Administration of Symantec Endpoint Protection 14

1. Match the following list of ports used by Symantec Endpoint Protection (SCP) to the defining characteristics by clicking and dragging the port on the left to the corresponding description on the right.

Exhibit A:

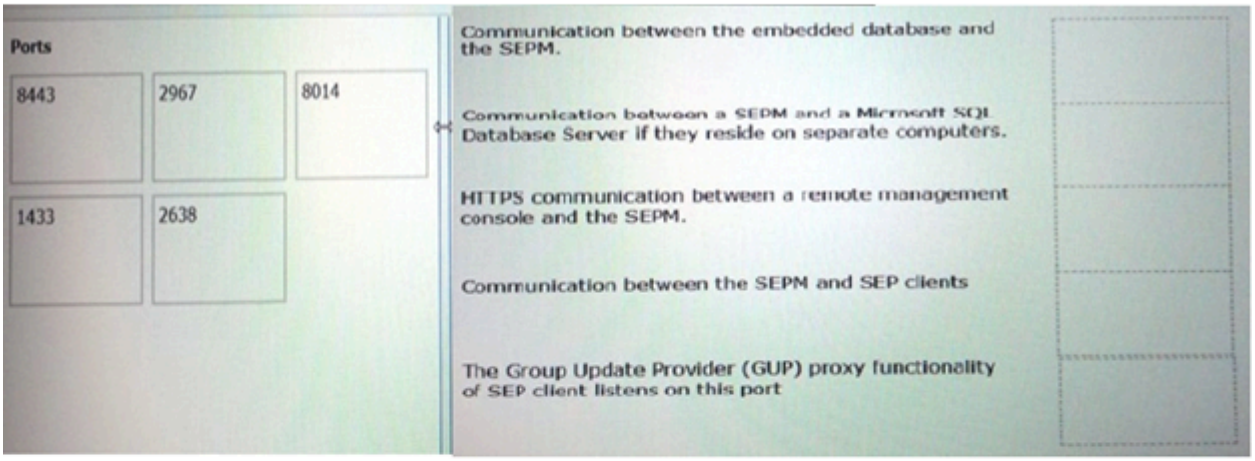
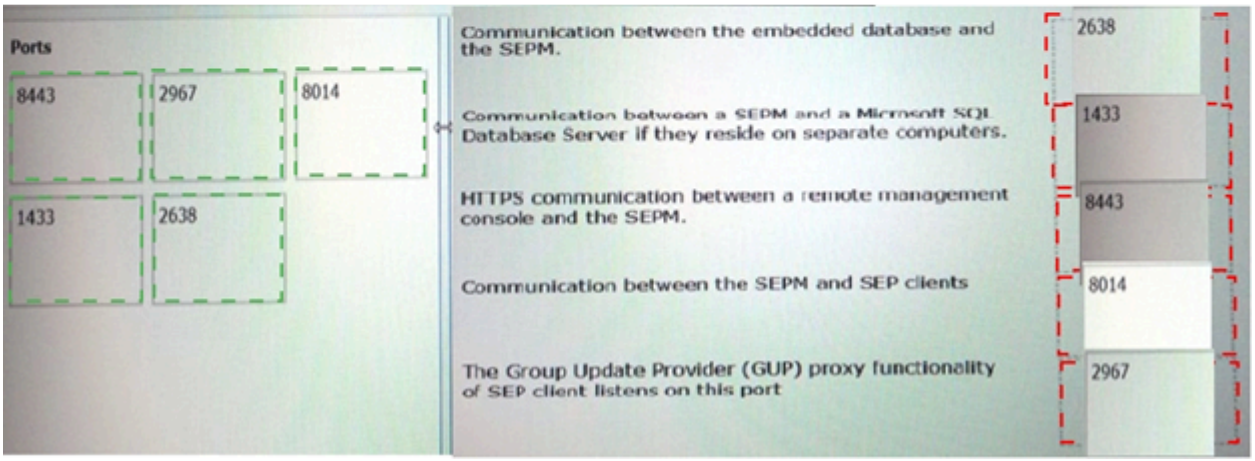


Exhibit B:



A. Please refer to Exhibit B for the answer.

Answer(s): A

---

2. Which ports on the company firewall must an administrator open to avoid problems when connecting to Symantec Public LiveUpdate servers?

A. 25, 80, and 2967

B. 2967, 8014, and 8443

C. 21, 443, and 2967

D. 21, 80, and 443

Answer(s): D

---

3. An administrator reports that the Home, Monitors, and Report pages are absent in the Symantec Endpoint Protection Management console when the administrator logs on. Which action should the administrator perform to correct the problem?

A. configure proxy settings for each server in the site

B. configure External Logging to Enable Transmission of Logs to a Syslog Server

C. grant the Administrator Full Access to Root group of the organization

D. grant View Reports permission to the administrator

Answer(s): D

---

4. Which option is unavailable in the Symantec Endpoint Protection console to run a command on the group menu item?

A. Disable SONAR

B. Scan

C. Disable Network Threat Protection

D. Update content and scan

Answer(s): A

---

5. Which task is unavailable for administrative accounts that authenticate using RSA SecurID Authentication?

A. reset forgotten passwords

B. import organizational units (OU) from Active Directory

C. configure external logging

D. enable Session Based Authentication with Web Services

Answer(s): A

---

6. A financial company enforces a security policy that prevents banking system workstations from connecting to the Internet.
Which Symantec Endpoint Protection technology is ineffective on this company's workstations?

