



TestKingonline.com

No Pass No Pay!

MCSE, CCNA, CCNP, OCP, CIW, JAVA, Sun Solaris, Checkpoint

World No 1 Cert Exams

70-557

Congratulations!

You have purchased a TestKingonline. Study Guide.

This study guide is a complete collection of questions and answers that have been developed by our professional & certified team.

You must study the contents of this guide properly in order to prepare for the actual certification test. The average time that we would suggest you for studying this study guide is approximately 10 to 20 hours and you will surely pass your exam. We guarantee it!
GOOD LUCK!

DISCLAIMER

This study guide and/or material is not sponsored by, endorsed by or affiliated with Microsoft, Cisco, Oracle, Citrix, CIW, Checkpoint, Novell, Sun/Solaris, CWNA, LPI, ISC, etc. All trademarks are properties of their respective owners.

Guarantee

If you use this study guide correctly and still fail the exam, send a scanned copy of your official score notice at:

Sales@Testkingonline.com

We will gladly refund the cost of this study guide or give you an exchange of study guide of your choice of the Free.

This material is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Question: 1

You deploy Forefront Client Security to all client computers. Your corporate security policy states that all client computers should update their status to a collection server every 24 hours. You need to identify the number of computers that do not adhere to the corporate security policy. What should you do?

- A. Review the Computer Summary report.
- B. Review the Connectivity Summary report.
- C. Run the gpresult.exe command with the /z parameter.
- D. Run the fcassondemand.exe command with the /v parameter.

Answer: B

Question: 2

You update your Forefront Client Security policy. You need to identify what percentage of client computers are using an outdated Client Security policy. What should you do?

- A. View the Malware Summary report.
- B. View the Deployment Summary report.
- C. Run the rptutil.exe command.
- D. Run the msascui.exe command.

Answer: B

Question: 3

You deploy Forefront Client Security to all client computers. You need to verify that all client computers have up-to-date antivirus definitions. What should you review?

- A. Deployment Summary report
- B. fcsam.log file
- C. Malware Summary report
- D. Security event log

Answer: A

Question: 4

You deploy Forefront Client Security to all client computers. You need to identify which client computers have not communicated to the Client Security collection server for more than 30 days. What should you do?

- A. Run the rptutil.exe command.
- B. Run the fcslocalpolicytool.exe command.
- C. Review the Alerts Detected report.
- D. Review the Connectivity Summary report.

Answer: D

Question: 5

You deploy Forefront Client Security to all client computers. You need to ensure that a client computer is clean of all known malware. What should you do?

- A. On the client computer, run cleanmgr.exe /d.

- B. From the Forefront Server Security Administrator, start a manual scan.
- C. From the Forefront Client Security Management Console, run a full scan.
- D. From the Microsoft Operations Manager (MOM) 2005 Administrator Console, run attribute discovery.

Answer: C

Question: 6

You deploy Forefront Client Security to all client computers. You need to identify how many computers the Client Security server failed to contact during the preceding 24 hours. What should you do?

- A. In the Forefront Client Security Management Console, review the Reporting Critical Issues chart.
- B. In the Forefront Client Security Management Console, review the Not Reporting chart.
- C. In the Microsoft Operations Manager (MOM) 2005 Operator Console, review the Critical State Count.
- D. In the Microsoft Operations Manager (MOM) 2005 Operator Console, review the Warning State Count.

Answer: B

Question: 7

You deploy Forefront Client Security to all client computers. You need to identify which client computers are running the World Wide Web Publishing Service. What should you do?

- A. Generate a Deployment Summary report.
- B. Generate a Security State Assessment report.
- C. Review the fcsam.log file on the client computers.
- D. Review the serversetup.log file on the Client Security server.

Answer: B

Question: 8

You deploy Forefront Client Security to all client computers. You need to identify which local user accounts have passwords that do not expire. What should you do?

- A. Use the msinfo32.exe command.
- B. Use the fscstarter.exe command.
- C. Review the Alerts Summary report.
- D. Review the Security State Assessment report.

Answer: D

Question: 9

You deploy Forefront Client Security to all client computers. You need to identify what percentage of computers has a Client Security policy deployed by using a registry file. Which value should you review in the Policy Deployment Status chart?

- A. Current Computers
- B. External Computers
- C. Older Computers
- D. Unknown Computers

Answer: B

Question: 10

You deploy Forefront Security for Exchange Server (FSE). You need to manually update the worm purging list with custom viruses. You must ensure that your edits are not overwritten when the new worm purge list is released. What should you do?

