

**Symantec ST0-085**

**Symantec Security Information Manager 4.7 Technical  
Assessment  
Version: 4.0**

**QUESTION NO: 1**

Which tab on the Information Manager Console allows you to view threat and vulnerability information?

- A. Rules
- B. Dashboard
- C. Reports
- D. Intelligence

**Answer: D**

**Explanation:**

**QUESTION NO: 2**

Which component escalates security events into incidents?

- A. rules
- B. events
- C. incidents
- D. tickets

**Answer: A**

**Explanation:**

**QUESTION NO: 3**

What does the Correlation Engine analyze events against once all rules are properly defined?

- A. the rule criteria, create triggers, and correlate conclusions into incidents
- B. false positives, create conclusions, and correlate conclusions into incidents
- C. the rule criteria, create conclusions, and correlate conclusions into incidents
- D. the rule criteria, create conclusions, and send conclusions to the database

**Answer: C**

**Explanation:**

**QUESTION NO: 4**

What is the purpose of the critical business assets management feature?

- A. It enables automatic identification and prioritization of security threats that impact business-critical applications.
- B. It obtains an overview of business assets.
- C. It makes it possible to change collectors' configurations to meet business assets needs.
- D. It provides a visual picture of where critical business assets are located.

**Answer: D**

**Explanation:**

#### QUESTION NO: 5

Which of the following vendor hardware is recommended to use with Symantec Security Information Manager (SSIM)?

- A. IBM
- B. NEC
- C. Dell
- D. Hitachi

**Answer: C**

**Explanation:**

#### QUESTION NO: 6

What are the hard drive specifications for the hardware?

- A. 6 drives (2 mirrored and 4 in RAID 5)
- B. 6 drives (2 mirrored and 4 in RAID 10)
- C. 6 drives (RAID 5)
- D. 2 drives (mirrored)

**Answer: A**

**Explanation:**

#### QUESTION NO: 7

---

Which third-party software components support LDAP for users, roles, and configurations?

- A. IBM Directory Server
- B. Microsoft Active Directory Server
- C. IBM DB2 8.1
- D. IBM DB2 8.2

**Answer: A**

**Explanation:**

#### QUESTION NO: 8

Which OS listed does hardware used for the Symantec Security Information Manager (SSIM) image support?

- A. SUSE
- B. Centos
- C. Redhat
- D. SE Linux

**Answer: C**

**Explanation:**

#### QUESTION NO: 9

Symantec Security Information Manager Series Appliance installs which operating system by default?

- A. Solaris
- B. Windows
- C. SUSE
- D. Red Hat

**Answer: D**

**Explanation:**

#### QUESTION NO: 10

Which database houses incidents and summary data?

- A. Oracle
- B. MySQL
- C. MSSQL
- D. IBM DB2

**Answer: C**

**Explanation:**

#### QUESTION NO: 11

Which component sends events to the Event Service for processing?

- A. the Symantec Security Information Manager (SSIM) collector
- B. the Symantec Security Information Manager (SSIM) on-box collector
- C. the Symantec Security Information Manager (SSIM) off-box collector
- D. the Symantec Security Information Manager (SSIM) agent

**Answer: D**

**Explanation:**

#### QUESTION NO: 12

What is the difference between Symantec Security Information Manager (SSIM) on-box and off-box collectors?

- A. Off-box collectors are installed on the SSIM products and on-box collectors are installed on the appliance.
- B. On-box collectors are installed prior to SSIM software installation and off-box collectors are installed separately.
- C. On-box collectors are automatically installed with the SSIM software and off-box collectors are installed separately.
- D. Off-box collectors are installed on the appliance and on-box collectors are installed on assets.

**Answer: C**

**Explanation:**

**QUESTION NO: 13**

Which Symantec Security Information Manager component retrieves security content in near-real-time from Symantec?

- A. LiveUpdate
- B. LiveUpdate and licensed DeepSight Integration Module simultaneously
- C. Licensed DeepSight Integration Module
- D. Security content retrieval is automatic.

**Answer: C**

**Explanation:**

**QUESTION NO: 14**

Which of the following are all on-box collectors?

- A. PIX, UNIX Syslog and Data Leakage Prevention
- B. Checkpoint, Snort and PIX
- C. PIX, Snort and Symantec Web Gateway
- D. Checkpoint, UNIX Syslog and Control Compliance Suite

**Answer: B**

**Explanation:**

**QUESTION NO: 15**

On which two operating systems can the Symantec Security Information Manager Agent be installed? (Select two.)

