CERTPARK CERTPARK OUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides, High Passing Rate! provides update free of charge in one year!



https://www.certpark.com

Exam : C2150-606

Title: IBM Security GuardiumV10.0 Administration

Version : Demo

1.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 <ip address> <port number>

D. Login as CLI and execute support show port open <ip address> <port number>

Answer: D

2.A Guardium administrator manages an environment containing four standalone Collectors. The administrator has been asked to provide a weekly report showing all Data Manipulation Language (DML) SQL statements performed by all database administrators on all databases. The administrator does not want to run the report on each Collector.

What should the administrator do to simplify this task and run the report in only one place every week? A. Replace the 4 Collectors with one Aggregator.

B. Create an Enterprise Report on one Collector combining the data.

C. Add a Guardium Aggregator to the environment. Create and run the report on the Aggregator.

D. install a Configuration Auditing System (CAS) on each Database Server. Configure the CAS Client to send data to a Collector. Create and run the report on the Collector.

Answer: C

3.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 customer. Then, while waiting, do a search of the Guardium Knowledge Center and Technotes for known issues and resolutions.

C. Request IBM Support to initiate a remote session and collect what they need to resolve the issue.

D. Search Guardium Knowledge Center and Technotes for known issues and resolutions. 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

4.A Guardium policy has been configured with the following two rules:

lule 1:																il and the	1
Necord Hute Description	Cat. Classif.		Sev.	Client IF		Client Host Nome	Server 1P	Server Nome	Server Host Name		DB Nome	DB User	A	pp. ser	Client II ¹¹ Src App./DB User/Server II ¹⁷ Svc, Nam		
199	ANY ANY (I)			9 9.8.7 / 255 255 255 255		ANY	ANY		ANY	ANY	ANY		ANY		ANY		
Svc. Namo	OS User			Net Protocol		Field		Patterń		XML Pattern		Cilent M		nt MAC	AC DB		Type
ANY	MIY				ANY	AJ		ALCY ALCY		ANY					ANY		ANY
Object Command	Object/Command Group			Object/Field Records Affected Threaho		Por	Maski Pattor			Min. Ct.	Resor Int.	Outerandine Min		Rec. Vals	Cont.	Period	Actic
MIT ANY		Atre		ANY	1.11 0		ANY			0	¢	0		191	1.	ANY	
App Event Exists	Event type			Ар	App Event Num, Vol.			App Event Dote			Event User Name			App Event Text Vol.			
				ANY			ANY			ANY			ANY				
ule 2:																	
Record Rule Description	Cot.	Cat. Classif. Sev. Client					Sorver Surver				DO Us				nit IP: See App. /DB Usee Pierry Svc. Name		
80	NNY	ANY ANY (ANY ANY		ANY		ANY ANY		ANY		NY	ANY		AUX		
Svc. Name	OS User			Not Protoc	Not Protocol		Fletd P		Antorn X		ML Patters		Client MAC		DB Type		
ATTY	ANTY			ANY		ANY		ANY		ANY				ANY		ANY	
Object Command		Object/Constraint Group		bjec.0Field roup	Records Alfected Threshold		Once Masking Per Patietin				n. Mi	narentino Rus In. Val				nod Action	
ANY OFICIT		ANY		ANY	0	D	MA			a	a	0	(a) <u>(</u>		Atry Carlos and		
App Event Exists Event Type				Ap	App Event Num. Vol.			App Event Unte			Event User Name			App Event Lost Vel.			
	MAN				ANY			ANY			AREY				AUT		

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

5.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