Vendor:IBM

Exam Code:C2150-606

Exam Name:IBM Security Guardium V10.0
Administration

Version: Demo

QUESTION 1

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.

Correct Answer: D

QUESTION 2

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. aserver 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.

Correct Answer: B

QUESTION 3

A Guardium administrator is planning to build an environment that contains an S-TAP with one primary Collector and one failover Collector. What must the administrator ensure when setting up this environment?

A. Both Collectors are centrally managed.

B. There is network connectivity between the S-TAP and both Collectors.

C. Guardium Installation Manager (GIM) is installed on the Database Server.

D. in the guard_tap.ini file of the S-TAP set participate_in_load_balancing=1

Correct Answer: B

QUESTION 4

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 5

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

D. Login as CLI and execute support show port open

Correct Answer: D

QUESTION 6

A Guardium administrator needs to use both CLI and GrdAPI functions to manage the system.

Which are the two commands that the administrator can use to search for the required commands and their syntax from within either CLI or GrdAPI?

A. CLI: commands GrdApi: grdapi --help

B. CLI: help GrdApi: grdapi --help

C. CLI: commands GrdAPI: grdapi command

D. CLI: -help GrdApi: grdapi -help=true

Correct Answer: D

QUESTION 7

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

Correct Answer: BC

QUESTION 8

AGuardium environment is set up to send daily reports to users. The users are complaining that their report has not been delivered to their inbox for the past week. What is the first action the Guardium administrator should take in order to diagnose the problem?

A. Open a ticket with IBM Support.

B. Pause the User Portal Sync process.

C. Check in the Aggregation/Archive log.

D. Check in the Scheduled Job Exceptions.

Correct Answer: D

QUESTION 9

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

Correct Answer: A

QUESTION 10

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.

Correct Answer: A

QUESTION 11

AGuardium administrator just finished installing the Guardium product to build a Collector. The administrator wants to make sure the Collector has the licenses needed to provide functionality for data activity monitoring, masking and blocking (terminate).

Which of the following lists the minimum licenses the administrator needs to install?

A. Base Collector license.

B. None, the licenses required are already installed automatically by the Guardium product installer.

C. Base Collector license plus IBM Security Guardium Standard Activity Monitor for Databases (DAM Standard).

D. Base Collector license plus IBM Security Guardium Advanced Activity Monitor for Databases (DAM Advanced).

Correct Answer: D

QUESTION 12

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)

Correct Answer: D