- A. Edit the pdmkl.dat file. Add the list of custom viruses to the file.
- B. Edit the wormprge.dat file. Add the list of custom viruses to the file.
- C. Create a file named vdl.dat. Add the list of custom viruses to the file.
- D. Create a file named custprge.dat. Add the list of custom viruses to the file.

Answer: D

Question: 11

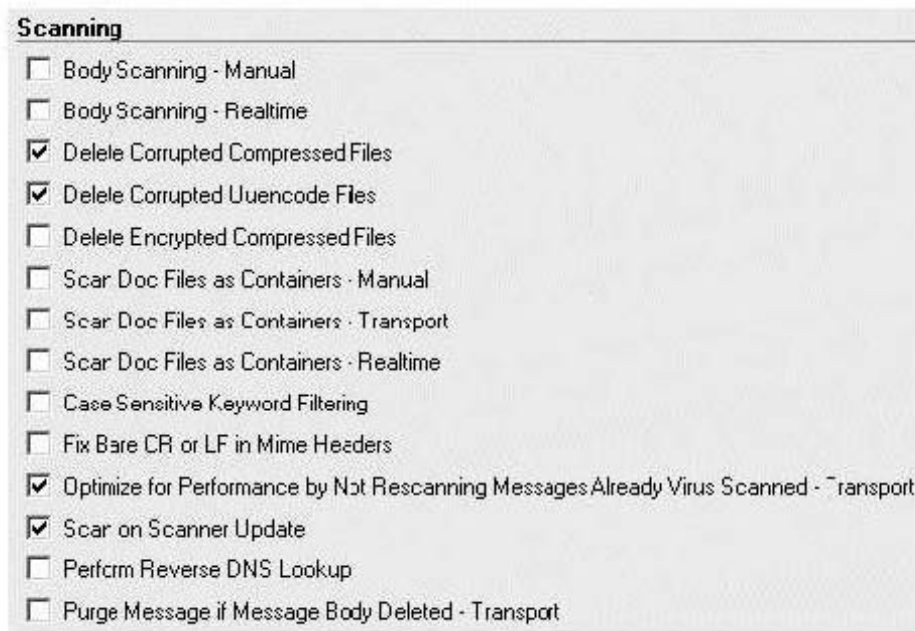
You deploy Forefront Security for Exchange Server (FSE). You enable a keyword filter list that contains the words SPAM, RICH, MILLIONS, and WATCH. You need to configure FSE to delete messages that contain all the words in the keyword filter list. What should you do?

- A. Modify the File Types option.
- B. Modify the Minimum Unique Keyword Hits value.
- C. Set the bias to Maximum Certainty for the Realtime Scan Job.
- D. Set the bias to Maximum Certainty for the Transport Scan Job.

Answer: B

Question: 12

You deploy Forefront Security for Exchange Server (FSE). Users report that access to new e-mail attachments is very slow.



Setting	Checked
Body Scanning - Manual	☐
Body Scanning - Realtime	☐
Delete Corrupted Compressed Files	☒
Delete Corrupted Uuencode Files	☒
Delete Encrypted Compressed Files	☐
Scan Doc Files as Containers - Manual	☐
Scan Doc Files as Containers - Transport	☐
Scan Doc Files as Containers - Realtime	☐
Case Sensitive Keyword Filtering	☐
Fix Bare CR or LF in Mime Headers	☐
Optimize for Performance by Not Rescanning Messages Already Virus Scanned - Transport	☒
Scan on Scanner Update	☒
Perform Reverse DNS Lookup	☐
Purge Message if Message Body Deleted - Transport	☐

You view the FSE Scanning settings as shown in the following exhibit. (Click the Exhibit button.) You need to reduce the amount of time it takes for users to access new e-mail attachments. What should you do?

- A. Clear the Scan on Scanner Updates option.
- B. Clear the Delete Corrupted Uencode Files option.
- C. Select the Perform Reverse DNS Lookup option.
- D. Select the Fix Bare CR or LF in Mime Headers option.

Answer: A

Question: 13

You need to configure Forefront Security for Exchange Server (FSE) to scan the bodies and attachments of all e-mail messages when you run a Manual Scan Job. What should you do?

- A. Select the Enable Store Scanning option.
- B. Select the Enable Transport Scanning option.
- C. Enable the Body Scanning C Manual option.
- D. Enable the Body Scanning C Realtime option.

