EDUSUM

#1 Online Certification Guide

GIAC GCFR

GIAC Cloud Forensics Responder Certification Questions & Answers

Exam Summary – Syllabus –Questions

GCFR

GIAC Cloud Forensics Responder (GCFR)

82 Questions Exam – 62% Cut Score – Duration of 180 minutes

Table of Contents:

Know Your GCFR Certification Well:

The GCFR is best suitable for candidates who want to gain knowledge in the GIAC Digital Forensics, Incident Response & Threat Hunting. Before you start your GCFR preparation you may struggle to get all the crucial GIAC Cloud Forensics Responder materials like GCFR syllabus, sample questions, study guide.

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

Passing the GCFR exam makes you GIAC Cloud Forensics Responder (GCFR). Having the GIAC Cloud Forensics Responder certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

GCFR GIAC Cloud Forensics Responder Certification Details:

Exam Name	GIAC Cloud Forensics Responder (GCFR)
Exam Code	GCFR
Exam Price	$979 (USD)
Duration	180 mins
Number of Questions	82
Passing Score	62%
Books / Training	**FOR509: Enterprise Cloud Forensics and Incident Response**
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GCFR Sample Questions**
Practice Exam	**GIAC GCFR Certification Practice Exam**

GCFR Syllabus:

Topic	Details
AWS Cloud Platform Logging	- The candidate will demonstrate an understanding of the information available from the generation, collection, retention and storage of logs from AWS
AWS Structure and Access Methods	- The candidate will demonstrate an understanding of AWS architectures, logging, data access and the investigative possibilities
Azure & M365 Cloud Platform Logging	- The candidate will demonstrate an understanding of the information available from the generation, collection, retention and storage of logs from Azure & M365
Azure & M365 Structure and Access Methods	- The candidate will demonstrate an understanding of Azure and M365 architectures, logging, data access and the investigative possibilities
Cloud Forensic Artifact Techniques	- The candidate will demonstrate an understanding of the services, tools and resources available to assist with and automate forensic investigations
Cloud Storage Platforms	- The candidate will demonstrate an understanding of the different characteristics of each cloud's storage resources. The candidate will demonstrate an understanding of ways to create, secure, access and use each storage type.
Cloud Virtual Machine Architecture	- The candidate will demonstrate an understanding of the different types, configuration and availability of virtual machines offered in each cloud environment.
Cloud-based Attacks	- The candidate will demonstrate an understanding of the tactics and techniques used to attack major cloud provider's computing resources.
GCP and Google Workspace Cloud Platform Logging	- The candidate will demonstrate an understanding of the information available from the generation, collection, retention and storage of logs from GCP and Google Workspace
GCP and Google Workspace Structure and Access Methods	- The candidate will demonstrate an understanding of GCP and Google Workspace architectures, logging, data access and the investigative possibilities
In-Cloud Investigations	- The candidate will demonstrate an understanding of how to collect forensic images and how to extract data from cloud resources to conduct forensic investigations.
Introduction to Enterprise Cloud Digital Forensics and	- The candidate will demonstrate an understanding of the most popular cloud concepts. The candidate will demonstrate an understanding of key cloud resources and

Topic	Details
Incident Response	logs used to facilitate incident response and forensics.
Multi-Cloud Virtual Networking	- The candidate will demonstrate an understanding of each cloud networking topology and the grouping of resources for network communication. The candidate will demonstrate an understanding of the inspection and control of network traffic.

GIAC GCFR Sample Questions:

Question: 1

An engineer has set up log forwarding for a new data source and wants to use that data to run reports and create dashboards in Kibana. What needs to be created in order to properly handle these logs?

a) Row
b) Parser
c) ingest script
d) Beat

Answer: b

Question: 2

In Azure, which of the following describes a "Contributor"?

a) A collection of permissions such as read, write, and delete
b) A designation on a PKI certificate
c) A specification of who can access a resource group
d) An object representing an entity

Answer: a

Question: 3

Which EBS volume type would be appropriate to support a business critical SQL server hosted In AWS?

a) ST1
b) GP3
c) GP2
d) I01

Answer: d

Question: 4

At what point of the OAuth delegation process does the Resource Owner approve the scope of access to be allowed?

a) After user credentials are accepted by the Authorization Server
b) Once the OAuth token is accepted by the Application
c) When the Resource Server receives the OAuth token
d) Before user credentials are sent to the Authentication Server

Answer: a

Question: 5

What approach can be used to enable Mac instances on AWS?

a) Emulating the M1 processor using ARM clusters
b) Installing OS X exclusively on I (Burstable) instance
c) Using physical Mac computers in the data center
d) Virtualizing OS X on Unix servers

Answer: c

Question: 6

The attack technique "Access Kubelet API" falls under which Mitre ATT&CK tactic?

a) Execution
b) Credential Access
c) Discovery
d) Initial Access

Answer: c

Question: 7

Which of the following is the smallest unit of computing hardware in Kubernetes?

a) Cluster
b) Node
c) Container
d) Pod

Answer: d

Question: 8

What logical AWS structure type is used to chain together accounts in a trust relationship which allows for single sign-on and cross-account management?

a) Subscription
b) Organisation
c) OU
d) Tenant

Answer: b

Question: 9

After registering the application in Azure AD, what is the next step to take in order to use Microsoft Graph API?

a) Request access tokens from Azure An
b) Call the Graph API
c) Configure app permission
d) Get Microsoft 365 global admin approval

Answer: c

Question: 10

Sensitive company data is found leaked on the internet, and the security team didn't get any alert and is unsure of how the breach occurred. Which logs would be a preferable starting point for an investigation?

a) Identity and Access Management
b) Application
c) Resource Management
d) Endpoint

Answer: a

Study Guide to Crack GIAC Cloud Forensics Responder GCFR Exam:

- Getting details of the GCFR 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 GCFR 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 GIAC provided training for GCFR 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 GCFR 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 GCFR practice tests is must. Continuous practice will make you an expert in all syllabus areas.