

100% Money Back Guarantee

Vendor: Symantec

Exam Code: ASC-029

Exam Name: ASC Enterprise Security 2010

Version: Demo

QUESTION: 1

When defining location switching criteria, which two can be used? (Select two.)

- A. MAC address
- B. Wins Server address
- C. host name
- D. NIC description
- E. OS type

Answer: B, D

QUESTION: 2

When identifying risks, an administrator should prioritize them according to what? (Select two.)

- A. likelihood of occurrence
- B. order of occurrence
- C. level of inconvenience to the customer
- D. impact to the project
- E. visibility to senior management

Answer: A, D

QUESTION: 3

An administrator has deployed LAN enforcer within the network and enabled 802.1x on all switch ports. How can the administrator ensure that printers directly connected to the switch are still accessible, and also prevent computers bypassing LAN enforcement should they be connected to the printer's network outlet?

- A. install Symantec Endpoint Protection on the printers
- B. add the MAC addresses of the printers to the Trusted Hosts list in the advanced settings of the Enforcer Group properties
- C. log on to the command line of the enforcer, at the command line enter mab enable
- D. log on to the command line of the enforcer, at the command line enter mac and the list of printer MAC addresses

Answer: C

QUESTION: 4

With an 802.1x enabled switch, the SNAC client communicates with the switch at which layer of the OSI reference model for EAP authentication?

- A. Layer 1 (Physical Layer)
- B. Layer 2 (Data Link Layer)
- C. Layer 3 (Network Layer)
- D. Layer 4 (Transport Layer)

Answer: B

QUESTION: 5

At an administrator's first meeting with a customer they realize that their customer is expecting the product to do a certain function that the administrator is sure it cannot accomplish. What should the administrator's response be?

- A. call the account team
- B. escalate to the administrator's manager
- C. provide alternative solutions
- D. call the product manager

Answer: C

QUESTION: 6

A company wants to allow remote users access to the corporate network through a VPN connection. The IT director is afraid that if they allow remote access they cannot be sure the remote users have proper security software installed and running on their PCs and may infect the corporate environment. Which form of NAC enforcement would be most effective in keeping this company safe?

- A. DHCP enforcement
- B. LAN enforcement
- C. Gateway enforcement
- D. Peer to Peer enforcement

Answer: C

QUESTION: 7

How does SEPprep prepare a system for the installation of Symantec Endpoint Protection (SEP)?

- A. SEPprep reports on all SEP dependencies.
- B. SEPprep removes competitive AV products.
- C. SEPprep updates content definitions in a package.
- D. SEPprep checks for communication with the SEPM.

Answer: B

QUESTION: 8

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 Extended Debugging to I
- D. review the system logs from the SMC GUI

Answer: A

QUESTION: 9

When is “Push Mode” preferable to “Pull Mode” when configuring Symantec Endpoint Protection (SEP) Communication settings?

- A. when there is a requirement to conserve network bandwidth
- B. when an administrator needs to quickly install SEP Agents to computers
- C. when managing greater than 5000 computers
- D. when frequentSEPM policychanges requirefrequentclientupdates

Answer: D

QUESTION: 10

Which port is utilized by default for Symantec Endpoint Protection Manager replication between sites?

- A. 8014
- B. 8443
- C. 9090
- D. 2967

Answer: B

QUESTION: 11

An organization has three Symantec Endpoint Protection Managers that are replicating to each other. At most, how often should replication occur?

- A. once perhour
- B. onceevery8 hours
- C. once perday
- D. onceevery4 hours

Answer: C

QUESTION: 12

What are the correct connect settings for a serial console connection?

- A. Data Bits 8, Parity none, Stop Bits 1
- B. Data Bits 8, Parity odd, Stop Bits 1
- C. Data Bits 8, Parity even, Stop Bits 1
- D. Data Bits 8, Parity odd, Stop Bits 2

Answer: A

QUESTION: 13

An administrator has a number of Vontu DLP Network Prevent appliances in their network. Which two configurations on the Brightmail Gateway will ensure that the email load will be distributed evenly between the Vontu appliances? (Select two.)

- A. assign equal priority to all Vontu appliances on the Control Center Console
- B. create DNS MX records for each Vontu appliance. Assign the same MX value for each appliance, use MX look up from the Vontu DLP Connect Connection Settings on the Control Center Console
- C. assign the same IP to all the Vontu appliances
- D. select the check box “enable bypass when all DLP servers are unreachable”
- E. use a NAT firewall to load balance the Vontu DLP servers

Answer: A, B

QUESTION: 14

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: 15

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?

