Free Questions for 156-536

Shared by Holmes on 02-09-2025

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How often does the AD scanner poll the server database for the current configuration settings?

Options:

A- Every 60 minutes
B- Every 150 minutes
C- Every 120 minutes
D- Every 30 minutes

Answer:

A

Explanation:

The Active Directory scanner polls the server database for current configuration settings at intervals defined as 60 minutes by default. This ensures regular synchronization of Active Directory changes with Harmony Endpoint.

Exact Extract from Official Document:

'The Scan Interval is the time, in minutes, between the requests... default is typically every 60 minutes.'

Check Point Harmony Endpoint Specialist R81.20 Administration Guide, 'Configuring a Directory Scanner Instance.'

Question 2

Question Type: MultipleChoice

To enforce the FDE policy, the following requirement must be met?

Options:

A- The client must obtain an FDE machine-based policy

B- The client must obtain an FDE certificate
C- Deployments must consist of at least one post-boot user
D- A recovery file must be encrypted

Answer:

A

Question 3

Question Type: MultipleChoice

One of the ways to install Endpoint Security clients is 'Automatic Deployment'. Which of this is true for automatic deployment of Endpoint Security clients?

Options:

A- Automatic deployment can be done on any Windows machine with Check Point SmartConsole first installed
B- Automatic deployment can be done on any Windows 10 machine without any Check Point component pre-installed
C- For automatic deployment to work, the client system must have SVN Foundation enabled in Windows 10 or downloaded and installed on other operating systems
D- Automatic deployment first requires installation of the Initial Client package, which is exported and distributed manually

Answer:

C

Question 4

Question Type: MultipleChoice

When deploying a policy server, which is important?

Options:

A- To have policies in place
B- To configure the heartbeat interval and define the amount of time that the client is allowed to

connect to the server
C- To configure the EPS and define the amount of time that the client is allowed to connect to the SMS
D- To install the heartbeat server first

Answer:

B

Explanation:

When deploying an Endpoint Policy Server, configuring the heartbeat interval is critical. The heartbeat interval defines how often the client must communicate with the server to verify policy status and updates. The amount of time allowed for the client to connect ensures consistent enforcement of policies.

Exact Extract from Official Document:

'The heartbeat interval and the time allowed for client connections are critical settings to configure when deploying an Endpoint Policy Server.'

Check Point Harmony Endpoint Specialist R81.20 Administration Guide, 'Endpoint Policy Server Proximity Analysis.'

Question 5

Question Type: MultipleChoice

What type of attack is Ransomware?

Options:

A- Where a victim encrypts files on a computer and demands payment for decryption key from an attacker.
B- Where an attacker encrypts files on a computer and demands payment for decryption key.
C- Ransomware is not an attack.
D- Where an attacker decrypts files on a computer and demands payment for encryption key.

Answer:

B

Explanation:

Ransomware is a form of malicious software (malware) where an attacker encrypts the victim's data, rendering it inaccessible. The attacker then demands a ransom payment from the victim to provide the decryption key that will restore access to the data.

Exact Extract from Official Document:

'Before a Ransomware attack can encrypt files, Anti-Ransomware backs up your files to a safe location. After the attack is stopped, it deletes files involved in the attack and restores the original files from the backup location.' This indicates that ransomware encrypts files, confirming that the attacker encrypts the files and demands a payment for a decryption key.

Check Point Harmony Endpoint Specialist R81.20 Administration Guide, Section: 'Anti-Ransomware'.

Question 6

Question Type: MultipleChoice

Endpoint's Media Encryption (ME) Software Capability protects sensitive data on what, and how?

Options:

A- Storage devices, removable media, and other input/output devices by requiring authorization before a user accesses the device
B- Input/output devices using Anti-Malware
C- Removable media and other input/output devices by using encryption methods
D- Storage devices by requiring multi-factor authorization

Answer:

A

Explanation:

The Media Encryption & Port Protection component specifically safeguards sensitive information by encrypting data and mandating authorization for access to storage devices, removable media, and other input/output devices. Users need explicit authorization to interact with these encrypted storage devices.

Exact Extract from Official Document:

'The Media Encryption & Port Protection component protects sensitive information by encrypting data and requiring authorization for access to storage devices, removable media, and other input/output devices.'

Check Point Harmony Endpoint Specialist R81.20 Administration Guide, Section: 'Media Encryption & Port Protection'.

