ST0-29B

Symantec Endpoint Protection 11 MR4 (STS)

Version 4.1

ST0-29B

Topic 1, Volume A

QUESTION NO: 1

An administrator has successfully installed Symantec Endpoint Protection Manager onto a Windows 2003 Server using the installation wizard. Which component is deployed to the server at this point in time?

A. AntiVirus/AntiSpyware Protection

B. Proactive Threat Protection

C. Apache Tomcat Server

D. Central Quarantine Server

E. Network Threat Protection

Answer: C

QUESTION NO: 2

Based on Symantec best practices, which two tasks should be performed before migrating from Symantec AntiVirus Corporate Edition to Symantec Endpoint Protection 11.0? (Select two.)

A.disable Auto-Protect

B.disable scheduled scans

C.disable Tamper Protection

D.scan all clients

E.purge the quarantine

Answer: B, C

ST0-29B

QUESTION NO: 3

Which Symantec Endpoint Protection client component must be installed to enable Unmanaged Detector mode?

A. AntiVirus and AntiSpyware

B. Application and Device Control

C. Network Threat Protection

D. Network Access Control

Answer: C

QUESTION NO: 4

How many Symantec Endpoint Protection Managers can connect to an embedded database?

A. one

B. two

C. four

D. unlimited

Answer: A

QUESTION NO: 5

Immediately after installation, what does a client do upon first contacting Symantec Endpoint Security Manager?

A. register with the manager

B. download the latest policy

C. update virus definitions

D. launch a full system scan

Answer: A

QUESTION NO: 6

Which file contains the Symantec Endpoint Protection client communication settings?

A. GRC.dat

B. Sylink.xml

C. GRC.xml

D. Sylink.dat

Answer: A

QUESTION NO: 7

What is the default replication frequency when adding an additional site to a Symantec Endpoint Protection deployment?

A. 1 hour

B. 8 hours

C. daily

D. weekly

Answer: C

QUESTION NO: 8

An administrator makes a change in the Active Directory structure, which has been imported into Symantec Endpoint Protection Manager (SEPM). By default, when will the change automatically be reflected in SEPM?

A. as soon as the change is made in Active Directory

B. maximum 1 hour

C. maximum 4 hours

D. maximum 24 hours

Answer: D

QUESTION NO: 9

In which client management log can an administrator identify when the client last connected to the Symantec Endpoint Protection Manager?

A. Control

B. Traffic

C. System

D. Event

Answer: C

QUESTION NO: 10

ST0-29B

Which setting can be enabled to report computers without a Symantec Endpoint Protection Agent?

A. LAN Detector

B. Unmanaged Detector

C. Segment Detector

D. Network Detector

Answer: D

QUESTION NO: 11

A Symantec Endpoint Protection Manager administrator is importing from an Active Directory environment. The director needs to know which object types are being imported. Which two object types are imported into Symantec Endpoint Protection Manager from Active Directory? (Select two.)

A.security groups

B.organizational units

C.computers

D.sites

E.domains

Answer: B, C

QUESTION NO: 12

What can an administrator do to proactively obtain information about unknown devices on a network?

A. script a network audit using the Find Unmanaged Computers feature

B. create an Unmanaged Computer notification

C. schedule an audit report to send to the administrator

D. schedule regular LDAP synchronization

Answer: B

QUESTION NO: 13

Which two features migrate from previous versions of Symantec AntiVirus? (Select two.)

A.Tamper Protection Settings

B.AntiVirus Settings

C.Uninstall Password

D.Client Group Structure

E.Firewall Settings

Answer: B, D

QUESTION NO: 14

If a Symantec Endpoint Protection (SEP) client is installed with AntiVirus and AntiSpyware components only, what must be done to install the SEP Firewall?

A. redeploy the original installation package to the client

B. deploy the firewall license file to the Symantec Endpoint Protection Manager

C. deploy a new package including the firewall component

D. deploy a firewall policy to that client through an XML file

Answer: C

ST0-29B

QUESTION NO: 15

Which remediation option is available to administrators using the Find Unmanaged Computers feature?

A. deploy a Symantec Endpoint Protection client package to the unmanaged host

B. monitor and log network traffic observed from the unmanaged host

C. install Microsoft Windows operating system security patches

D. disable network access pending Symantec Endpoint Protection client installation

Answer: C

QUESTION NO: 16

When using the Push Deployment Wizard, which two methods can be used to identify the target machines to which you want to install the Symantec Endpoint Protection client? (Select two.)

A.browse through Windows networking

B.import a file containing IP addresses

C.specify a UNC path

D.import a file containing MAC addresses

E.import hostnames from an LDAP server

Answer: A, B

QUESTION NO: 17

Which feature can be configured to increase or decrease performance of scheduled scans?

A. scan frequency

B. CPU throttling

C. heartbeat interval

D. tuning options

Answer: D

QUESTION NO: 18

Which two actions can the Centralized Exception policy perform? (Select two.)

A.exclude a specific folder from AntiVirus and AntiSpyware File System Auto-Protect scanning

B.specify an exclusion to keep a known risk from being scanned

C.specify machines from which the Symantec Endpoint Protection Manager console cannot be run

D.exclude forwarding of certain log types from the Symantec Endpoint Protection client

E.specify Intrusion Prevention system signatures for exclusion

Answer: A, B

QUESTION NO: 19

Which two actions are available when TruScan Proactive Threat Scan detects a trojan or worm? (Select two.)

A.delete

B.ignore

C.terminate

D.quarantine

E.clean

Answer: C, D

QUESTION NO: 20

An administrator needs a TruScan Proactive Threat scan that will detect a potential trojan, worm, or keylogger as quickly as possible. How should the administrator set the scan frequency?

A. set it to continuous

B. set it to scan new processes immediately

C. select the default setting

D. set it to 5 minutes

Answer: B

QUESTION NO: 21

Lifeline Supply Company deploys a freeware application, EasyWeatherView, that is funded by advertising. It is detected by Symantec Endpoint Protection as Adware.WeatherBorg because it includes banner advertisements in its client interface. The company accepts the risk and treats EasyWeatherView as an undetected application and bypasses the standard adware policy actions. How can this best be configured in Symantec Endpoint Protection?

A. edit the AntiVirus and AntiSpyware policy and set the Primary Action for security risks to Leave Alone

B. edit the Exclusion policy to exclude Adware.WeatherBorg from detection by marking the Exclude checkbox in the Threat list and clearing the

Log Option checkbox