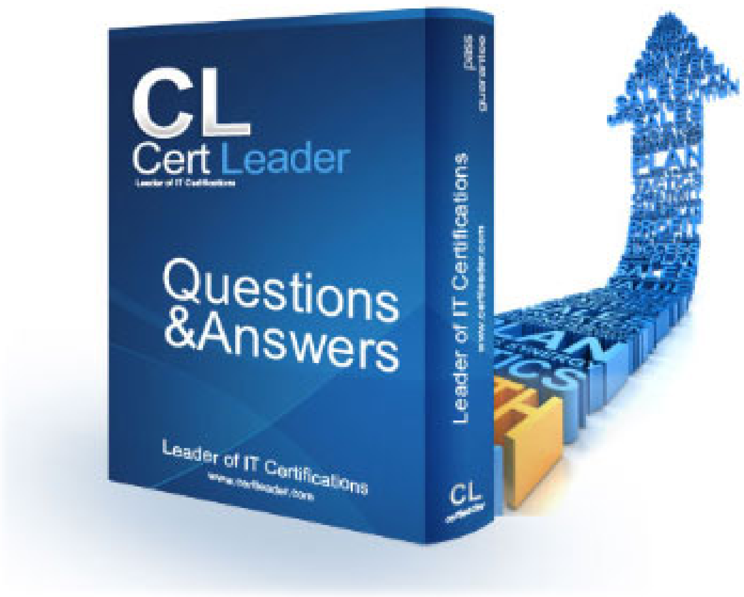
C2150-606 Dumps

IBM Security Guardium V10.0 Administration

https://www.certleader.com/C2150-606-dumps.html



NEW QUESTION 1
A Guardium administrator installed the BUNDLE-STAP module and is monitoring the state of the install. Which state requires a database server reboot to complete the installation process?

A. Ip
B. IP-PR
C. FAILED
D. PENDING-UPDATE

Answer: B

NEW QUESTION 2
Which port must be open for encrypted communication between UNIX S-TAP and Collector?

A. 9500
B. l60l6
C. l60l7
D. l60l8

Answer: D

NEW QUESTION 3
A Guardium administrator installed an S-TAP but is not seeing any data in reports on the collector. The administrator discovered that an Inspection Engine is not configured for that S-TAP.
What is an Inspection Engine?

A. A piece of software residing on the Collectors.
B. Another software to be installed on the Database server.
C. The same thing as the policy and it runs on the S-TAP to inspect the traffic in real-time.
D. A set of parameters needed for the S-TAP to define how to monitor traffic for a particular database instance on a server.

Answer: C

NEW QUESTION 4
A Guardium administrator is preparing commands to install or upgrade an S-TAP using the command line method. Which operating system can use the ktap_allow_module_combos parameter for the installation and upgrade?

A. AIX
B. Linux
C. Solaris
D. HP-UX

Answer: B

NEW QUESTION 5
A Guardium administrator is setting up a Collector schedule to export data to an Aggregator and Archive its data to an Archive storage unit for additional data safety.
Given this scenario, which is true regarding the purge schedule?

A. The Archive and the Export have independent purge schedules but should not be run at the same time.
B. The Guardium unit would run the Export and Archive before any purge, so you would only see the last purge run each day.
C. it would not be possible to configure both on a Collector, the Aggregator should do the archiving and only export from the Collector.
D. Any time that Data Export and Data Archive are both configured, the purge age must be greater than both the age at which to export and the age at which to archive.

Answer: D

NEW QUESTION 6
A Guardium administrator has an issue with Guardium. The administrator has not seen this particular issue before and needs to get it fixed. To get this resolved, what should the administrator do?

A. Log a PMR and request an answer from IBM Support.
B. Log a PMR so IBM Support can contact the custome
C. Then, while waiting, do a search of the Guardium Knowledge Center and Technotes for known issues and resolutions.
D. Request IBM Support to initiate a remote session and collect what they need to resolve the issue.
E. Search Guardium Knowledge Center and Technotes for known issues and resolution
F. Then, if still needed, collect must_gather information and full problem details required for a new PMR so that IBM Support can review the Problem before contacting the customer.

Answer: D

NEW QUESTION 7
A Guardium administrator needs to use CLI commands to maintain the internal database, clean static orphans, produce static system reports and to monitor live network traffic filtered by IP addresses and port numbers.
Which combination of commands should the administrator use for these tasks?

A. diag and iptraf
B. diag and trace_route
C. jptraf and support must_gather
D. support must_gather and show network verify

Answer: C

NEW QUESTION 8
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_l, INV_2, or INV_3 (case-sensitive).
B. The users must login as one of the predefined user accounts INV_l, INV_2, orlNV_3 (case-sensitive).
C. A separate user must be used with a role of either INV_l, 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_l, INV_2, or INV_3 (case-sensitive).