Question 7

Question Type: MultipleChoice

The CEO of the company uses the latest Check Point Endpoint client on his laptop. All capabilities are enabled, and FDE has been applied. The CEO is on a business trip and remembers that he needs to send some important emails, so he is forced to boot up his laptop in a public are

a. However, he suddenly needs to leave and forgets to lock or shut down his computer. The laptop remains unattended. Is the CEO's data secured?

Options:

A- The data is not secured. The laptop was left unlocked in the email client window. Everyone who accesses the laptop, before it automatically locks, has access to all data.
B- The laptop is not secure because anyone in the local connected Wi-Fi can access the CEO's corporate data.
C- The laptop is totally secure since the Endpoint client will automatically detect the emergency and has set the OS in hibernate mode.
D- The laptop is using the latest technology for Full Disk Encryption. Anyone who finds the laptop can't access its data due to the data encryption used.

Answer:

A

Explanation:

Full Disk Encryption (FDE) primarily protects data when the computer is turned off or locked. If the laptop is booted and left unattended without being locked or shut down, the encryption does not actively protect data at the moment. Anyone who gains physical access to the device during this time can view and access all open data and applications until the computer auto-locks or is manually locked.

Exact Extract from Official Document:

'Pre-boot Protection requires users to authenticate to their computers before the computer boots. This prevents unauthorized access to the operating system using authentication bypass tools at the operating system level or alternative boot media to bypass boot protection.' This implies that once booted and logged in, the data is accessible if the laptop is left unattended and unlocked.

Check Point Harmony Endpoint Specialist R81.20 Administration Guide, Section: 'Pre-boot Protection'.

Question 8

Question Type: MultipleChoice

In addition to passwords, what else does the pre-boot environment also support?

Options:

A- Options for remote authentication method
B- Options for multi-factor authentication methods
C- Options for double-factor authentication method
D- Options for single-factor authentication method

Answer:

B

Explanation:

The Check Point Harmony Endpoint documentation clearly specifies that the pre-boot environment supports multi-factor authentication methods. These methods combine different authentication mechanisms to enhance security significantly beyond traditional password-based authentication alone.

Exact Extract from Official Document:

'You can also use TPM in addition to Pre-boot authentication for two-factor authentication.'

Check Point Harmony Endpoint Specialist R81.20 Administration Guide, Section: 'Authentication before the Operating System Loads (Pre-boot).'

Question 9

Question Type: MultipleChoice

Which solution encrypts various types of removable storage media including USB drives, backup hard drives, and SD cards?

Options:

A- Full Disk Encryption and File Recovery
B- Endpoint's Media Encryption (ME) Software Capability
C- Media Encryption and Port Protection (MEPP)
D- Full Recovery with Media Encryption

Answer:

B

Question 10

Question Type: MultipleChoice

Harmony Endpoint's Full Disk Encryption (FDE) only allows access to authorized users using what?

Options:

A- Multifaceted pre-boot capabilities
B- Strong Passwords
C- Single login
D- Username verification

Answer:

A

Explanation:

Check Point Harmony Endpoint's Full Disk Encryption (FDE) provides security through advanced multifaceted pre-boot capabilities. These capabilities require users to authenticate before the

system boots, significantly enhancing data security by preventing unauthorized access using alternative boot methods or system bypass tools.

Exact Extract from Official Document:

'Pre-boot Protection requires users to authenticate to their computers before the computer boots. This prevents unauthorized access to the operating system using authentication bypass tools at the operating system level or alternative boot media to bypass boot protection.'

Check Point Harmony Endpoint Specialist R81.20 Administration Guide, Section: 'Full Disk Encryption.'

Question 11

Question Type: MultipleChoice

The Endpoint administrator prepared deployment rules for remote deployment in a mixed desktop environment. Some of the non-Windows machines could not install Harmony Endpoint clients. What is the reason for this?

Options:

A- macOS clients are not supported by Harmony Endpoint
B- Administrator doesn't run chmod command, to allow execution permission to the deployment script
C- Deployment rules are not supported on macOS clients
D- Deployment rules were assigned to users not to machines

Answer:

C

Explanation:

The official Check Point Harmony Endpoint documentation clearly states that deployment rules (automatic deployment) are not supported for macOS clients. macOS client deployments must instead be performed manually using exported packages or third-party deployment methods.

Exact Extract from Official Document:

'Deploy New Endpoints... macOS: No' (indicating that deployment rules cannot automatically deploy endpoints for macOS)

Check Point Harmony Endpoint Specialist R81.20 Administration Guide.