

Symantec ST0-132

Symantec Messaging Gateway 9.5 Exam

Practice Test

Version: 14.20

QUESTION NO: 1

In which two situations are multiple group policies useful? (Select two.)

- A. when the entire organization wants to delete spam
- B. when only the Human Resources department wants to receive spam
- C. when only the Engineering department wants to keep message logs
- D. when only the Legal department should be allowed to send archive files
- E. when all of the departments want to scan outbound messages

Answer: B,D

Explanation:

QUESTION NO: 2

Which two actions must be taken to allow end-users to create personal Good and Bad Senders lists? (Select two.)

- A. Add "Hold message in Spam Quarantine" action to Local Bad Senders domains.
- B. Check the option "Enable end-user settings for this policy group".
- C. Configure an LDAP source with Authentication and Recipient Validation functions.
- D. Configure an LDAP source with Authentication and Routing functions.
- E. Configure an LDAP source with Authentication and Address Resolution functions.

Answer: B,E

Explanation:

QUESTION NO: 3

An administrator tests the default antivirus policies by sending a message with an encrypted attachment. When the administrator checks the recipient inbox, what appears?

- A. The test email appears with a modified subjectline.
- B. A system-generated message appears concerning an unscannable attachment.
- C. A pointer to the Suspect Virus Quarantine appears.
- D. The email is missing due to deletion by the system.

Answer: A

Explanation:

QUESTION NO: 4

What is the default time period that a suspect virus can reside in the Suspect Virus Quarantine?

- A. 2 hours
- B. 4 hours
- C. 6 hours
- D. 8 hours

Answer: C

Explanation:

QUESTION NO: 5

How could an administrator filter email more aggressively by adjusting the suspected spam score?

- A. Raise the suspected spam score from the default to 99.
- B. Lower the suspected spam score from the default to 60.
- C. Lower the suspected spam score from the default to 24.
- D. Raise the suspected spam score from the default to 91.

Answer: B

Explanation:

QUESTION NO: 6

A company uses multiple control centers. What must be done to ensure legitimate NDRs are recognized by Bounce Attack Prevention across all scanners?

- A. Configure the same seed value on each control center.
- B. Configure different seed values on each control center.
- C. Configure the same seed value on each scanner.
- D. Configure different seed values on each scanner.

Answer: A

Explanation:

QUESTION NO: 7

Which prerequisite must be met to take advantage of the Connection Classification and Fastpass features?

- A. Symantec Messaging Gateway must use a virtual IP address.
- B. Symantec Messaging Gateway must be configured with two network interfaces.
- C. Symantec Messaging Gateway must be the first SMTP hop into the network.
- D. Symantec Messaging Gateway must be configured in scanner-only mode.

Answer: C

Explanation:

QUESTION NO: 8

Symantec Messaging Gateway 9.5 is certified for non-virtual deployment on which hardware devices?

- A. Symantec 2950 series appliances
- B. Symantec 3570 series appliances
- C. Symantec 7100 series appliances
- D. Symantec 8300 series appliances

Answer: B

Explanation:

QUESTION NO: 9

Message throughput of a Symantec Messaging Gateway scanner-only appliance can be reduced by which two features? (Select two.)

- A. rapid release definitions
- B. real-time updates
- C. DKIM signing
- D. SMTP authentication
- E. hourly quarantine expunging

Answer: C,D

Explanation:

QUESTION NO: 10

What happens if a Symantec Messaging Gateway scanner is behind another internal messaging gateway?

- A. Symantec Messaging Gateway scanners might quarantine all mail from the internal gateway MTA if DKIM is disabled.
- B. Symantec Messaging Gateway scanners might identify the IP address of the internal gateway MTA as a source of spam.
- C. Symantec Messaging Gateway scanners will trust all mail from the internal gateway MTA.
- D. Symantec Messaging Gateway scanners will grant the internal gateway MTA a Fastpass.

Answer: B

Explanation:

QUESTION NO: 11

What is the current name of the LDAP synchronization technology used within the Symantec Messaging Gateway?

- A. Dynamic Data Cache
- B. Directory Data Service
- C. Data Directory Tool
- D. LDAP Directory Service

Answer: B

Explanation:

QUESTION NO: 12

An administrator recently investigated the debug logs for Symantec Messaging Gateway 9.5 and resolved an issue. A few days later the administrator discovers that the disk storage is filling up quickly. What is the likely cause?

- A. Real-time update level is turned up.
- B. Local log level is turned up.
- C. Active user data is turned up.
- D. Remote log level is turned up.

Answer: B

Explanation:

QUESTION NO: 13

Symantec Messaging Gateway 9.5 is running out of disk space due to storing extended logs. The administrator is required to store extended log data for more than a year. Which action should the administrator take?

- A. Lower the maximum log storage limit.
- B. Increase the Messaging Gateway server threads.
- C. Configure remote logging.
- D. Delete messages from the queue.

Answer: C

Explanation:

QUESTION NO: 14

An employee reports that a message sent to a customer was rejected. The employee provides sufficient information for the administrator to find the message using the Message Audit log. The employee wants to know why that message was blocked. Which section of the Message Audit Log detail page would provide this information?

- A. Verdict
- B. Message Header
- C. Tracker
- D. Destination

Answer: A

Explanation:

QUESTION NO: 15

Which Directory Data Source function must be configured to enable end-user spam quarantine?

- A. SMTP authentication
- B. address resolution

- C. recipient validation
- D. authentication

Answer: D

Explanation:

QUESTION NO: 16

A message released from Spam Quarantine is delivered to the intended recipient. Under the default configuration, where is a copy of the misidentified message also sent?

- A. intended recipient's manager
- B. Symantec Security Response
- C. Administrator@localhost
- D. Admin@localhost

Answer: B

Explanation:

QUESTION NO: 17

A diagnostics package for a scanner-only appliance can be generated from the GUI in Symantec Messaging Gateway 9.5. If the package is small (less than 5 MB), which transfer protocol type should be used by the administrator to verify the diagnostics package before providing it to technical support for analysis?

- A. email to administrator
- B. download to desktop
- C. FTP
- D. SCP

Answer: B

Explanation:

QUESTION NO: 18

Where are options for backup and restore of Symantec Messaging Gateway 9.5 located?

- A. Administration -> Version
- B. Administration -> Configuration
- C. Administration -> Control Center
- D. Administration -> Recovery

Answer: A

Explanation:

QUESTION NO: 19

Before performing a software update on a scanner-only appliance, which MTA operation/mode should be chosen if there are messages in the queues?

- A. Stop the MTA.
- B. Accept and deliver messages normally.
- C. Pause message scanning and delivery.
- D. Do not accept incoming messages.

Answer: D

Explanation:

QUESTION NO: 20

What should an administrator do before performing a software update of Symantec Messaging Gateway 9.5?

- A. store backup on local server
- B. store backup on a remote location using FTP
- C. encrypt local backup
- D. purge all backups from the appliance

Answer: C

Explanation:

QUESTION NO: 21

What is the maximum number of incident folders that may be created in Symantec Messaging Gateway 9.5?