C2150-606 Q&As

IBM Security Guardium V10.0 Administration

Pass IBM C2150-606 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/c2150-606.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

QUESTION 1

A Guardium administrator handles a large environment and has been asked to restore old data for auditors to review. This old data needs to be restored so that it does not impact the current data being collected or any merge settings. In order to keep the reports separate (old datavs current data), the administrator sets up an Investigation Center.

Which is a key requirement for users of the Investigation Center?

A. The user must be in one of the groups INV_1, INV_2, or INV_3 (case-sensitive).

B. The users must login as one of the predefined user accounts INV_1, INV_2, orINV_3 (case-sensitive).

C. A separate user must be used with a role of either INV_1, INV_2, or INV_3 (case- sensitive).

D. To correctly configure an investigation user, the user\\'s Last Name must be set to the name of one of the three investigation databases, INV_1, INV_2, or INV_3 (case-sensitive).

Correct Answer: D

QUESTION 2

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, 1 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.

Correct Answer: A

QUESTION 3

A Guardium administrator noticed that while the data activity monitoring is working fine, the Guardium appliance is slower than usual. The administrator wants to check the current CPU load of the Guardium appliance.

Which predefined Guardium report(s) allows the administrator to determine the current system CPU load of the Guardium Appliance?

A. CPU Util report

B. CPU Tracker report

C. Unit summary and CPU Util report

D. Buff Usage Monitor and System monitor report

Correct Answer: D

QUESTION 4

A Guardium administrator needs to build new appliances with the latest version of Guardium. How should the administrator obtain the ISO image?

A. Contact IBM Support.

B. Download fromibm.com

C. Download from IBM Fix Central.

D. Download from IBM Passport Advantage.

Correct Answer: D

QUESTION 5

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

Correct Answer: D

QUESTION 6

An administrator just installed the Guardium product using the Guardium ISO image. Which step must the administrator perform as part of the initial set-up of the new appliance?

A. Generate the GUI certificate request.

B. Configure network settings on the appliance.

C. Restart the sniffer process from the CLI command prompt.

D. Obtain the passwords for the databases to be monitored by the appliance.

Correct Answer: B

QUESTION 7

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 (PII) or proprietary confidential information on Linux Unix Windows (LUW) systems.

Correct Answer: AE

QUESTION 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.

Correct Answer: D

QUESTION 9

Which port must be open for encrypted communication between UNIX S-TAP and Collector?

A. 9500

B. 16016

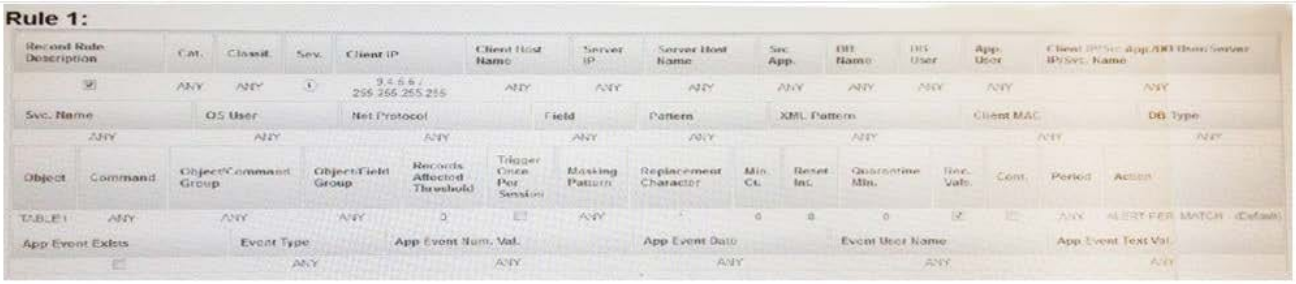
C. 16017

D. 16018

Correct Answer: D

QUESTION 10

A Guardium policy has been configured with the following two rules:



AGuardium 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

Correct Answer: A