A. Insight

B. Intrusion Prevention

C. Network Threat Protection

D. Browser Intrusion Prevention

Answer(s): A

---

7. Which action does SONAR take before convicting a process?

A. quarantines the process

B. blocks suspicious behavior

C. reboots the system

D. checks the reputation of the process

Answer(s): D

---

8. An administrator is using the SylinkDrop tool to update a Symantec Endpoint Protection client install on a system. The client fails to migrate to the new Symantec Endpoint Protection Manager (SEPM), which is defined correctly in the Sylink.xml file that was exported from the SEPM.
Which settings must be provided with SylinkDrop to ensure the successful migration to a new Symantec Endpoint Protection environment with additional Group Level Security Settings?

A. -s "silent"

B. -t "Tamper Protect"

C. -r "reboot"

D. -p "password"

Answer(s): D

---

9. A Symantec Endpoint Protection (SEP) administrator is remotely deploying SEP clients, but the clients are failing to install on Windows XP.
What are two possible reasons for preventing installation? (Select two.)

- [ ] A. Windows firewall is enabled.
- [ ] B. Internet Connection firewall is disabled.
- [ ] C. Administrative file shares are enabled.
- [ ] D. Simple file sharing is enabled.
- [ ] E. Clients are configured for DHCP.

Answer(s): A D

---

10. Which protection engine should be enabled to drop malicious vulnerability scans against a client system?

A. SONAR

B. Intrusion Prevention

C. Tamper Protection

D. Application and Device Control

Answer(s): B

---

11. What are two criteria that Symantec Insight uses to evaluate binary executables? (Select two.)

- [ ] A. sensitivity
- [ ] B. prevalence
- [ ] C. confidentiality
- [ ] D. content
- [ ] E. age

Answer(s): B E

---

12. Which setting can an administrator configure in the LiveUpdate Policy?

A. specific content revision to download from a Group Update Provider (GUP)

B. specific content policies to download

C. Linux Settings

D. frequency to download content

Answer(s): D

13. The Security Status on the console home page is failing to alert a Symantec Endpoint Protection (SEP) administrator when virus definitions are out of date.
How should the SEP administrator enable the Security Status alert?

A. lower the Security Status thresholds

B. raise the Security Status thresholds

C. change the Notifications setting to "Show all notifications"

D. change the Action Summary display to "By number of computers"

Answer(s): A

---

14. You have executed the vxdg -g diskgroup adddisk disk_name= command.
Which switch needs to be added to force VxVM to take the disk media name of the failed disk and assign it to the new replacement disk?

A. -force

B. -k

C. -f

D. -assign

Answer(s): C

---

15. Which two instances could cause Symantec Endpoint Protection to be unable to remediate a file? (Select two.)

- [ ] A. Another scan is in progress.
- [ ] B. The detected file is in use.
- [ ] C. There are insufficient file permissions.

- [ ] D. The file is marked for deletion by Windows on reboot.
- [ ] E. The file has good reputation.

Answer(s): B C

---

16. After several failed logon attempts, the Symantec Endpoint Protection Manager (SFPM) has locked the default admin account. An administrator needs to make system changes as soon as possible to address an outbreak, but the admin account is the only account.
Which action should the administrator lake to correct the problem with minimal impact to the existing environment?

A. Wait 15 minutes and attempt to log on again

B. Restore the SEPM from a backup

C. Run the Management Server and Configuration Wizard to reconfigure the server

D. Reinstall the SEPM

Answer(s): A

---

17. Users report abnormal behavior on systems where Symantec Endpoint Protection is installed. Which tool can an administrator run on the problematic systems to identify the likely cause of the abnormal behavior?

A. smc.exe -stop

B. SymHelp.exe

C. PowerShell.exe

D. CleanWipe.exe

Answer(s): B

---

18. What does SONAR use to reduce false positives?

A. Virus and Spyware definitions

B. File Fingerprint list

C. Symantec Insight

D. Extended File Attributes (EFA) table

Answer(s): C

---

19. A company plans to install six Symantec Endpoint Protection Managers (SEPMs) spread evenly across two sites. The administrator needs to direct replication activity to SEPM3 server in Site 1 and SEPM4 in Site 2.
Which two actions should the administrator take to direct replication activity to SEPM3 and SEPM4? (Select two.)

- [ ] A. Install SEPM3 and SEPM4 after the other SEPMs
- [ ] B. Install the SQL Server databases on SEPM3 and SEPM4
- [ ] C. Ensure SEPM3 and SEPM4 are defined as the top priority server in the Site Settings
- [ ] D. Ensure SEPM3 and SEPM4 are defined as remote servers in the replication partner configuration
- [ ] E. Install IT Analytics on SEPM3 and SEPM4

Answer(s): C D

---

20. The LiveUpdate Download Schedule is set to the default on the Symantec Endpoint Protection Manager (SEPM).
How many content revisions must the SEPM keep to ensure clients that check in to the SEPM every 10 days receive xdelta content packages instead of full content packages?

A. 10

B. 20

C. 30

D. 60

Answer(s): C
