



IBM C1000-197

**IBM Guardium Data Protection Administrator Professional
Certification Questions & Answers**

Exam Summary – Syllabus – Questions

C1000-197
IBM Certified Guardium Data Protection v12.x Administrator - Professional
60 Questions Exam – 68% Cut Score – Duration of 90 minutes

Table of Contents:

Know Your C1000-197 Certification Well:	2
IBM C1000-197 Guardium Data Protection Administrator Professional Certification Details:	2
C1000-197 Syllabus:	3
IBM C1000-197 Sample Questions:	4
Study Guide to Crack IBM Guardium Data Protection Administrator Professional C1000-197 Exam:.....	6

Know Your C1000-197 Certification Well:

The C1000-197 is best suitable for candidates who want to gain knowledge in the IBM Security. Before you start your C1000-197 preparation you may struggle to get all the crucial Guardium Data Protection Administrator Professional materials like C1000-197 syllabus, sample questions, study guide.

But don't worry the C1000-197 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 C1000-197 syllabus?
- How many questions are there in the C1000-197 exam?
- Which Practice test would help me to pass the C1000-197 exam at the first attempt?

Passing the C1000-197 exam makes you IBM Certified Guardium Data Protection v12.x Administrator - Professional. Having the Guardium Data Protection Administrator Professional 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 C1000-197 Guardium Data Protection Administrator Professional Certification Details:

Exam Name	IBM Certified Guardium Data Protection v12.x Administrator - Professional
Exam Code	C1000-197
Exam Price	\$200 (USD)
Duration	90 mins
Number of Questions	60
Passing Score	68%
Books / Training	Guardium Data Protection
Schedule Exam	Pearson VUE
Sample Questions	IBM Guardium Data Protection Administrator Professional Sample Questions
Practice Exam	IBM C1000-197 Certification Practice Exam

C1000-197 Syllabus:

Topic	Details	Weights
Architecture / Planning / Designing	<ul style="list-style-type: none"> - Explain GDP Architecture - Monitoring Methods - Define License Types - Plan advanced analytics 	13%
Deploy and Configure	<ul style="list-style-type: none"> - Appliances - Anomaly Detection - Deploy Monitoring Agents - Configure Advanced Analytics - Manage Groups - Create Data Source Definitions - Configure Integrations - Access Management 	23%
Discover, Assess and Harden	<ul style="list-style-type: none"> - Database Discovery - Sensitive Data Discovery & Classification - Vulnerability Assessment - CAS 	8%
Policy Management	<ul style="list-style-type: none"> - Define Policy - Install a Policy - Policy Maintenance 	12%
Reporting and Alerting	<ul style="list-style-type: none"> - Report Building - Alerts - Investigation Dashboard 	10%
System Health	<ul style="list-style-type: none"> - Check Guardium Deployment Health - Data Management - Alert Builder 	12%
Maintenance	<ul style="list-style-type: none"> - Appliance - Agents 	10%
Troubleshooting	<ul style="list-style-type: none"> - Support - Reviewing Configurations - Troubleshooting Problems 	12%

IBM C1000-197 Sample Questions:

Question: 1

What is the purpose of Guardium Installation Manager (GIM)?

- a) Specifying the database platform and the instances that the S-TAP monitors on the S-TAP host.
- b) Capturing change audit information of configuration files and more on the database server.
- c) Facilitating installation, updating and configuration of agents.
- d) Monitoring activity between the client and the database and forwards that information to the Guardium collector.

Answer: c

Question: 2

Where can data archived on an aggregator be restored?

- a) On any collector
- b) On any aggregator
- c) On a standalone collector
- d) On a collector that was exported to the aggregator

Answer: b

Question: 3

Which method is used to send alerts and events to a SIEM product?

- a) Syslog Forwarding
- b) Policy Event Forwarding
- c) Service Ticket Forwarding
- d) Correlated Message Forwarding

Answer: a

Question: 4

Which two (2) parameters are required in the 'Choose Parameters' section when installing the S-TAP client for Linux via 'Set Up by Client' using GIM?

- a) STAP_TAP_IP
- b) STAP_ENABLED
- c) STAP_INSTALL_DIR
- d) STAP_SQLGUARD_IP
- e) KTAP_ALLOW_MODULE_COMBOS

Answer: a, d

Question: 5

How can a datasource be created for use with Guardium Classifier application?

- a) Using Guardium STAP
- b) Using Database platform
- c) Using Datasource Guardium API
- d) Using Uploading a Word Doc file

Answer: c

Question: 6

Which data security logging rule action creates policy violations?

- a) Log Only
- b) Log Full Details
- c) Log Masked Details
- d) Log Full Details with Values

Answer: a

Question: 7

What action is required for a collector to apply changes after a group member is updated in an active policy?

- a) Select the group from the Group Builder page, then click the Refresh Table icon.
- b) Select the policy from the Security Policies page that uses the group, then click the Refresh Table icon.
- c) Select the group from the Group Builder page, go to Actions, and choose Flatten Hierarchical Groups.
- d) Select the policy from the Security Policies page that uses the group, then click Install and Reinstall.

Answer: d

Question: 8

What is the main reason to purge data in the Guardium system?

- a) Speed up access operations on the internal database
- b) To avoid adding disk partitions for the internal database
- c) GDPR security compliance reasons for internal database
- d) Minimize the risk to access sensitive data in the internal database

Answer: a

Question: 9

A Guardium has two security policies installed. What would prevent another policy, with limited logging, from being installed?

- a) 'Install Last' must be selected when adding a new policy
- b) 'Selective Audit trail' was enabled in the policy
- c) 'Run Once Now' must be executed after policy installation
- d) 'Run Once Now' must be executed before policy installation

Answer: b

Question: 10

What is the underlying technology in the architecture of Guardium Universal Connector?

- a) Kafka nodes
- b) Kafka cluster
- c) Filebeat server
- d) Logstash pipeline

Answer: d

Study Guide to Crack IBM Guardium Data Protection Administrator Professional C1000-197 Exam:

- Getting details of the C1000-197 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 C1000-197 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 C1000-197 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 C1000-197 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 C1000-197 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for C1000-197 Certification

Make EduSum.com your best friend during your IBM Guardium Data Protection v12.x Administrator - Professional exam preparation. We provide authentic practice tests for the C1000-197 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual C1000-197 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 C1000-197 exam.

Start Online practice of C1000-197 Exam by visiting URL

<https://www.edusum.com/ibm/c1000-197-ibm-guardium-data-protection-v12-x-administrator-professional>