Answer: D

NEW QUESTION 9
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

NEW QUESTION 10
An administrator just installed the Guardium product using the Guardium ISO image. Which step must the administrator perform as part of the initial set-up of the new appliance?

A. Generate the GUI certificate request.
B. Configure network settings on the appliance.
C. Restart the sniffer process from the CLI command prompt.
D. Obtain the passwords for the databases to be monitored by the appliance.

Answer: B

NEW QUESTION 10
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).

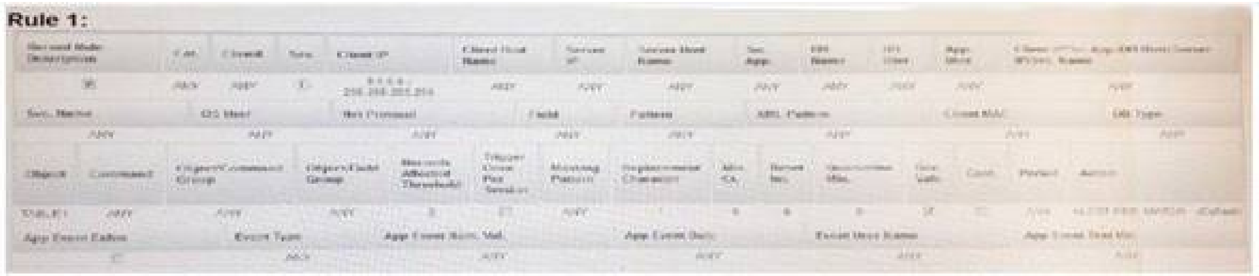
Answer: D

NEW QUESTION 14
AGuardium 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=l
B. KTAP_NO_ROLLBACK=l
C. KTAP_LIVE_UPDATE=Y
D. KTAP_ALLOW_MODULE_COMBOS=Y

Answer: C

NEW QUESTION 15
A Guardium policy has been configured with the following two rules:



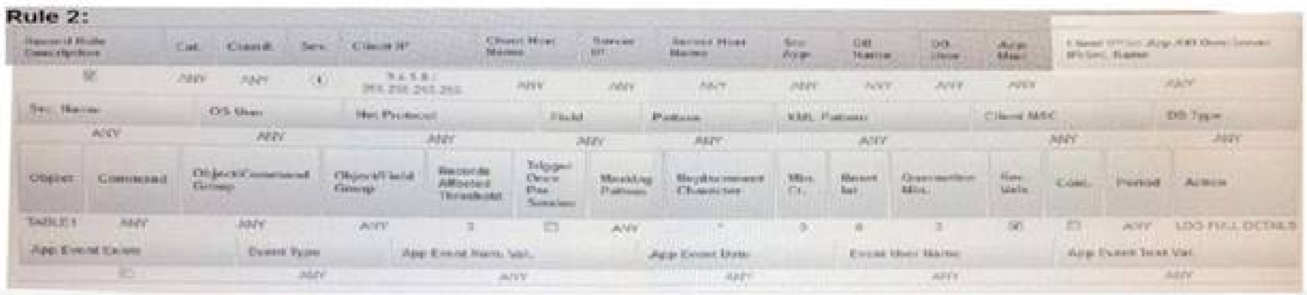
Rule 1:

[illegible] Rule Description	Cat.	Classif.	Sev.	Client IP	Client Host Name	Server IP	Server Host Name	Svc. App.	DB Name	DB User	App. User	Client IP/Src. App./DB User/Server IP/Svc. Name
☒	ANY	ANY	1	9.4.5.6 / 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
TABLE1	ANY	ANY	ANY	3	☐	ANY	*	0	0	0	☒	☐	ANY	ALERT PER MATCH (Default)

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:

[illegible] Rule Description	Cat.	Classif.	Sev.	Client IP	Client Host Name	Server IP	Server Host Name	Svc. App.	DB Name	DB User	App. User	Client IP/Src. App./DB User/Server IP/Svc. Name
☒	ANY	ANY	4	9.4.5.6 / 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
TABLE1	ANY	ANY	ANY	3	☐	ANY	*	0	0	1	☒	☐	ANY	LOG FULL DETAILS

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

A Guardium administrator is required to check for SQL statements from client IP 9.4.5.6 executed on object "TABLET.
What domain(s) can the administrator create a report in to see the SQL?

A. Access
B. Policy Violations
C. Access and Access Policy
D. Access and Policy Violations

Answer: A

NEW QUESTION 20
......