EDUSUM

#1 Online Certification Guide

IBM C2150-606

IBM Security Guardium Administration Certification Questions & Answers

Exam Summary – Syllabus –Questions

C2150-606

IBM Certified Administrator - Security Guardium V10.0

55 Questions Exam – 64% Cut Score – Duration of 90 minutes

Table of Contents:

Know Your C2150-606 Certification Well:

The C2150-606 is best suitable for candidates who want to gain knowledge in the IBM Security. Before you start your C2150-606 preparation you may struggle to get all the crucial Security Guardium Administration materials like C2150-606 syllabus, sample questions, study guide.

But don't worry the C2150-606 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the C2150-606 syllabus?
- How many questions are there in the C2150-606 exam?
- Which Practice test would help me to pass the C2150-606 exam at the first attempt?

Passing the C2150-606 exam makes you IBM Certified Administrator - Security Guardium V10.0. Having the Security Guardium Administration certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

IBM C2150-606 Security Guardium Administration Certification Details:

Exam Name	IBM Certified Administrator - Security Guardium V10.0
Exam Code	C2150-606
Exam Price	$200 (USD)
Duration	90 mins
Number of Questions	55
Passing Score	64%
Books / Training	**C2150-606: Software Support Handbook**
Schedule Exam	**Pearson VUE**
Sample Questions	**IBM Security Guardium Administration Sample Questions**
Practice Exam	**IBM C2150-606 Certification Practice Exam**

C2150-606 Syllabus:

Topic	Details	Weights
Product features and capabilities	- Understand high-level components of a Guardium solution. - Describe the features and capabilities of Data Activity Monitoring (DAM) and File Activity Monitoring (FAM). - Describe the features and capabilities of Classification, Entitlement, and Vulnerability Assessment. - Use data level access control features (SGATE and Redaction). - Describe features and capabilities of available agents and modules (GIM, S-TAP, CAS, etc).	15%
Planning, sizing and capacity	- Identify the main factors that affect the volume of data managed by Guardium including backups and archives. - Plan appliance location architecture. - Understand properties of the systems to be monitored such as operating systems, databases, type of data and volume and their effects. - Plan strategy for high availability. - Calculate the number and type of appliances required based on Processor Value Unit (PVU) load. - Identify the system requirements of Guardium appliances.	15%
Installation and configuration	- Locate and download appropriate Guardium appliance and agent installers. - Build new collectors and aggregators. - Perform initial appliance setup and configuration. - Configure appliance data management processes and schedules. - Configure the appliance for interfacing with standard systems (mail, SNMP, LDAP, SIEM). - Manage the access of Guardium users. - Install Guardium Installation Manager (GIM) and upgrade agents and modules with GIM. - Install software tap (S-TAP) from command line. - Demonstrate detailed understanding of agent configuration and inspection engine parameters.	25%
Data monitoring, policy rules and reporting	- Perform a Vulnerability Assessment test. - Differentiate the effects of policy rules and associated actions.	15%

Topic	Details	Weights
	- Define and use monitoring features such as queries, reports, audit processes, and alerts. - Use Enterprise Search.	
Self-monitoring and performance	- Use Guardium self-monitoring reports and alerts. - Analyze and act upon errors or exceptions. - Identify and resolve appliance performance issues. - Optimize internal database tables to maintain performance. - Monitor and report on Guardium user activity. - Maintain a managed environment.	15%
Maintenance and support	- Use available IBM troubleshooting resources and services, for example, Knowledge Center, technotes and IBM Support. - Plan and install appliance patches and agent upgrades. - Collect diagnostic information and troubleshoot problems. - Use common Command Line Interface (CLI) and GrdAPI commands including support commands. - Restore data and configuration from backups and archives.	15%

IBM C2150-606 Sample Questions:

Question: 1

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

a) 9500
b) 16016
c) 16017
d) 16018

Answer: d

Question: 2

In a centrally managed environment, while executing the report 'Enterprise Buffer Usage Monitor', a Guardium administrator gets an empty report. Why is the report empty?

a) The report is not executed with a remote source on the Aggregator.
b) Correct custom table upload is not scheduled on the Central Manager.
c) Sniffers are not running on the Collectors.
d) The report is not executed with a remote source on the Collector.

