

Exam : C1000-197

**Title : IBM Certified Guardium
Data Protection v12.x
Administrator - Professional**

Version : DEMO

1.Where should administrators first look when Guardium anomaly detection is not producing expected results?

- A. Baseline configuration settings on collectors
- B. Appliance firmware version history
- C. Report builder custom templates
- D. LDAP server connection logs

Answer: A

2.What two tasks should administrators schedule to maintain long-term appliance performance? (Choose two)

- A. Periodic log rotation and cleanup
- B. Manual shutdowns after each policy update
- C. Continuous disabling of anomaly detection
- D. Regular firmware and patch updates

Answer: AD

3.Which two steps must be taken to configure Guardium groups effectively for access and policy management? (Choose two)

- A. Assign members based on database roles or departments
- B. Create groups only on aggregators for scalability
- C. Define group-specific permissions and roles
- D. Restrict groups to a single appliance only

Answer: AC

4.Which two elements must be configured when defining a Guardium policy for monitoring sensitive queries? (Choose two)

- A. Policy rules with specific conditions
- B. Enforcement actions such as alert or block
- C. Appliance firmware upgrade schedules
- D. Database license type allocation

Answer: AB

5.Which factor is critical when planning integrations between Guardium and ticketing systems like ServiceNow?

- A. Ensuring that Guardium supports SNMP traps
- B. Confirming API compatibility for automated incident creation
- C. Assigning the ticketing system as a collector appliance
- D. Using Guardium's central manager to run ServiceNow scripts

Answer: B