Answer: C

Question: 14

You deploy Forefront Security for SharePoint (FSSP). You need to configure FSSP to meet the following requirements: Scans all documents that are stored on a SharePoint site Removes all documents that contain a specific word What should you do?

- A. Configure the Realtime Scan Job to use a keyword filter list, and then select Delete: remove infection.
- B. Configure the Realtime Scan Job to use a file filter list, and then select Block: prevent transfer.
- C. Configure the Manual Scan Job to use a keyword filter list, and then select Delete: remove infection.
- D. Configure the Manual Scan Job to use a file filter list, and then select Delete: remove contents.

Answer: C

Question: 15

You deploy Forefront Security for SharePoint (FSSP) to a server. You need to configure FSSP so that all files copied to the document store are scanned by at least five scan engines. What should you do?

- A. Set the bias for the Realtime Scan Job to Neutral.
- B. Set the bias for the Quick Scan Job to Maximum Certainty.
- C. Set the bias for the Realtime Scan Job to Maximum Certainty.
- D. Set the bias for the Quick Scan Job to Maximum Performance.

Answer: C

Question: 16

You deploy two Forefront Security for SharePoint (FSSP) servers named Server1 and Server2. Server1 downloads scan engine updates from Server2. Server2 fails. You need to force an immediate update of the scan engines on Server1. What should you do on Server1?

- A. Enable the Send Update Notification option.
- B. Enable the Scan On Scanner Updates option.
- C. Modify the primary update path, and then click the Update Now button.
- D. Modify the primary update path, and then clear the Redistribution Server option.

Answer: C

Question: 17

You deploy Forefront Security for Exchange Server (FSE). You need to identify e-mail attachments that have been removed from specific messages. What should you do?

- A. Review viruslog.txt for entries that begin with State:.
- B. Review the Security event log for Object Access events.
- C. Review hrlog.txt for entries that contain antigenpmdatamap.
- D. Review programlog.txt for entries that contain Realtime Scanner Index.

Answer: A

Question: 18

You need to identify which scan engine version is being used by Forefront Security for Exchange Server (FSE). Which command should you use?

- A. fscdiag.exe
- B. fscmonitor.exe
- C. fscutility.exe
- D. getenginefiles.exe

Answer: A

Question: 19

You need to configure Forefront Security for Exchange Server (FSE) so that attachments are not scanned when forwarded from quarantine. What should you do?

- A. Select Secure Mode from the Deliver from Quarantine Security list.
- B. Select Compatibility Mode from the Deliver from Quarantine Security list.
- C. Select Quarantine as Single EML file from the Quarantine Messages list.
- D. Select Quarantine Message Body and Attachments Separately from the Quarantine messages list.

Answer: B

Question: 20

You deploy Forefront Security for Exchange Server (FSE) to a server. The server quarantines an attachment that was delivered in an e-mail message. You need to make the attachment available to the intended recipient. What should you do?

- A. In Forefront Security for Exchange Server, click the Export button.
- B. In Forefront Security for Exchange Server, click the Deliver button.
- C. In Forefront Security for Exchange Server, add the recipient to the Allowed Senders list.
- D. Copy quarantine.mdb from the %programfiles%\Microsoft Forefront Security\Exchange Server\Data\Quarantine directory to the recipients computer.

Answer: B

Question: 21

You deploy Forefront Security for Exchange Server (FSE) on a computer named Server1. Server1 is configured to receive all

e-mail messages sent from the Internet. You need to configure FSE to only scan e-mail messages that are received from the Internet. What should you do?

- A. Configure the Realtime Scan Job to scan all mailboxes.
- B. Configure the Transport Scan Job to scan inbound messages.
- C. Configure the Transport Scan Job to scan internal messages.
- D. Configure the Transport Scan Job to scan outbound messages.

Answer: B

Question: 22

You deploy Forefront Security for Exchange Server (FSE).

You need to configure a scan job to meet the following requirements: It must support scanning of mailbox databases. It must support scheduling. It must only use a single scan engine.

What should you do?

- A. Modify the bias of the Realtime Scan Job to Neutral.
- B. Modify the bias of the Transport Scan Job to Favor Certainty.
- C. Modify the bias of the Realtime Scan Job to Favor Performance.
- D. Modify the bias of the Manual Scan Job to Maximum Performance.

Answer: D

Question: 23

You deploy Forefront Client Security to all client computers. Client Security is configured to perform security state assessment (SSA) scans of all client computers. You need to configure Client Security to generate alerts when the SSA scans fail to run. What should you do?

