Vendor: IBM

Exam Code: C2150-606

Exam Name: IBM Security Guardium V10.0 Administration

Version: DEMO

QUESTION 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 2
An administrator manages a Guardium environment including 4 Collectors exporting data to an Aggregator. The Collectors export their data daily at 2, 3, 4 and 5 am Eastern Standard Time (EST) respectively. The Collectors receive traffic every day. The logs on all the Collectors confirm data is exported daily without errors, and all the exported files always have data. A Session report is run on the Aggregator at noon EST for data from the last day.

Which of the following will ensure there is data in the report?

A. Schedule Data Purge on the Aggregator to run every day after 5 am EST.
B. Schedule Data Import on the Aggregator to run at any time of the day.
C. Schedule Data Import in the Aggregator to run every day before 2 am EST.
D. Schedule Data Import on the Aggregator to run every day at 6 am EST or later.

Answer: C

QUESTION 3
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: BC
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 4
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: DE
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 5
A Guardium administrator must configure real time policy alerts to be sent to a remote SIEM for

every SQL statement run on a sensitive object. There is no requirement for the data to be viewed or reported on in the Guardium appliance.

Which policy action would achieve that task and store the least amount of data in the Guardium internal database?

A. Log Only
B. Alert Only
C. Alert Daily
D. Alert Per Match

Answer: C
Explanation:
Guardium Version 9 introduced a new policy rule action - ALERT ONLY.
This rule action will populate only the message tables and constructs. It will no longer populate Policy Violations tables. With this policy rule action logging Policy Violations in IBM InfoSphere Guardium can be avoided.
Alert Only - action that will write to message and message_text tables. This action permits all policy violation notifications to be sent to a remote destination. Designed to improve Guardium integration with other database security solutions.
Incorrect:
Not C: Alert Daily sends notifications only the first time the rule is matched each day.
Reference: https://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.5.0/com.ibm.guardium95.doc/protect/topics/rule_actions.html

QUESTION 6
A Guardium 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
Explanation:
Data Activity Monitor and Audit - Advanced: All capabilities in Data Activity Monitor Audit - Standard, plus the ability to:
* Block data traffic according to policy (data-level access control)
* Mask unauthorized extraction of sensitive data
Etc.
Reference: http://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/3/897/ENUS215-173/index.html&lang=en&request_locale=en

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**