DUMPSARENA

IBM Security Guardium V10.0 Administration

IBM C2150-606

Version Demo

Total Demo Questions: 9

Total Premium Questions: 55

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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 from ibm.com

C. Download from IBM Fix Central.

D. Download from IBM Passport Advantage.

ANSWER: D

Explanation:

On Passport Advantage (PA) you will find Guardium Product Image - ISO file, Licences, Product Keys, Manuals, etc. You may only download products that your are entitled.

Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21675411

QUESTION NO: 2

An infrastructure manager is presented with a few new servers that are available to deploy as a Guardium Collector appliance as part of Guardium project expansion. The Guardium administrator is asked which server option is best for a Guardium Collector.

Which server option can the Guardium administrator use for the new Collector?

A. ia64 Intel Processor with quad-core CPU, 32GB memory, 4 NICs, 2TB disk

B. x86_64 Intel Processor with 8-core CPU, 32GB memory, 2 NICs, 1 TB disk

C. x86_64 Intel Processor with dual-core CPU, 24GB memory, and 2 NICs, and 200GB disk

D. linuxppc64 Power Processor with 8-core CPU, 24GB memory, and 4 NICs, and 4TB disk

ANSWER: B

Explanation:

The IBM Guardium solution works only on x86 Intel-based or AMD-based platforms (for example, x86_64). A minimum of 4 cores is also required.

Reference: http://www-01.ibm.com/support/docview.wss?uid=swg27046184

QUESTION NO: 3

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 data vs 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, or INV_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).

ANSWER: D

Explanation:

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).

When creating an investigation user, it is suggested that the user's name correspond or have some representation that denotes which investigation database that will be used. For instance, if a user will be using the INV_1 database, the user's name could be "john1" or "inv1" .

Reference: http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.5.0/com.ibm.guardium91.doc/aggregation_cm/topics/investigation_center.html

QUESTION NO: 4

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

A. 9500

B. 16016

C. 16017

D. 16018

ANSWER: D

Explanation:

The ports for CAS pertain to Change Audit System. If CAS is installed, those ports must be opened as well. Please enable the ports as listed in the table below, depending on whether you want the traffic between the STAP and the collector to be encrypted or not.

16016: Clear Unix S-TAP (including IBM i S-TAP running in PASE)

16017: Clear Unix CAS

16018: Encrypted Unix S-TAP (optional)

16019: Encrypted Unix CAS (optional)

Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21569674

QUESTION NO: 5

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: 6

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: 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

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: 8

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:

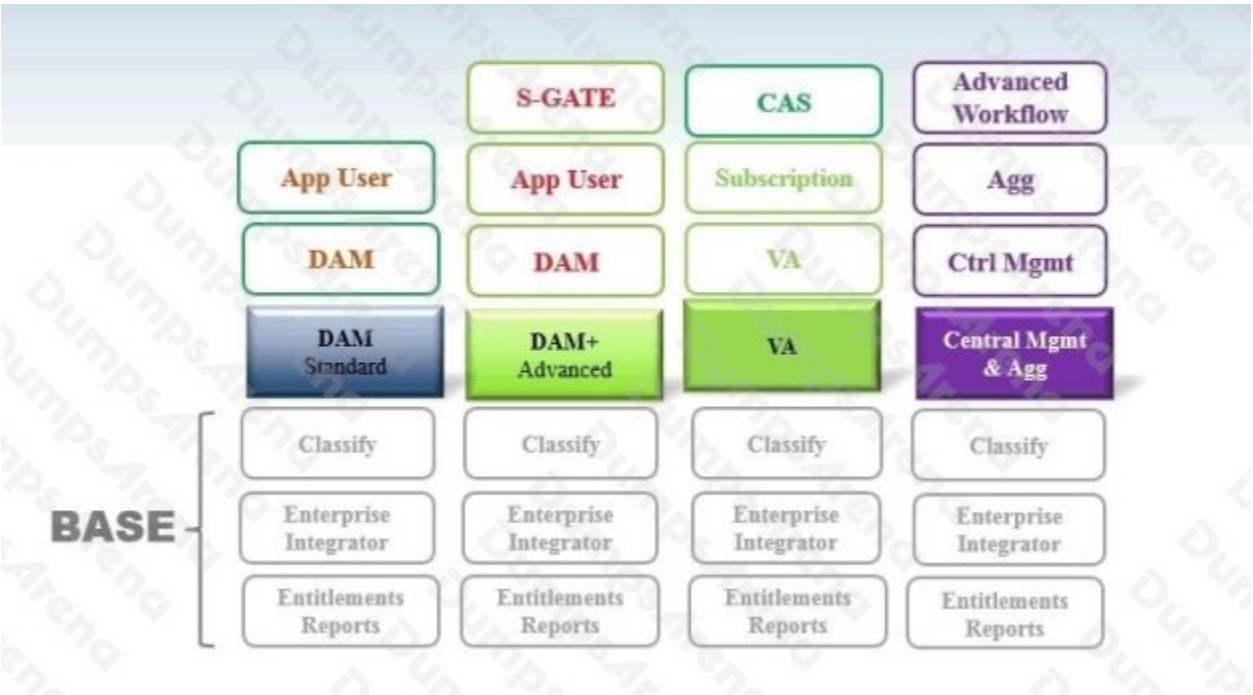
B: Guardium comes with out of the box compliance regulation accelerators.

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: 9

A Guardium 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.

ANSWER: D

Explanation:

The Scheduled Job Exceptions displays a timestamp and the description for each scheduled job exception (including assessment errors).

Reference: http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.0.0/com.ibm.guardium.using.doc/dita-appendices_help1_book/topics/predefined_admin_reports.html