- A. On the client computers, run `ipconfig /registerdns`.
- B. On the client computers, run `clientsetup.exe /i policyname.reg`.
- C. On the Client Security server, run `fcslocalpolicytool.exe /i policyname.reg`.
- D. On the Forefront Client Security Management Console, set the reporting alert level to 3.

Answer: D

Question: 24

Your network contains a Windows Server Update Services server named Server1. Server1 distributes updates from Microsoft Update to all client computers. Forefront Client Security is deployed to all client computers. You need to ensure that all client computers receive up-to-date malware definition updates from Server1. What should you do?

- A. Synchronize Windows Defender definition updates.
- B. Synchronize Forefront Client Security definition updates.
- C. Synchronize Microsoft Windows 2000, Windows XP, and Windows Vista updates.
- D. Configure the Allow Automatic Updates immediate installation Group Policy setting.

Answer: B

Question: 25

Your network contains several file servers managed by a Microsoft Operations Manager (MOM) server named Server1. You deploy a Forefront Client Security server on the network. You need to deploy a Client Security agent and reporting components to all file servers.

You must maintain the association between the file servers and Server1. What should you do?

- A. Deploy a MOM agent to each file server.
- B. Create a Client Security policy, and then deploy the policy to each file server.
- C. Use the MOM Administrator console to configure the failover options of Server1.
- D. Use Client Security client setup to add a second management group to each file server.

Answer: D

Question: 26

You need to deploy Forefront Client Security to all client computers without installing the reporting components. Which command should you use?

- A. clientsetup.exe /nomom
- B. fcslocalpolicytool.exe
- C. msixexec.exe /i asdat.msi
- D. msixexec.exe /i momagent.msi

Answer: A

Question: 27

Your network contains a single Active Directory domain. All desktop and portable computers are located in an organizational unit (OU) named Workstations. You deploy the Forefront Client Security agent to all computers. You create a security group named Executive Users that contains the user accounts of all executives. You create a security group named Executive Laptops that contains the computer accounts of all executives portable computers. You need to design a solution that meets the following requirements: All Client Security events that occur on the executive portable computers must be reported to the Client Security collection server. Default reporting settings must be maintained for desktop computers located in the Workstations OU. You create a new Client Security policy. What should you do next?

- A. Set the alert level to 1, and then deploy the new policy to the domain.
- B. Set the alert level to 1, and then deploy the new policy to the Workstations OU.
- C. Set the alert level to 5, and then deploy the new policy to the Executive Users group.
- D. Set the alert level to 5, and then deploy the new policy to the Executive Laptops group.

Answer: D

Question: 28

Your internal network contains a Forefront Client Security server. A firewall separates the internal network from the perimeter network. You need to configure the firewall so that the Client Security server can manage a server in the perimeter network. Which TCP and UDP port should you open?

- A. Port 443
- B. Port 1723
- C. Port 1433
- D. Port 1270

Answer: D

Question: 29

You subscribe to the Forefront Client Security Malware Summary report. The report is automatically saved to a shared folder on a report server. You need to automatically receive the Malware Summary report by e-mail. What should you do?

- A. Set the SpyNet reporting level to Advanced in the Client Security policy.
- B. Configure the SMTP settings in the Mail item of the Client Security server Control Panel.
- C. Configure the SMTP settings on the Microsoft Operations Manager (MOM) 2005 Administration Console.
- D. Configure the SMTP settings by using the Microsoft SQL Server 2005 Reporting Services Configuration tool.

Answer: D

Question: 30

Your network contains one Forefront Client Security server. You plan to deploy a Client Security agent to a client computer. You need to configure the Client Security agent to report to the Client Security collection server. What should you do?

- A. Run msascui.exe with the /q parameter.
- B. Run clientsetup.exe with the /ms and /cg parameters.
- C. Deploy fcassa.msi by using a Group Policy object (GPO).
- D. Deploy fcslocalpolicytool.exe by using a Group Policy object (GPO).

Answer: B

Question: 31

You deploy Forefront Client Security to all client computers. You schedule a full scan to run every night at 21:00. You need to configure the client computers to perform the scan by using the most up-to-date definition updates available. What should you do?

- A. Configure Windows Server Update Services to synchronize every night at 20:50.
- B. On the client computers, create a scheduled task to run gpupdate /force every night at 21:00.
- C. On the client computers, enable the Allow Automatic Updates immediate installation Group Policy setting.
- D. In the Client Security policy, select the Check for updates before starting a scheduled scan check box.