- A. Solaris 9
- B. Windows 2000
- C. Centos
- D. IBM AIX 5
- E. HP-UX 11

**Answer: A,B**

**Explanation:**

**QUESTION NO: 16**

Where do Symantec Security Information Manager collectors send events?

- A. Event Disposition
- B. Event Archive
- C. Event Reporting
- D. Event Logger

**Answer: D**

**Explanation:**

**QUESTION NO: 17**

What is Device-level aggregation?

- A. parsing data with data sensors
- B. grouping data to reduce traffic and database size
- C. forwarding event data to the appliance
- D. event and logcensoring

**Answer: B**

**Explanation:**

**QUESTION NO: 18**

What information must be obtained prior to product deployment and configuration of the Symantec Security Information Manager appliance?

- A. which on-box collectors are appropriate for installation
- B. the number of nodes found in the customer's infrastructure
- C. the number of security events per day the appliance will handle
- D. the air-conditioning and power requirements

**Answer: C**

**Explanation:**

**QUESTION NO: 19**

What information is necessary to properly size a deployment?

- A. hard drive space, events per second and geographic locations
- B. events per second, collector types and incident-to-event ratio
- C. hard drive space, incidents per second and collector types
- D. events per second, geographic locations and event-to-incident ratio

**Answer: D**

**Explanation:**

**QUESTION NO: 20**

What are the specified minimum hardware requirements for installing and running the Symantec Security Information Manager Console?

- A. 1 GB RAM and 1 GB disk space
- B. 1 GB RAM and 512 MB disk space
- C. 512 MB RAM and 1 GB disk space
- D. 512 MB RAM and 103 MB disk space

**Answer: D**

**Explanation:**

**QUESTION NO: 21**

Which LDAP port is used by the security directory?

- A. Port 22
- B. Port 389
- C. Port 443
- D. Port 636

**Answer: D**

**Explanation:**

**QUESTION NO: 22**



How is the Symantec Security Information Manager (SSIM) Console installed?

- A. On the SSIM DVD, go to Tools and install the client.
- B. Go to the SSIM web interface, download the client and click Run.
- C. From the SSIM appliance, deploy the console to your machine.
- D. No installation is necessary because SSIM is a browser-based tool.

**Answer: B**

**Explanation:**

#### QUESTION NO: 23

Where are the database options configured after installation?

- A. Symantec Security Information Manager Console --> Systems tab
- B. use the dbpurge command at the server console
- C. Symantec Security Information Manager --> Configure Appliance --> Purge tab
- D. Symantec Security Information Manager --> Settings--> Database Utilities tab

**Answer: D**

**Explanation:**

#### QUESTION NO: 24

Where is LiveUpdate for Symantec Security Information Manager (SSIM) configured?

- A. SSIM Start Page --> Maintenance--> LiveUpdate tab
- B. SSIM Console --> Systems tab --> LiveUpdate tab
- C. from a command prompt
- D. SSIM Client --> Maintenance tab --> LiveUpdate tab

**Answer: A**

**Explanation:**

#### QUESTION NO: 25

After setting up the Symantec Security Information Manager (SSIM) appliance, where are network settings changed?

- A. Command Prompt --> ifconfig
- B. SSIM Console --> Maintenance tab --> Network Settings
- C. SSIM Client --> Configuration tab --> Network Settings
- D. SSIM Start Page --> Settings--> Network Settings

**Answer: D**

**Explanation:**

#### **QUESTION NO: 26**

How do you install a valid DeepSight Integration License?

- A. Open the Symantec Security Information Manager Console; select Configure Appliance; click on DeepSight Integration Manager Configuration.
- B. Open Symantec Security Information Manager Console; select Configure Appliance; click on Licenses.
- C. On the appliance, place the license in the /opt/Symantec/license folder. D. Use the Install License Wizard.

**Answer: C**

**Explanation:**

#### **QUESTION NO: 27**

Which critical SSIM service status is displayed on the "status" console command when troubleshooting the installation of Symantec Security Information Manager (SSIM)?

- A. Information Manager
- B. DB2 database
- C. Tomcat servlet engine
- D. Apache web server

**Answer: B**

**Explanation:**

#### **QUESTION NO: 28**

Which console command would you use to determine the "status" of the HTTP server when troubleshooting the installation of Symantec Security Information Manager (SSIM)?