C2150-606$^{Q\&As}$

IBM Security Guardium V10.0 Administration

Pass IBM C2150-606 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/c2150-606.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

QUESTION 1

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. ja64 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. Iinuxppc64 Power Processor with 8-core CPU, 24GB memory, and 4 NICs, and 4TB disk

Correct Answer: B

QUESTION 2

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 datavs 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, orINV_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).

Correct Answer: D

QUESTION 3

A Guardium administrator needs to monitor changes to the Oracle configuration file on a production Oracle database server. Assuming all valid licenses are applied, which Guardium component does the administrator need to install and where?

A. Guardium Installation Manager (GIM) on the Database Server

B. Configuration Auditing System (CAS) on the Database Server.

C. Configuration Auditing System (CAS) on the Guardium Collector.

D. Configuration Auditing System (CAS) on the Database Server and on the Guardium Collector.

Correct Answer: D

QUESTION 4

AGuardium 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.

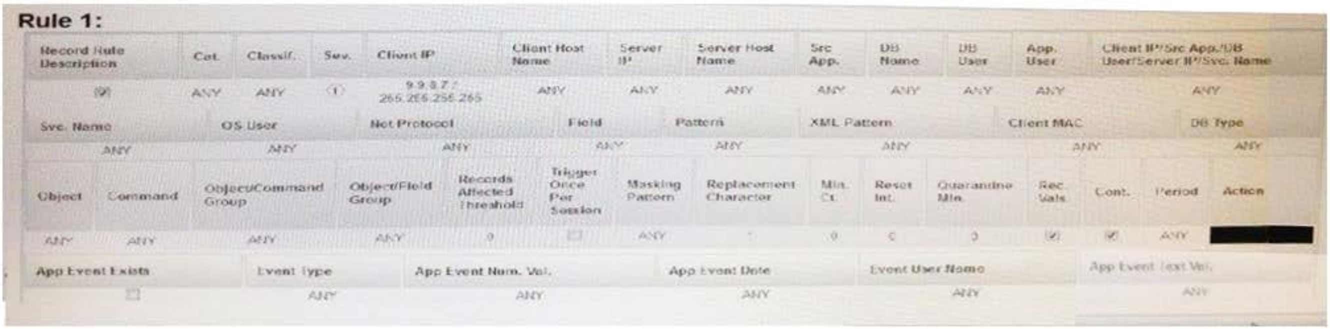
Correct Answer: DE

QUESTION 5

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.



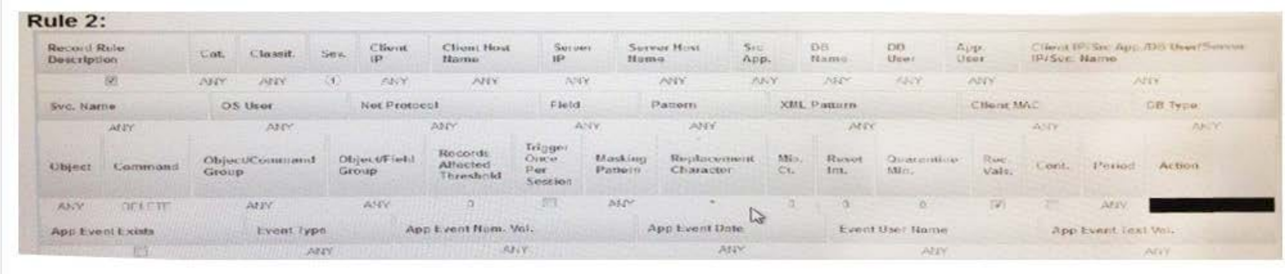
Rule 1:

Record Rule Description	Cat.	Classif.	Sev.	Client IP	Client Host Name	Server IP	Server Host Name	Src App.	DB Name	DB User	App. User	Client IP/Src App./DB User/Server IP/Svc. Name
☑	ANY	ANY	1	9.9.8.7 / 255.255.255.255	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY

Svc. Name	OS User	Net Protocol	Field	Pattern	XML Pattern	Client MAC	DB Type
ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY

Object	Command	Object/Command Group	Object/Field Group	Records Affected Threshold	Trigger Once Per Session	Masking Pattern	Replacement Character	Min. Ct.	Reset Int.	Quarantine Min.	Rec Vals	Cont.	Period	Action
ANY	ANY	ANY	ANY	0	☐	ANY	*	0	0	0	☑	☑	ANY	[redacted]

App Event Exists	Event Type	App Event Num. Val.	App Event Date	Event User Name	App Event Text Val.
☐	ANY	ANY	ANY	ANY	ANY



Rule 2:

Record Rule Description	Cat.	Classif.	Sev.	Client IP	Client Host Name	Server IP	Server Host Name	Src App.	DB Name	DB User	App. User	Client IP/Src App./DB User/Server IP/Svc. Name
☑	ANY	ANY	1	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY

Svc. Name	OS User	Net Protocol	Field	Pattern	XML Pattern	Client MAC	DB Type
ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY

Object	Command	Object/Command Group	Object/Field Group	Records Affected Threshold	Trigger Once Per Session	Masking Pattern	Replacement Character	Min. Ct.	Reset Int.	Quarantine Min.	Rec Vals.	Cont.	Period	Action
ANY	DELETE	ANY	ANY	0	☐	ANY	*	0	0	0	☑	☐	ANY	[redacted]

App Event Exists	Event Type	App Event Num. Val.	App Event Date	Event User Name	App Event Text Val.
☐	ANY	ANY	ANY	ANY	ANY

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.

What actions should the administrator configure?

A. Rule 1 - S-GATE Attach Rule2 - S-GATE Detach

B. Rule 1 - S-GATE Detach Rule 2 - S-GATE Terminate

C. Rule 1 - S-GATE Attach Rule 2 - S-GATE Terminate

D. Rule1 - S-TAP Terminate Rule 2 - S-GATE Terminate

Correct Answer: A

QUESTION 6

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 7

A Guardium administrator is creating a policy to alert on actions by users that are stored on an LDAP server. How can the administrator populate a group to use in the policy?

A. Schedule the LDAP user import into the group.

B. Schedule the LDAP user import from accessmgr and run portal user sync.

C. Schedule the LDAP user import from accessmgr and populate the group from a query.

D. Populate the group from a query in access domain with a condition on the LDAP server as the Server IP.

Correct Answer: C

QUESTION 8

A Guardium administrator needs to configure EMC Centera for Archive and/or Backup.

In addition to the server IP address, what else is required to establish connection with an EMC Centera on the network?

A. ciipID

B. PEA file

C. Shared secret

D. Certificate signed request (CSR)

Correct Answer: B

QUESTION 9

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 10

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.

Correct Answer: AB