Answer: D

Question: 32

You deploy a Forefront Client Security policy to an organizational unit (OU) that includes several user and computer accounts. You need to ensure that the policy is immediately applied. What should you do?

- A. On each computer, run ipconfig /flushdns.
- B. On each computer, run gpupdate /target:user /force.
- C. On each computer, run gpupdate /target:computer /force.
- D. Instruct each user to log off the computer, and then log on again.

Answer: C

Question: 33

You deploy Forefront Client Security to all client computers. Client computers are located in offices in three cities. You need to configure Client Security to display reports based on the client computers in each city. What should you do?

- A. For each city, create a separate Active Directory site.
- B. For each client computer, modify the Location attribute in Active Directory.
- C. For each city, create a separate organizational unit (OU) that contains the client computers in that city. Deploy a Client Security

policy to the domain.

- D. For each city, create a separate security group that contains the client computers in that city. Deploy a separate Client Security policy to each security group.

Answer: D

Question: 34

You deploy Forefront Client Security to all client computers. You configure a Microsoft Operations Manager (MOM) 2005 operator group named FCS Admins. FCS Admins contains e-mail-enabled user accounts. You notice that the FCS Admins operator group is not notified when Client Security alerts are generated in the MOM 2005 Administrator Console. You verify that MOM 2005 is configured with a valid SMTP server and that FCS Admins contains the appropriate user accounts. You need to ensure that FCS Admins receives Client Security alerts by e-mail. What should you do next?

- A. In the MOM 2005 Administrator Console, add FCS Admins to Custom Fields 1 on the Custom Alerts Field tab.
- B. In the MOM 2005 Administrator Console, add the FCS Admins operator group to the Client Security notification group.
- C. On the Client Security server, add the FCS Admins operator group to the local MOM 2005 Administrators group.
- D. In the Client Security policy, change the reporting alert level to 5.

Answer: B

Question: 35

You deploy Forefront Security for SharePoint (FSSP) to two computers named Server1 and Server2. You need to configure Server1 to download scan engine updates from Server2 only. What should you do?

- A. Configure Server1 as a redistribution server.
- B. Configure Server1 to send update notifications.
- C. On Server1, modify the primary network update path in the Scanner Updates options.
- D. On Server1, modify the secondary network update path in the Scanner Updates options.

Answer: C

Question: 36

You deploy Forefront Security for SharePoint (FSSP). You need to receive a notification when a user attempts to upload a document that contains a blocked word to a SharePoint site. What should you do?

- A. Add your user account to the SharePoint administrators group.
- B. From the Forefront Server Security Administrator, configure the File Administrators (SP Realtime Scan, Email) notification.
- C. From the Forefront Server Security Administrator, configure the Keyword Administrators (SP Manual Scan, Email) notification.
- D. From the Forefront Server Security Administrator, configure the Keyword Administrators (SP Realtime Scan, Email) notification.

Answer: D Question: 37

You need to disable scanning engine updates on a Forefront Security for SharePoint (FSSP) server. What should you do?

- A. From the General Options work pane, clear the Perform Updates at Startup option.
- B. From the Scanner Updates work pane, select and disable all scanning engines.
- C. From the Antivirus work pane, select SharePoint (Manual scan job), and then disable the engine.
- D. From the Antivirus work pane, select SharePoint (Realtime scan job), and then disable the engine.

Answer: B

Question: 38

You install Microsoft Exchange Server 2007 and Forefront Security for Exchange Server (FSE) on two computers named Server1 and Server2. You install only the Mailbox server role on Server1. You install only the Hub Transport server role on Server2. You need to configure FSE to scan all e-mail messages opened by users, following each scan engine update. What should you do?

- A. Enable Scan on Scanner Update on Server1.
- B. Enable Scan on Scanner Update on Server2.
- C. Set the bias to Maximum Certainty on the Realtime Scan Job.
- D. Set the bias to Maximum Certainty on the Transport Scan Job.

Answer: A

Question: 39

You deploy Forefront Security for Exchange Server (FSE) to all five Microsoft Exchange Server 2007 servers in your company. You need to scan e-mail messages for viruses before the messages are delivered to the Mailbox servers. What should you do?

- A. Create a Transport Scan Job template. Load the Transport Scan Job template to all Hub Transport servers.
- B. Create a Realtime Scan Job template. Load the Realtime Scan Job template to all Mailbox servers.
- C. Create a Realtime Scan Job template. Load the Realtime Scan Job template to all Hub Transport servers.
- D. Create a Manual Scan Job template. Load the Manual Scan Job template to all Mailbox servers.

