DUMPSARENA

IBM Security Guardium V10.0 Administration

IBM C2150-606

Version Demo

Total Demo Questions: 9

Total Premium Questions: 56

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

QUESTION NO: 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: A B

Explanation:

B: Guardium comes with out of the box compliance regulation accelerators.

Incorrect:

Not C, Not D: DAM Advanced is DAM Standard functionality plus fine-grained access control, masking, quarantine, and blocking (activity terminate).

Note: Payment Card Industry (PCI) Data Security Standard (DSS) is a set of technical and operational requirements designed to protect cardholder data and applies to all organizations who store, process, use, or transmit cardholder data.

Review the following information to determine which license key must be added. This will depend on what features of the product have been purchased.



Reference: http://www-01.ibm.com/support/knowledgecenter/SSMPHH_10.0.0/com.ibm.guardium.doc.install/install/licenses.html

QUESTION NO: 2

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: B C

Explanation:

B: Use this command to send a test email using the configured SMTP server.

1. Select Test Email from the Interactive Queries menu.

2. You are prompted to select a recipient. Select Custom and press Enter.

3. You are prompted to supply an email address. Type an email address and press Enter. You will be informed of the output of the operation.

C: Note that on the Administration Console, the Test Connection link in the SMTP pane of the Alerter configuration panel only tests that an SMTP port is configured, not that mail can actually be delivered via that server. You can use this command to test email delivery without having to configure and trigger a statistical or real-time alert, or an audit process notification.

Reference: https://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.guardium91.doc/appendices/topics/diag_cli_command.html

QUESTION NO: 3

A Guardium administrator needs to install and configure a physical appliance to ensure network redundancy.

Which port should the administrator use to configure IP teaming (bonding)?

A. eth1 only

B. eth2 only

C. eth3 only

D. any port

ANSWER: D

Explanation:

Bonding or teaming turns eth0 and another specified network interface card (NIC) into a bonded pair with standby failover.

Reference: http://www-01.ibm.com/support/knowledgecenter/SSWL9Z_10.0.0/com.ibm.guardium.appmask.doc/config/system_configuration.html

QUESTION NO: 4

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.

ANSWER: A E

Explanation:

A: Use case example:

Critical application files can be accessed, modified, or even destroyed through back-end access to the application or database server

Solution: File Activity Monitoring can discover and monitor your configuration files, log files, source code, and many other critical application files and alert or block when unauthorized users or processes attempt access.

E: Use case example:

Need to protect files containing Personally Identifiable Information (PII) or proprietary information while not impacting day-to-day business.

Solution: File Activity Monitoring can discover and monitor access to your sensitive documents stored on many file systems. It will aggregate the data, give you a view into the activity, alert you in case of suspicious access, and allow you to block access to select files and folders and from select users.

Note: File activity monitoring consists of the following capabilities:

* Discovery to inventory files and metadata.

* Classification to crawl through the files to look for potentially sensitive data, such as credit card information or personally identifiable information.

* Monitoring, which can be used without discovery and classification, to monitor access to files and, based on policy rules, audit and alert on inappropriate access, or even block access to the files to prevent data leakage.

Reference: https://www-01.ibm.com/support/knowledgecenter/SSMPHH_10.0.0/com.ibm.guardium.doc/protect/fam_intro.html

QUESTION NO: 5

A Guardium 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

Explanation:

You can ignore capturing the activity of some specific processes by defining INGNORE S-TAP SESSION policy.

Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21497163

QUESTION NO: 6

A Guardium 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

ANSWER: D

Explanation:

The support show port open command is similar to using telnet to detect an open TCP port locally or on a remote host.

If we are able to connect successfully you will see a message like: Connection to 127.0.0.1 8443 port [tcp/*] succeeded!

If you are unable to connect you will see a message like: connect to 127.0.0.1 port 1 (tcp) failed: Connection refused

Syntax: support show port open

IP port - IP must be a valid IPv4 address like 127.0.0.1. Port must be an integer with a value in 1-65535.

Reference: https://www-01.ibm.com/support/knowledgecenter/SSMPHH_10.0.0/com.ibm.guardium.doc.reference/cli_api/support_cli_commands.html

QUESTION NO: 7

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: D E

Explanation:

D: Guardium Vulnerability Assessment enables you to identify and correct security vulnerabilities in your database infrastructure.

E: As the size and organization of the corporate database grows, sensitive information like credit card numbers and transactions, or personal financial data, may be present in multiple locations, without the knowledge of the current owners of that data. This frequently happens in corporations that have experienced mergers and acquisitions and in older corporations where legacy systems have outlasted their original owners. Even in the best of cases, integration and enhancement projects between disparate systems can easily leave sensitive data unknown and unprotected.

Guardium provides the Classification feature to discover and classify sensitive data, so that you can make and enforce effective access policy decisions.

Incorrect:

Not A: The Guardium S-TAP is a lightweight software agent installed on a database server system. The S-TAP monitors database traffic and forwards information about that traffic to a Guardium system. Guardium S-TAP includes support for:

Capture of all database activities on DB2 for z/OS by privileged users, mainframe-resident applications, and network clients

Capture of critical operations such as SELECTs, DML, DDL, GRANTS, and REVOKES

Not C: Use Guardium's predefined database entitlement (privilege) reports) to see who has system privileges and who has granted these privileges to other users and roles. Database entitlement reports are important for auditors tracking changes to database access and to ensure that security holes do not exist from lingering accounts or ill-granted privileges.

Reference: http://www-01.ibm.com/support/knowledgecenter/SSMPHH_10.0.0/com.ibm.guardium.doc/assess/va_intro.html?lang=en

Reference: https://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.guardium91.doc/discover/topics/classification.html

QUESTION NO: 8

A Guardium administrator needs to upgrade BUNDLE-STAP on a Linux server to the latest version using GIM.

What parameter should the administrator set to ensure the upgrade will not require a reboot of the server?

A. KTAP_ENABLED=1

B. KTAP_NO_ROLLBACK=1

C. KTAP_LIVE_UPDATE=Y

D. KTAP_ALLOW_MODULE_COMBOS=Y

ANSWER: C

Explanation:

If specifying KTAP_LIVE_UPDATE=Y, no reboot is required.

Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21644770

QUESTION NO: 9

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

Explanation:

Configuration Auditing System Overview

Databases can be affected by changes to the server environment; for example, by changing configuration files, environment or registry variables, or other database or operating system components, including executable files or scripts used by the database management system or the operating system. CAS tracks such changes and reports on them. The data is available on the Guardium system and can be used for reports and alerts.

Reference: https://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.guardium91.doc/assess_harden/topics/cas.html