Answer: a

Question: 3

A Guardium administrator has a standalone Collector which is monitoring critical production databases during the working day.
Archives are taken daily before work starts and purges take place on all data older than 5 days.
This is all working well. However, an auditor arrives at 10:00 am local time and wants to review data from 3 weeks ago.
When can the administrator restore the data for the auditor?

a) The restore can be done in the morning as it will not impact data collection.
b) The restore can be done at lunch time, to avoid a performance impact during high volume of current traffic.
c) The restore can only take place outside of working hours as the data cannot be captured during the restore process.
d) The restore can be done anytime, but might need to accept some data loss if the performance is impacted too much.

Answer: c

Question: 4

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) Login as CLI and execute support show port open <ip address> <port number>
c) Login as CLI and execute telnet <ip address> <port number>
d) Ask IBM technical support to login as root and verify.

Answer: b

Question: 5

During the installation phase, the Guardium administrator ensured that the same S-TAP installation procedures were performed on both Oracle 11 and DB2 10.5 systems. They both run on servers with the same version of Linux.

However, during the testing, it was found that all local DB2 connection activities were not captured in the activity report. Meanwhile, all activities on Oracle and all DB2 TCP activities were captured.

What additional step should the administrator take on the database server to capture the missing DB2 shared memory traffic?

a) Reboot the Linux server.
b) Restart the DB2 instance.
c) Configure the DB2 EXIT Library.
d) Configure both the A-TAP and DB2 EXIT Library.

Answer: c

Question: 6

A Guardium administrator needs to configure daily purge. What is the default value for purge data older than configured on the Guardium appliance?

a) 60 days
b) 90 days
c) 180 days
d) 365 days

Answer: a

Question: 7

An audit process is currently scheduled to run with User1 as a receiver. User1 leaves the company and the Guardium administrator is asked to replace User1 with User2. How can the administrator achieve this?

a) Create another audit process with User2 as the receiver.
b) Modify the audit process to add the User2 as the receiver.
c) Clone the current audit process, remove User1, and add User2.
d) Modify the audit process, delete the User1 as the receiver, and add User2 as the receiver.

Answer: c

Question: 8

A Guardium administrator has a Collector exporting to an Aggregator. Both appliances are set to Eastern Standard Timezone (EST). The administrator runs a report at 9:00 am EST every day on the Aggregator to show activity for yesterday for all units exporting to the Aggregator.

However, the administrator does not see data for this Collector in the report output. The administrator looks at both screenshots below. First screen shot is the Data Export configuration on the Collector, and there is a schedule to run this every day at 11:00 am EST. Data Import runs every day at 7:00 am EST on the Aggregator.

What problem does the administrator see in the configuration that may be causing the issue? And what can the administrator do to fix it?

a) Problem: Export data older than and Ignore data older than are inverted. Solution: Invert the settings.
b) Problem: Export data older than and Ignore data older than are too low. Solution: Increase both settings by 1.
c) Problem: Reports are run after Data Import runs. Solution: Run the reports on the Aggregator before the Data Import runs.
d) Problem: The Data Export on the Collector runs after the Data Import on the Aggregator. Solution: Modify the schedules so Data Export on Collector runs before the Data Import on the Aggregator.

Answer: d

Question: 9

A Guardium administrator is building a policy to monitor files on a datasource. Which actions can the administrator use in the policy?

a) Allow
b) Audit only
c) Alert and Audit
d) Alert per match
e) Ignore S-TAP Session

Answer: b, c

Question: 10

A Guardium administrator is notified by the Security Incident Event Manager (SIEM) administrator in the organization that Guardium is sending real time policy alerts to the SIEM in an incorrect format.

How can the Guardium administrator verify the format that is being used?

a) Check the policy violations report.
b) Check on the IBM Knowledge Center to find the template.
c) On the GUI Anomaly Detection page, find the active alerts and check their definitions.
d) On the GUI Global Profile page, check the Named Template used in the policy action.

Answer: d

Study Guide to Crack IBM Security Guardium Administration C2150-606 Exam:

- Getting details of the C2150-606 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the C2150-606 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the IBM provided training for C2150-606 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the C2150-606 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on C2150-606 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for C2150-606 Certification

Make EduSum.com your best friend during your IBM Security Guardium V10.0 Administration exam preparation. We provide authentic practice tests for the C2150-606 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual C2150-606 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the C2150-606 exam.

Start Online practice of C2150-606 Exam by visiting URL
https://www.edusum.com/ibm/c2150-606-ibm-security-guardium-v100-administration