



**Vendor:** IBM

**Exam Code:** C1000-127

**Exam Name:** IBM Security Guardium v11.x Administrator

**Version:** DEMO

#### QUESTION 1

Which of the following best describes the quarterly updated tests feature of IBM Guardium's vulnerability assessment?

- A. It provides updates on the latest database encryption techniques
- B. It includes the newest compliance regulations and how to meet them
- C. It updates the test library with the latest vulnerabilities and remediation strategies
- D. It enhances the user interface for easier navigation and report generation

**Answer: C**

#### QUESTION 2

Viewing the enterprise load balancing load map in Guardium is useful for: (Select two)

- A. Identifying underutilized resources
- B. Tracking real-time data access patterns
- C. Understanding the distribution of monitoring load across appliances
- D. Assessing the geographical distribution of threats

**Answer: AC**

#### QUESTION 3

Runtime parameters enable which two IBM Guardium Query-Report capabilities?

- A. S-TAP limiting
- B. data mart creation
- C. attribute sort order
- D. drill-down capability
- E. specifying condition parameter values at report runtime

**Answer: DE**

#### QUESTION 4

Which of the following components are essential in the IBM Security Guardium architecture for data activity monitoring? (Select two)

- A. Central Manager
- B. Aggregator
- C. Collector
- D. Universal Connector

**Answer: BC**

#### QUESTION 5

Which of the following can you view in the results of a vulnerability assessment? (Select two)

- A. Encryption standards used in the database
- B. Database uptime and performance metrics
- C. Identified vulnerabilities and their severities

D. Suggested remediation activities for identified vulnerabilities

**Answer:** CD

**QUESTION 6**

On which IBM Guardium appliance is the monitoring policy installed?

- A. collector
- B. collection node
- C. central manager
- D. external S-TAP cluster

**Answer:** A

**QUESTION 7**

What is the difference between a scan job and a probe job in Database Auto-discovery?

- A. Scan job scans each specified host or hosts in a specified subnet and probe job uses the list of open ports compiled during the latest completed scan only.
- B. Scan job determines if database services are running on those ports and probe job uses the list of open ports compiled during the latest completed scan only.
- C. Scan job determines if database services are running on those ports and probe job compiles a list of open ports from the list of ports specified for that host.
- D. Scan job compiles a list of open ports from the list of ports specified for that host and probe job discovers sensitive data for targeted databases on the server.

**Answer:** A

**QUESTION 8**

If an S-TAP fails to start on Linux/Unix due to a buffer size error, you should:

- A. Decrease the database buffer size.
- B. Modify the S-TAP buffer size parameter to a lower value.
- C. Increase the size of the /tmp directory.
- D. Reinstall S-TAP without modifications.

**Answer:** B

**QUESTION 9**

What needs to occur in order for an audit workflow to send files to an external server without sending an email and without adding results to the to-do list?

- A. Define a dummy receiver.
- B. Define an audit process without receivers.
- C. Configure cli to allow audit external receivers.
- D. Configure a master user to audit the receivers results with accessmgr.

**Answer:** B

**QUESTION 10**

Which of the following are true about Guardium's support for cloud environments? (Select two)

- A. It can monitor database activity in real-time in cloud environments.
- B. It lacks support for private cloud deployments.
- C. It offers a virtual appliance option for cloud deployments.
- D. Cloud-based databases are excluded from vulnerability assessment capabilities.

**Answer:** AC

**QUESTION 11**

Which two capabilities does IBM Guardium provide?

- A. Endpoint monitoring of user's activities.
- B. Monitoring of malicious traffic on the network.
- C. Purpose-built tooling for ransomware protection.
- D. Heterogeneous support across databases, data warehouses, files, and big data.
- E. Single compliance reporting, analytics, and forensics solution for distributed and IBM System Z.

**Answer:** DE

**QUESTION 12**

How can the results of analytic engines in IBM Guardium be interpreted to enhance data security? (Select two)

- A. By identifying patterns of normal behavior to whitelist benign activities
- B. By detecting anomalies that could indicate potential data breaches
- C. By automatically patching detected vulnerabilities in the database
- D. By monitoring the uptime of the Guardium appliance

**Answer:** AB

**QUESTION 13**

Which feature is essential for achieving high availability load balancing for Guardium appliances?

- A. SNMP monitoring
- B. Centralized management
- C. Enterprise Load Balancer (ELB)
- D. Scheduled backups

**Answer:** C

## Thank You for Trying Our Product

### Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



**10% Discount Coupon Code: ASTR14**