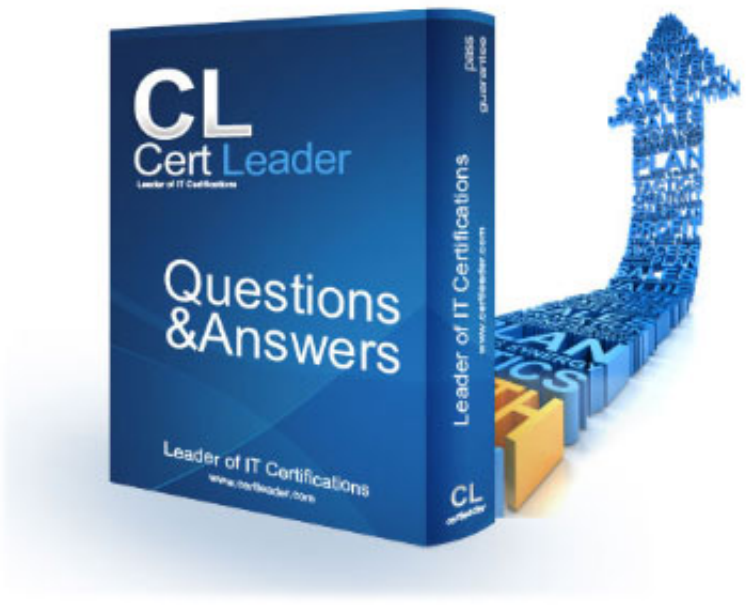
C2150-606 Dumps

IBM Security Guardium V10.0 Administration

https://www.certleader.com/C2150-606-dumps.html



NEW QUESTION 1
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: AB

NEW QUESTION 2
In a centrally managed environment, while executing the report 'Enterprise Buffer Usage Monitor', a Guardium administrator gets an empty report. Why is the report empty?

A. Sniffers are not running on the Collectors.
B. The report is not executed with a remote source on the Collector.
C. The report is not executed with a remote source on the Aggregator.
D. Correct custom table upload is not scheduled on the Central Manager.

Answer: C

NEW QUESTION 3
A Guardium administrator needs to monitor an Oracle database on a production database server.
Which component does the administrator need to install on this database server that will monitor the traffic?

A. S-TAP
B. Guardium Collector
C. Guardium Installation Manager (GIM)
D. Configuration Auditing System (CAS)

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
A company wants to deploy S-TAPs for 2 groups of database servers located in 2 different data centers. The current set of Collectors are fully utilized. The Aggregators and Central Manager can handle more load.
What should a Guardium administrator recommend?

A. Deploy 2 new Collectors, l in each data center.
B. Connect S-TAPs directly to Aggregators to avoid network latency.
C. Connect S-TAPs directly to the Central Manager to avoid network latency.
D. Deploy 2 new Collectors in the third data center located in between the 2 data centers.

Answer: A

NEW QUESTION 6
A Guardium administrator needs to use CLI commands to maintain the internal database, clean static orphans, produce static system reports and to monitor live network traffic filtered by IP addresses and port numbers.
Which combination of commands should the administrator use for these tasks?

A. diag and iptraf
B. diag and trace_route
C. jptraf and support must_gather
D. support must_gather and show network verify

Answer: C

NEW QUESTION 7
A Guardium administrator is preparing a command to install Configuration Auditing System (CAS) on a Linux server using the command line method. Which parameter is required?

A. dir

B. tapip
C. java-home
D. sqlguardip

Answer: D

NEW QUESTION 8
A Guardium administrator observes certain changes to the configuration and policies. How would the administrator identify the changes that were made and who made them?

A. Review the Audit Process Log report.
B. Review the sniffer buffer usage report.
C. Review the /var/log/messages log file.
D. Review the results of 'Detailed Guardium User Activity' report.

Answer: D

NEW QUESTION 9
AGuardium administrator is checking the scheduled jobs exceptions report on a standalone Collector The following error is repeating every l5 minutes.
java.lang.NumberFormatException: empty String
The administrator also notices that the anomaly detection polling interval is l5 minutes. What should the administrator do next to contribute troubleshooting the problem?

A. Pause all scheduled jobs and check if the exception comes back.
B. identify the alert that is causing the problem by deactivating one alert at a time.
C. Check in the alert builder to see which alerts have accumulation interval of l5 minutes.
D. in the CLI run support must_gather aggjssues and send the file to IBM support.

Answer: B

NEW QUESTION 10
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
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 server
D. The exact uname -a output is required to determine the correct K-TAP module for the server.
E. K-TAP is required on the Linux DB server
F. The exact uname -a output is required to determine the correct K-TAP module for the server.

Answer: B

NEW QUESTION 14
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 18
A Guardium administrator is using the Classification, Entitlement and Vulnerability assessment features of the product. Which of the following are correct with regards to these features? (Select two.)

A. Vulnerability Assessment reports are populated to the Guardium appliance via S-TAP.
B. Classification for databases and files use the same mechanisms and patterns to search for sensitive data.
C. Entitlement reports are predefined database privilege reports and are populated to the Guardium appliance via S-TAP.
D. Vulnerability Assessment identifies and helps correct security vulnerabilities and threats in the database infrastructures.
E. The classification feature discovers sensitive assets including credit card numbers or national card numbers from various data sources.

Answer: DE

NEW QUESTION 21
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 TURBINE database using diag CLI command.

Answer: D

NEW QUESTION 25
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your C2150-606 Exam with Our Prep Materials Via below:

https://www.certleader.com/C2150-606-dumps.html