IBM

Exam C2150-606

IBM Security Guardium V10.0 Administration

Version: 6.0

[Total Questions: 55]

Question No : 1

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).

Answer: D

Question No : 2

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

Answer: B

Question No : 3

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.

Answer: B

Question No : 4

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 : 5

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

Answer: D

Question No : 6

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

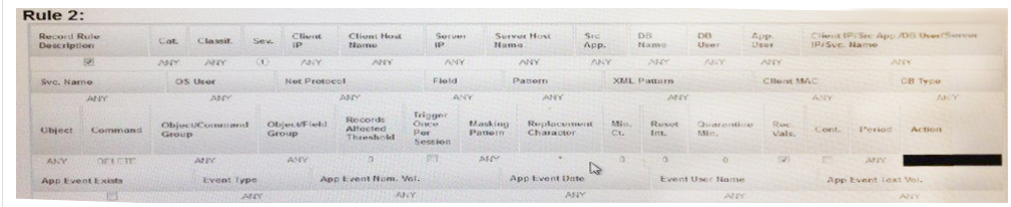
Answer: D

Question No : 7

The quard_tap.ini of a UNIX S-TAP is configured with the following parameters:

```
firewall_installed=1
firewall_fail_close=0
firewall_default_state=0
firewall_timeout=10
```

A Guardium administrator applies a policy to the Collector with two rules as below. The actions of the rules have been hidden.



The administrator must create a policy that will terminate the session on the delete statement in the below scenario:

A session is started to the monitored database from client IP 9.9.8.7. In the session the user plans to perform a select statement and then a delete statement.