Checkpoint

Exam 156-715.70

Check Point Certified Endpoint Expert R70 (Combined SA, FDE, MI, ME)

Version: 7.0

[Total Questions: 374]

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	74

Topic 1, Volume A

Question No : 1 - (Topic 1)

If Full Disk Encryption is written to bad sectors on the hard drive, which of the following may occur?

A. The recovery file is not created and encryption does not occur.
B. The recovery file is created but encryption does not occur.
C. The installation fails with errors.
D. The installation fails with no errors.

Answer: A

Question No : 2 - (Topic 1)

Which system setting CANNOT be changed using Full Disk Encryption Update Profiles?

A. Change Accounts settings
B. Adding/deleting groups/users to/from user systems
C. Change Group settings
D. Add additional encrypted volumes

Answer: D

Question No : 3 - (Topic 1)

Which of the following methods for data protection is considered the most secure?

A. File encryption
B. Encryption
C. Boot protection and encryption
D. Boot protection

Answer: C

Question No : 4 - (Topic 1)

When deleting actively logged-in users in Full Disk Encryption, when does Full Disk Encryption notify online users that their logins have been locked?

A. Once the users log out of Windows.
B. Once the screen-saver lock is activated.
C. At next reboot.
D. The users will be locked out of the system immediately.

Answer: D

Question No : 5 - (Topic 1)

If Single Sign On is active for a Full Disk Encryption user, where does Pointsec store the user credentials?

A. In the secure local Data Base
B. In the Pointsec administration tool
C. Encrypted under %PROGRAM FILES%\Pointsec \Pointsec\SSO
D. In the Registry

Answer: C

Question No : 6 - (Topic 1)

How many authorized Full Disk Encryption users must install and authorize a software-upgrade patch for distribution to clients?

A. Three
B. One
C. Two
D. None

Answer: D

Question No : 7 - (Topic 1)

Full Disk Encryption stores up to ___________ events in the local event Data Base.

A. 1024
B. 255
C. 640
D. 512

Answer: B

Question No : 8 - (Topic 1)

What steps are needed to enroll a smart-card driver after installation?

A. Edit precheck.txt and deploy it to the Client.
B. Deploy drivers and run pscontrol.exe on Clients to install the drivers.
C. Add the drivers in Windows with the existing Deployment tool.
D. Copy drivers to the smart-card profile, and create a rule in the SmartCenter Policy.

Answer: B

Question No : 9 - (Topic 1)

Each Full Disk Encryption profile is password protected and encrypted two times with _________ AES.

A. 394 bit
B. 256 bit
C. 128 bit
D. 512 bit

Answer: B

Question No : 10 - (Topic 1)

For a machine-specific update within Full Disk Encryption, the Administrator could do all EXCEPT:

A. Configure the settings manually on that machine.
B. Place the update profile in the Publish root-directory.

C. Place the update profile in the update search-path subfolder.
D. Configure the update profile's settings to affect the specific machine only, and push the .upp file in the Work directory.

Answer: C

Question No : 11 - (Topic 1)

Which of the following is NOT a directory path designated in the Full Disk Encryption profile?

A. Logs
B. Software update
C. Recovery
D. Upgrade

Answer: B

Question No : 12 - (Topic 1)

Which of the following choices is not a viable method for configuring the Service Start Account? By modifying the:

A. update profile.
B. settings of the prot_srv service.
C. local folder in the FDEMC.
D. installation profile.

Answer: B

Question No : 13 - (Topic 1)

When you install the SmartCenter for Full Disk Encryption webRH server, how many Administrator accounts do you have to create?

A. None
B. One

C. Ten
D. Two

Answer: D

Question No : 14 - (Topic 1)

From which of the three Full Disk Encryption services running on the local machine is the monitoring program accessible to end users?

A. Prot_srv.exe
B. P95Tray.exe
C. PstartSr.exe

Answer: B

Question No : 15 - (Topic 1)

How many times can a response be used when created with the proper challenge?

A. Two
B. Four
C. One
D. Three

Answer: C

Question No : 16 - (Topic 1)

You are a new administrator for CoopUSA, and are asked to modify settings in an existing configuration set for users in Singapore. Where do you modify these settings?

A. SmartCenter for Pointsec Remote Help
B. FDEMC Remote folder
C. SmartCenter for Pointsec Remote folder
D. FDEMC Local folder

Answer: B

Question No : 17 - (Topic 1)

Which of the following examples is NOT a risk associated with a hard drive that is only protected with Boot Protection/Authentication?

A. Brute force attacks by linking the drive to a separate bootable drive.
B. Bypassing the protection by booting from a floppy.
C. Illicit access to the drive, which can be gained via network connectivity.
D. BIOS passwords, which are weak and susceptible to attacks.

Answer: C

Question No : 18 - (Topic 1)

Which Full Disk Encryption profile type requires two different administrator authentications?

A. Update
B. Install
C. Uninstall
D. Upgrade

Answer: C

Question No : 19 - (Topic 1)

When an installation fails, where is the error log file written?

A. On a floppy disk
B. The NT system-event log
C. The error log directory at the installation point
D. The error log file on the desktop

Answer: C

Question No : 20 - (Topic 1)

Which is a Full Disk Encryption Remote Help property?

A. Both the user and assisting accounts must have the proper rights assigned to give and receive Remote Help.
B. The challenges and responses are always static.
C. The challenge-and-response phrases are always alphanumeric.
D. Preboot messages to end users are clear and concise.

Answer: A

Question No : 21 - (Topic 1)

Which data-protection method provides an effective deterrent to illicit network access via network-connected machines, especially if these machines are linked as part of a VPN?

A. File encryption
B. Full disk encryption
C. User authentication
D. Boot protection

Answer: C

Question No : 22 - (Topic 1)

Which input devices are not supported at the Pre-Boot authentication?

A. X9.9 Dynamic Challenge / Response Tokens
B. Biometric devices
C. USB keyboards
D. USB smartcard tokens

Answer: B

Question No : 23 - (Topic 1)

What must a user do when upgrading a Windows 2000 operating system to Windows XP with Full Disk Encryption installed?

A. Run the operating-system upgrade patch.
B. Uninstall Pointsec before upgrading.
C. Defragment the hard drive before upgrading the operating system.
D. Log in as Administrator.

Answer: B

Question No : 24 - (Topic 1)

When creating an image using software such as Ghost, at what point is Full Disk Encryption installed when creating the image?

A. Pointsec can not be installed in an image.
B. At anytime, as long as the machine is first rebooted.
C. As the first application.
D. As the last application before imaging.

Answer: D

Question No : 25 - (Topic 1)

Which Microsoft file does Full Disk Encryption chain when Pointsec Single Sign On is enabled?

A. MicroSSO.dll
B. Ssogina.dll
C. Msso.dll
D. MSGina.dll

Answer: D

Question No : 26 - (Topic 1)

Which log entry element is unique to each entry and should be given to support?