleOS and Unix operating systems

Correct Answer: B

Section:

QUESTION 5
On which desktop operating systems are Harmony Endpoint Clients supported?

A. Windows, MacOS, Linux and Unix
B. Only Windows and MacOS
C. Windows Servers and Clients, MacOS and Linux
D. Windows Client, MacOS and Linux

Correct Answer: C
Section:

QUESTION 6
You must make a decision of which FDE algorithm to be used by one of your clients who specializes in multimedia video editing. What algorithm will you choose?

A. The implementation of a Secure VPN with very strong encryption will make your data invisible in cases of live internet transmission.
B. In Multimedia applications you do not need to implement any kind of Full disk encryption. You can use software like 7Zip in order to encrypt your data.
C. Any kind of data is very important and the Full Disk Encryption technic must be used with the strongest secret key possible. Your client has to use strong encryption like XTS-AES 256 bit.
D. Video processing is a high bandwidth application which utilizes a lot of HDD access time. You have to use a FDE algorithm with small secret key like XTS-AES 128 bit.

Correct Answer: C
Section:

QUESTION 7
What does pre-boot authentication disable?

A. Workarounds to computer security
B. Identity theft
C. Incorrect usernames
D. Weak passwords

Correct Answer: A
Section:

QUESTION 8
Does the Endpoint Client GUI provide automatic or manual prompting to protect removable storage media usage?

A. Manual Only
B. Either automatic or manual
C. Automatic Only
D. Neither automatic or manual

Correct Answer: B
Section:

QUESTION 9

Full Disk Encryption (FDE) protects data at rest stored on__________.

A. RAM Drive
B. SMB Share
C. NFS Share
D. Hard Drive

Correct Answer: D
Section:

QUESTION 10
What does FDE software combine to authorize accessibility to data on desktop computers and laptops?

A. post-logon authentication and encryption
B. OS boot protection with pre-boot authentication and encryption
C. OS boot protection and post-boot authentication
D. Decryption

Correct Answer: B
Section:

QUESTION 11
What does pre-boot protection require of users?

A. To authenticate before the computer will start
B. To answer a security question after login
C. To authenticate before the computer's OS starts
D. To regularly change passwords

Correct Answer: C
Section:

QUESTION 12
One of the Data Security Software Capability protections included in the Harmony Endpoint solution is....

A. Data Leak Firewall
B. Memory Encryption
C. Dynamic Data Protection
D. Remote Access VPN

Correct Answer: A
Section:

QUESTION 13
An Innovative model that classifies new forms of malware into known malware families based on code and behavioral similarity is called:

A. Sanitization (CDR)

B. Polymorphic Model
C. Behavior Guard
D. Anti-Ransomware

Correct Answer: C
Section:

QUESTION 14
What capabilities does the Harmony Endpoint NGAV include?

A. Anti-Ransomware, Anti-Exploit & Behavioral Guard
B. Anti-IPS, Anti-Firewall & Anti-Guard
C. Zero-Phishing, Anti-Bot& Anti-Virus
D. Threat Extraction, Threat-Emulation & Zero-Phishing

Correct Answer: A
Section:

QUESTION 15
Which Endpoint capability ensures that protected computers comply with your organization's requirements and allows you to assign different security levels according to the compliance state of the endpoint computer?

A. Compliance Check
B. Capsule Cloud Compliance
C. Forensics and Anti-Ransomware
D. Full Disk Encryption

Correct Answer: A
Section:

QUESTION 16
Which User Roles are on the Endpoint Security Management Server for On-Premises servers?

A. Primary Administrator and Read-Only
B. Super Admin, Primary Administrator, User Admin, Read-Only
C. Admin and Read-Only
D. Super Admin, Read-Write All, Read-Only

Correct Answer: B
Section:

QUESTION 17
External Endpoint policy servers (EPS) decrease X and reduce X between sites?

A. Decrease policies and reduce traffic between sites
B. Decrease power and reduce accidents between sites
C. Decrease clients and reduce device agents between sites
D. External Endpoint policy servers (EPS) decrease the load of the EMS and reduce the bandwidth required between sites

Correct Answer: D
Section:

QUESTION 18
What does Unauthenticated mode mean?

A. Computers and users might present a security risk, but still have access.
B. Computers and users are trusted based on their IP address and username.
C. Computers and users have credentials, but they are not verified through AD.
D. Computers and users are trusted based on the passwords and usernames only.

Correct Answer: A
Section:

QUESTION 19
If there are multiple EPS in an environment, what happens?

A. One Endpoint client automatically communicates with the server
B. Each Endpoint client automatically communicates with the EMS
C. Each Endpoint client does an analysis to find which EPS is 'closest' and automatically communicates with that server.
D. Each Endpoint client automatically communicates with the SMS

Correct Answer: C
Section:

QUESTION 20
You are facing a lot of CPU usage and high bandwidth consumption on your Endpoint Security Server. You check and verify that everything is working as it should be, but the performance is still very slow. What can you do to decrease your bandwidth and CPU usage?

A. The managements High Availability sizing is not correct. You have to purchase more servers and add them to the cluster.
B. Your company's size is not large enough to have a valid need for Endpoint Solution.
C. Your company needs more bandwidth. You have to increase your bandwidth by 300%
D. You can use some of your Endpoints as Super Nodes since super nodes reduces bandwidth as well as CPU usage.