- A. do nothing, as the current appliances meet the “Green IT” standards
- B. replace only the scanners with virtual edition
- C. replace only the Control Center with a virtual edition, as the virtual scanners can only cope with 1,000 or fewer email users
- D. replace all physical appliances with the equivalent virtual edition

Answer: D

QUESTION: 16

What is a goal of the Kick-off meeting?

- A. to confirm hardware order/receipt
- B. to confirm that the client is ready on both business and technical tasks
- C. to confirm key responsibilities and assign initial tasks
- D. to confirm server access and security requirements

Answer: C

QUESTION: 17

Before going to a customer site for solution deployment, what should a consultant check for?

- A. places to stay and eat
- B. product updates
- C. competitive products
- D. customer's competition

Answer: B

QUESTION: 18

After reorganizing a client's network, an administrator is asked to move the Control Center to a different subnet. After updating the IP address of the Control Center appliance, what should the administrator's next action be?

- A. log in to the Management console and reboot the scanners so they will recognize the new IP address of the Control Center
- B. log in to the Management console and restart all the services on the scanners so they will recognize the new IP address of the Control Center
- C. log in to each scanner and use the command `cc-config` twice, once to delete the old Control Center IP address and once to add the new Control Center IP address
- D. log in to each scanner and use the command `agentconfig` twice, once to delete the old Control Center IP address and once to add the new Control Center IP address

Answer: D

QUESTION: 19

Why would an administrator use an ELSE statement when creating a custom HI requirement using IFTHENIENDIF logic?

- A. to identify actions to be taken when the specified conditions are True
- B. to identify actions to be taken when the specified conditions are False
- C. to identify the next step in the logic tree after the ENDIF
- D. to create a loop to check a requirement more than once

Answer: B

QUESTION: 20

Symantec Brightmail Gateway is deployed with a separate Control Center and Scanner. An administrator has enabled end user quarantine and configured an LDAP source for authentication. They have been assigned a troubleshooting ticket that shows users unable to release email quarantine from their quarantine storage. Why is this happening?

- A. Port 22 is blocked between the Control Center and Scanner, preventing the release of quarantine emails.
- B. Port 25 is blocked between the Control Center and the downstream email server, preventing the release of quarantine emails.

- C. Port 41002 is blocked between the Control Center and Scanner, preventing the release of quarantine emails.
- D. Port 41025 is blocked between the Control Center and Scanner, preventing the release of quarantine emails.

Answer: B

QUESTION: 21

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: 22

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: 23

Refer to the exhibit.



What is the most likely cause of the error shown?

- A. uS has been configured to require authentication.
- B. The anonymous account does not have the correct readwrite access to the Symantec Endpoint Protection Manager folders.
- C. The default application pool has not been configured correctly.
- D. The PHP application extension mapping has been configured to limit the number of verbs available.

Answer: D

QUESTION: 24

How can the Symantec Endpoint Protection client debug log be enabled?

- A. set the registry key smc_debug_log_level to Debug
- B. set the registry key smc_debug_log_level to 0
- C. set the registry key smc_debug_log_level to 3
- D. set the registry key smc_debug_log_level to Fatal

Answer: B

QUESTION: 25

What are two goals of the project closeout meeting? (Select two.)

- A. to review solutions to open incidents
- B. to discuss new service opportunities
- C. to obtain project sign-off
- D. to review recommended configuration changes
- E. to review deliverables

Answer: C, E

QUESTION: 26

An administrator is trying to determine when a client last connected to the Symantec Endpoint Protection Manager. Which log on the client machine would have that information?

- A. Event B.
- System C.
- Control D.
- Traffic

Answer: B

QUESTION: 27

When turning on the SNAC on-demand agent on a gateway enforcer, which two settings must be configured on the enforcer prior to turning on the on-demand server? (Select two.)

- A. spm-domain
- B. authentication
- C. client-group D.
- 8021x

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Trying our product !



- ★ **100%** Guaranteed Success
- ★ **100%** Money Back Guarantee
- ★ **365 Days** Free Update
- ★ **Instant Download** After Purchase
- ★ **24x7** Customer Support
- ★ Average **99.9%** Success Rate
- ★ More than **69,000** Satisfied Customers Worldwide
- ★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.	 Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.	 Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.
---	---	--

Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.