Practice Exam Questions

IBM | Professional Certification

C1000-127

IBM Security Guardium Administrator

EXAMKILLER

Help Pass Your Exam At First Try

Total Question: 55 QAs

Question No: 1
A Guardium administrator is registering a new Collector to a Central Manager (CM). The registration failed. As part of the investigation, the administrator wants to identify if the firewall ports are open-How can the administrator do this?
A. Ask the company's network administrators.
B. Ask IBM technical support to login as root and verify.
C. Login as CLI and execute telnet <ip address> <port number>
D. Login as CLI and execute support show port open <ip address> <port number>
Answer: D

Question No: 2
A Guardium administrator manages an environment containing four standalone Collectors. The administrator has been asked to provide a weekly report showing all Data Manipulation Language (DML) SQL statements performed by all database administrators on all databases. The administrator does not want to run the report on each Collector.
What should the administrator do to simplify this task and run the report in only one place every week?
A. Replace the 4 Collectors with one Aggregator.
B. Create an Enterprise Report on one Collector combining the data.
C. Add a Guardium Aggregator to the environment. Create and run the report on the Aggregator.
D. install a Configuration Auditing System (CAS) on each Database Server. Configure the CAS Client to send data to a Collector. Create and run the report on the Collector.
Answer: C

Question No: 3
A Guardium administrator has an issue with Guardium. The administrator has not seen this particular issue before and needs to get it fixed. To get this resolved, what should the administrator do?
A. Log a PMR and request an answer from IBM Support.
B. Log a PMR so IBM Support can contact the customer. Then, while waiting, do a search of the Guardium Knowledge Center and Technotes for known issues and resolutions.
C. Request IBM Support to initiate a remote session and collect what they need to resolve the issue.
D. Search Guardium Knowledge Center and Technotes for known issues and resolutions. Then, if still needed, collect must_gather information and full problem details required for a new PMR so that IBM Support can review the Problem before contacting the customer.
Answer: D

Question No: 4
A Guardium policy has been configured with the following two rules:
A Guardium administrator is required to check for SQL statements from client IP 9.4.5.6 executed on object "TABLET. What domain(s) can the administrator create a report in to see the SQL?
A. Access
B. Policy Violations

C. Access and Access Policy
D. Access and Policy Violations
Answer: A

Question No: 5
A Guardium administrator needs to upgrade BUNDLE-STAP on a Linux server to the latest version using GIM. What parameter should the administrator set to ensure the upgrade will not require a reboot of the server?
A. KTAP_ENABLED=1
B. KTAP_NO_ROLLBACK=1
C. KTAP_LIVE_UPDATE=Y
D. KTAP_ALLOW_MODULE_COMBOS=Y
Answer: C

Question No: 6
A Guardium administrator must configure a policy to ignore all traffic from an application with a known client IP. Due to the high amount of traffic from this application, performance of the S-TAP and sniffer is a concern. What action should the administrator use in the rule?
A. Ignore Session
B. ignore S-TAP Session
C. ignore SQL per Session
D. ignore Responses per Session
Answer: B

Question No: 7
A Guardium administrator needs to configure EMC Centera for Archive and/or Backup.
In addition to the server IP address, what else is required to establish connection with an EMC Centera on the network?
A. ciipID
B. PEA file
C. Shared secret
D. Certificate signed request (CSR)
Answer: B

Question No: 8
After a successful purge, a Guardium administrator observes that the full percentage of the Guardium internal database is not decreasing. The administrator uses support show db-top-tables all and finds the size of the largest tables has decreased significantly.
What should the administrator do?
A. Increase the retention period and rerun the purge.
B. Rebuild the appliance and restore from the backup.
C. Login to CLI and execute stop inspection-core.
D. Optimize the internal TURBINEdatabase using diag CLI command.
Answer: D

Question No: 9
A Guardium administrator manages portal user synchronization by using a Central Manager.
When a change is made on the Central Manager such as, for example, adding a Guardium user to a Guardium group, how long should be allowed for the update to be synced with the managed units in a fully working environment?
A. 0minutes
B. 15 minutes
C. 30 minutes
D. 60 minutes
Answer: D

Question No: 10
A Guardium administrator must configure real time policy alerts to be sent to a remote SIEM for every SQL statement run on a sensitive object. There is no requirement for the data to be viewed or reported on in the Guardium appliance.
Which policy action would achieve that task and store the least amount of data in the Guardium internal database?
A. Log Only
B. Alert Only
C. Alert Daily
D. Alert Per Match
Answer: C

Question No: 11
While looking at the S-TAP Status report on a Collector, a Guardium administrator notices that the status of the S-TAPs is changing every few minutes. The administrator suspects that the sniffer is restarting every few minutes and that is why the status change is happening.
How can the Guardium administrator confirm if the sniffer is restarting every few minutes?
A. Review the Audit Process Log for 'Sniffer stopped' message.
B. Review the Aggregation/Archive Log for 'Sniffer is restarting message.
C. Review the Scheduled Jobs Exceptions for 'Sniffer process failed' message.
D. Review the Buff Usage Monitor for the column TID to see if it changed every few minutes.
Answer: D

Question No: 12
During a Guardium deployment planning meeting, the team decides to deploy all S-TAP agents on all Unix/Linux database systems. A Unix/Linux system administrator team manager asks a Guardium administrator if there are any differences between Guardium S-TAPs for AIX and Linux systems that the team should be aware of.
What should be the Guardium administrator's response?
A. A-TAP is required on all AIX DB Servers.
B. a server reboot is required to capture shared memory traffic from all databases on AIX.
C. K-TAP is required on the AIX DB servers. The exact uname -a output is required to determine the correct K-TAP module for the server.

D. K-TAP is required on the Linux DB servers. The exact uname -a output is required to determine the correct K-TAP module for the server.
Answer: B

Question No: 13
A company has recently acquired Guardium software entitlement to help meet their upcoming PCI-DSS audit requirements. The company is entitled to Standard Guardium DAM offering.
Which of the following features can the Guardium administrator use with the current entitlement? (Select two.)
A. Run Vulnerability Assessment reports
B. Generate audit reports using PCI-DSS Accelerator
C. Block and quarantine an unauthorized database connection
D. Mask sensitive PCI-DSS information from web application interface
E. Log and alert all database activities that access PCI-DSS Sensitive Objects.
Answer: A,B

Question No: 14
The guard_tap.ini of a UNIX S-TAP is configured with the following parameters:
firewall_installed=1
firewall_fail_close=1
firewall_default_state=1
firewall_timeout=10
The collector that this S-TAP is sending data to has become unavailable and there is no failover option configured. A Guardium administrator must communicate the impact of this outage to users of the monitored database.
What should the administrator advise is the expected behavior for a database session?
A. The session will not experience any latency or termination.
B. No SQL can be executed and after 10 seconds the session will be terminated.
C. in the first 10 seconds of the session SQL can be executed, then the session is terminated.
D. in the first 10 seconds of the session no SQL can be executed, then the session will work as normal.
Answer: C

Question No: 15
The Quick Search window does not show up on the GUI of a standalone Collector What technical feature should the Guardium administrator check first?
A. That the Collector has at least 24 GB.
B. That the Collector has at least 32 GB.
C. That the Collector has at least 64 GB.
D. Check the contract and verify whether that feature was purchased.
Answer: A

Question No: 16
An administrator manages a Guardium environment including 4 Collectors exporting data to an Aggregator. The Collectors export their data daily at 2, 3, 4 and 5 am Eastern Standard Time (EST) respectively. The Collectors receive traffic every day. The logs on all the Collectors confirm data is exported daily without errors,