Symantec

Exam ASC-029

ASC Enterprise Security 2010

Version: 6.1

[Total Questions: 70]

Question No : 1

If a consultant fails to identify who will be responsible for post-engagement technical support, who will end up being responsible?

A. the consultant
B. Symantec Support
C. the customer
D. the project manager

Answer: A

Question No : 2

An administrator is seeing errors when host integrity is being evaluated on one client. What will permit them to debug the host integrity script?

A. review the AVScript.js in the Endpoint Protection folder
B. enable SMC Debugging by executing smc -debug at the command line
C. enable Extended TSE Debugging by setting the registry key ExtendedDebuging to 1
D. review the system logs from the SMC GUI

Answer: A

Question No : 3

What is considered a phase within the Symantec Endpoint Protection (SEP) Implementation engagement process?

A. Assess
B. Plan
C. Review
D. Pilot

Answer: A

Question No : 4

An administrator has just installed NAC using a LAN enforcer for a company. They have two LAN enforcers at the corporate data center. Remote office users are complaining that the WAN link is really slow. Using a sniffer, the administrator determines that there is an excessive amount of 802.1x traffic on the WAN link. What should the administrator do to help resolve this issue?

A. turn off 802.1x logging on the switch
B. increase the eap re-authentication period
C. switch eap authentication to eap-tls
D. turn off Symantec Transparent mode NAC

Answer: B

Question No : 5

Which Antivirus and Antispyware administrator-defined policy option may significantly decrease scan time and improve client performance if enabled?

A. run an Active Scan when new definitions arrive
B. trust files on remote computers running Auto-Protect
C. schedule TruScan Proactive Threat Scan to run at the default frequency
D. allow client computers to submit processes detected by scans

Answer: B

Question No : 6

An administrator has enabled Spam Quarantine along with the default Spam policies. A review of the contents of Spam Quarantine shows no legitimate emails. The size of the quarantine is very large and is affecting performance of the Symantec Brightmail Gateway Control Center. Which action should the administrator take?

A. increase the Spam threshold in the Spam to increase the number of messages identified as spam
B. reduce the Suspect Spam threshold to reduce the number of messages identified as Suspect Spam
C. increase the Suspect Spam threshold to reduce the number of messages identified as Suspect Spam
D. set the setting "Do you want messages to be flagged as suspect spam" to "No"

Answer: D

Question No : 7

What is the command line syntax to make the Symantec Endpoint Client Service check for a more recent configuration file on the management server?

A. smc -updateconfig
B. smc -luall
C. smc -getsylink
D. smc -getconfig

Answer: A

Question No : 8

Which two factors should an administrator consider when sizing the database for a Symantec Endpoint Protection design? (Select two.)

A. how often logs a gathered
B. the amount of Symantec Endpoint Protection Manager Groups
C. log retention frequency and size
D. the amount of scheduled reports
E. frequency of notifications

Answer: A,C

Question No : 9

What is the default recommendation for how many content revisions should be retained on the Symantec Endpoint Protection Manager?

A. 12
B. 22
C. 42
D. 52

Answer: C

Question No : 10

The keystore in Symantec Endpoint Protection Manager contains the private-public key pair and the self-signed certificate. These are crucial to have available in a DR scenario. The keystore is password protected, and the password is needed for a recovery. Which file can the administrator find the keystore password in?

A. sylink.xml
B. server.xml
C. conf.properties
D. keystore.jks

Answer: B

Question No : 11

Which two SNAC enforcement options are available without a 6100 Series appliance? (Select two.)

A. LAN Enforcement
B. DCHP Enforcement
C. Gateway Enforcement
D. Peer to Peer Enforcement
E. 802.1x Enforcement

Answer: B,D

Question No : 12

A company's CEO has recently read about "Green IT" and wants it implemented. The administrator has been asked to provide recommendations for the company's existing Brightmail Gateway Scanners and Control Center. The CIO has asked to also ensure that: - There is no impact to the companies 5,000 email users. - The result is easier to manage and perform changes with zero downtime maintenance. - The solution can quickly cope with a substantial increase in spam. What should the administrator recommend?