IBM

Exam Questions C2150-606

IBM Security Guardium V10.0 Administration

NEW QUESTION 1
AGuardium 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

NEW QUESTION 2
Which use cases are covered with the File Activity Monitoring feature? (Select two.)

A. Classify sensitive files on mainframe systems.
B. Encrypts database data files on file systems based on policies.
C. Selectively redacts sensitive data patterns in files based on policies.
D. Provides audit trail of access to files, alert and/or block when unauthorized users or processes attempt access.
E. Identifies files containing Personally Identifiable Information (Pll) or proprietary confidential information on Linux Unix Windows (LUW) systems.

Answer: AE

NEW QUESTION 3
During the initial phase of the Guardium deployment, the Guardium administrator wants to figure out an ideal time period to purge data from the appliance based on the data load.
Which predefined Guardium report(s) allows the administrator to determine the current database disk usage of the Guardium Appliance?

A. Disk UtiI report
B. Aggregation/Archive log
C. DB Server throughput report
D. Buff Usage Monitor and System Monitor reports

Answer: D

NEW QUESTION 4
A Guardium administrator needs to check the traceroute information between one appliance and its Central Manager. Which CLI command should the administrator run?

A. iptraf
B. support show iptables
C. show network routes operational
D. support must_gather network_issues

Answer: D

NEW QUESTION 5
During a Guardium deployment planning meeting, a database administrator indicated that the mission critical databases were clustered. How should the Guardium administrator handle S-TAP installation and configuration with respect to clustered databases?

A. Install S-TAP agents on all active node
B. Set ALL_CAN_CONTROL=l to failover the S-TAP process to the passive nodes when a database failover occurs.
C. install S-TAP agents on all active nodes Set WAIT_FOR_DB_EXEC=-l to set the agent process to failover to the passive node when a database failover occurs.
D. Install S-TAP agents on all active and passive node
E. Set ALL_CAN_CONTROL=0 to disable all passive nodes until a database failover occurs.
F. Install S-TAP agents on all active and passive nodes: Set WAIT_FOR_DB_EXEC>0 on all nodes to start S-TAP processes without waiting for a correct DB home.

Answer: A

NEW QUESTION 6
A Guardium administrator is setting up a Collector schedule to export data to an Aggregator and Archive its data to an Archive storage unit for additional data safety.
Given this scenario, which is true regarding the purge schedule?

A. The Archive and the Export have independent purge schedules but should not be run at the same time.
B. The Guardium unit would run the Export and Archive before any purge, so you would only see the last purge run each day.
C. it would not be possible to configure both on a Collector, the Aggregator should do the archiving and only export from the Collector.
D. Any time that Data Export and Data Archive are both configured, the purge age must be greater than both the age at which to export and the age at which to archive.

Answer: D

NEW QUESTION 7
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 custome
C. Then, while waiting, do a search of the Guardium Knowledge Center and Technotes for known issues and resolutions.
D. Request IBM Support to initiate a remote session and collect what they need to resolve the issue.
E. Search Guardium Knowledge Center and Technotes for known issues and resolution
F. 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

NEW QUESTION 8
Simple Mail Transfer Protocol (SMTP) has recently been configured on a Guardium appliance. How can the administrator confirm the configuration is correct? (Select 2)

A. Restart the Anomaly detection process
B. Send a test email with CLI diag command
C. From the GUI Alerter page, test the SMTP connection
D. Create a query in access domain to see the sent messages
E. Obtain the syslog file from fileserver and check for SMTP messages

Answer: BC

NEW QUESTION 9
AGuardium 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

NEW QUESTION 10
Auditors request a report of all unsuccessful login attempts to a database monitored by Guardium. How should a Guardium administrator create such a report?

A. Add a failed login rule to the policy.
B. Create a failed login query and report using access domain in Guardium.
C. Create a failed login query and report using exceptions domain in Guardium.
D. Create a failed login query and report using application data domain in Guardium.

Answer: C

NEW QUESTION 10
An administrator has a new standalone Guardium appliance that will be placed into production next week. The appliance will monitor traffic from a number of databases with a high volume of traffic. The administrator needs to configure the schedule to ensure the appliance internal database does not get full with incoming data.
Which data management function does the administrator need to configure?

A. Purge
B. Data Export
C. Data Restore
D. System Backup

Answer: A

NEW QUESTION 13
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

C2150-606 Practice Exam Features:

* C2150-606 Questions and Answers Updated Frequently

* C2150-606 Practice Questions Verified by Expert Senior Certified Staff

* C2150-606 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* C2150-606 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year