Answer: A

Question: 40

You deploy Forefront Security for SharePoint (FSSP) to the network. You need to design a solution that meets the following requirements: Prevents users from copying MPG files to the SharePoint sites Allows administrators to use Forefront Server Security reports to identify when users attempt to copy restricted files What should you do?

- A. Modify the blocked file types list on the SharePoint Central Administration page.
- B. Use a Group Policy object to deploy fscrealtimeScanner.exe to all client computers.
- C. Create a custom Web Part. Publish the Web Part to the SharePoint site default home page.
- D. Assign a file filter list to the Realtime Job Scan from the Forefront Server Security Administrator.

Answer: D

Question: 41

You deploy Forefront Security for Exchange Server (FSE). You need to configure FSE to notify you when a scan job is initiated on the FSE server. What should you do?

- A. Add your e-mail address to the Critical Notification List option, and then run fscutility.exe /status.
- B. Add your e-mail address to the Internal Address option, and then run fscutility.exe /status.
- C. Add your e-mail address to the File Administrators notification role, and then enable Notify on Startup.
- D. Add your e-mail address to the Virus Administrators notification role, and then enable Notify on Startup.

Answer: D

Question: 42

You need to configure Forefront Security for Exchange Server (FSE) to scan e-mail messages sent from the contoso.com domain. E-mail messages sent from contoso.com must be delivered even if they contain potentially harmful attachments. What should you

do?

- A. Add *.contoso.com to the allowed sender list. Enable the list for a Transport Scan Job.
- B. Add *@contoso.com to the sender-domains filter. Enable the filter for a Realtime Scan Job, and then set the filter action to Skip: detect only.
- C. Add *@contoso.com to the keyword filter. Enable the filter for a Transport Scan Job, and then set the filter action to Identify: tag message.
- D. Add *@contoso.com to the sender-domains filter. Enable the filter for a Realtime Scan Job, and then set the filter action to Purge: eliminate message.

Answer: B

Question: 43

You deploy Forefront Security for SharePoint (FSSP). You need to configure FSSP to send a notification to a user who copies a virus-infected file to a SharePoint site. Notifications must not be sent to other users. Which notification role should you modify?

- A. Virus Author
- B. Virus Administrators
- C. File Author
- D. File Last Modified User

Answer: A

Question: 44

You deploy Forefront Security for SharePoint (FSSP). You need to reduce the amount of Internet bandwidth the FSSP servers use when they download antivirus updates. What should you do?

- A. Enable the Send Updates Notification option.
- B. Set a secondary Network Update Path for each FSSP server.
- C. Enter a UNC Username and Password, and then enable the Use UNC Credentials option on each FSSP server.
- D. Create a redistribution server, and then configure the remaining FSSP servers to use the redistribution server.

Answer: D

Question: 45

You need to create a script to deploy Forefront Security for Exchange Server (FSE) templates to a server. Which tool should you use in the script?

- A. fscdiag.exe
- B. fscexec.exe
- C. fscstarter.exe
- D. fscutility.exe

Answer: C

Question: 46

Your company has two servers running Forefront Security for Exchange Server (FSE). The servers are named Server1 and Server2. You need to modify the deletion text for the Transport Scan Job on both servers. What should you do?

- A. Create a new template on Server1 named Transport Scan Job. Modify the deletion text for the new template.

- B. Modify the deletion text for the Default (Transport Template) template on Server1. Copy scanjobs.fdb from Server1 to Server2.
- C. Modify the deletion text for the Transport Scan Job on Server1. Restart the Forefront Server Controller Service on Server2.
- D. Modify the deletion text for the Default (Transport Template) template on Server1. Load the template to the Transport Scan Job on Server1 and Server2.

Answer: D

Question: 47

You deploy Forefront Security for Exchange Server (FSE). You configure one FSE server as a redistribution server. You configure the other FSE servers to pull updates from the redistribution server. You need to configure the update path of the FSE servers to pull updates from a default Microsoft update server when the redistribution server is unavailable. What should you do?

- A. On the FSE servers, enable Windows Update.
- B. On a DNS server, add an SRV resource record for a Windows Update server. Set the weight of the record to 200.
- C. On the FSE servers, set the secondary update path to use the default Microsoft update path.
- D. On the FSE servers, set the secondary update path to use the UNC path of the redistribution server.

Answer: C