Correct Answer: D
Section:

QUESTION 21
What does Port Protection protect, and why?

A. Activity on the ports of a client computer to help prevent data leakage
B. Activity on the ports of a client computer to review logs
C. Activity on the ports of a client computer to help unauthorized user access
D. Activity on the ports of a client computer to monitor devices

Correct Answer: A
Section:

QUESTION 22

Media Encryption and Port Protection (MEPP) provide strong encryption for removable media, such as?

A. USB drives, CD/DVDs, and SD cards, and for external ports

B. Cables and Ethernet cords

C. External ports only

D. USB drives and CD/DVDs

Correct Answer: A
Section:

QUESTION 23

Where are the Endpoint policy servers located?

A. Between the Endpoint clients and the EPS

B. Between the Endpoint clients and the EMS

C. Between the Endpoint clients and the NMS

D. Between the Endpoint clients and the SMS

Correct Answer: B
Section:

QUESTION 24

How is the Kerberos key tab file created?

A. Using Kerberos principals

B. Using the AD server

C. Using encryption keys

D. With the ktpass tool

Correct Answer: D
Section:

QUESTION 25

External Policy Servers are placed between the Endpoint clients and the Endpoint Security Management Server. How many Policy Servers are supported per environment?

A. From 1 to 25 Policy Servers are supported

B. From 1 to 15 Policy Servers are supported

C. From 1 to 20 Policy Servers are supported

D. From 1 to 5 Policy Servers are supported

Correct Answer: A
Section:

QUESTION 26

When in the Strong Authentication workflow is the database installed on the secondary server?

A. After Endpoint security is enabled
B. Before Endpoint security is enabled
C. Exactly when Endpoint security is enabled
D. After synchronization and before Endpoint security has been enabled

Correct Answer: D
Section:

QUESTION 27
What does the Kerberos key tab file contain?

A. Pairs of authentication settings and un-authentication settings
B. Pairs of encryption and decryption keys
C. Pairs of Kerberos principals and encryption keys
D. Pairs of ktpass tools

Correct Answer: C
Section:

QUESTION 28
External Policy Servers are placed between the Endpoint clients and the Endpoint Security Management Server. What benefit does the External Endpoint Policy Server bring?

A. Cluster and Delta requests
B. Heartbeat and synchronization requests
C. Test packet and delta requests
D. Polling beat and delta requests

Correct Answer: B
Section:

QUESTION 29
Which permissions apply the same access level to the entire organization?

A. Organization-wide permission settings
B. Regional user permission settings
C. Universal user permission settings
D. Global user permission settings

Correct Answer: A
Section:

QUESTION 30
Endpoint Security Clients are applications installed on company-owned desktop and laptop computers which include the following

A. Endpoint security software Capabilities and a device agent which operates as a container for the Capabilities and communicates with the Endpoint Management Server
B. GUI client that connects to the Endpoint Security Management Server to manage the policy an other configuration for Endpoints
C. Endpoint Security software Capabilities and a GUI client to manage policies for all capabilities

D. GUI client that connects to the local Endpoint Capability Software to manage the policy and all other configuration for that Endpoint only

Correct Answer: A
Section:

QUESTION 31
When can administrators prepare the client for the FDE software package installation and deployment?

A. Once a client meets the maximum system requirements
B. Once the policy is installed
C. Once the client system volumes have 32 MB of space
D. Once a client machine meets the minimum system requirements

Correct Answer: D
Section:

QUESTION 32
Before installing FDE on a client machine, what should administrators make sure of?

A. That system volumes include at least 32 MB of continuous space
B. That system volumes include at least 50 MB of continuous space
C. That system volumes include at least 36 MB of continuous space
D. That system volumes include at least 25 MB of continuous space

Correct Answer: A
Section:

QUESTION 33
How many digits are required in the FDE policy settings to enable a Very High-Security level for remote help on pre-boot?

A. 40 digits
B. Maximum 30 digits
C. 24 digits
D. Minimum 20 digits

Correct Answer: C
Section:

QUESTION 34
The CISO office evaluates Check Point Harmony Endpoint and needs to know what kind of post-infection capabilities exist. Which Post-infection Capabilities does the Harmony Office Suite include?

A. IPS Attack Analysis (Forensics), Deploy and Destroy and Isolation
B. Automated Attack Analysis (Forensics), Remediation and Response and Quarantine
C. FW Attack Analysis (Forensics), Detect and Prevent and Isolation
D. IPS Attack Analysis (Forensics), Detect and Prevent and Isolation

Correct Answer: B

Section:

QUESTION 35

As an Endpoint Administrator you are facing with some errors related to AD Strong Authentication in Endpoint Management server. Where is the right place to look when you are troubleshooting these issues?

A. $FWDIR/log/Authentication.log

B. $FWDIR/logs/Auth.log

C. $UEPMDIR/logs/Authentication.log

D. $UEMPDlR/log/Authentication.elg

Correct Answer: C
Section:

QUESTION 36

Before installing the Endpoint Security Management Server, it is necessary to consider this...

A. A Network Security Management Server must be installed

B. A Network Security Management Server must NOT be installed on the same machine

C. An Endpoint Security Gateway must be installed

D. MS SQL Server must be available with full admin access

Correct Answer: D
Section: