

IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!

Exam : **GCFR**

Title : **GIAC Cloud Forensics
Responder (GCFR)**

Version : **DEMO**

1. Below is an extract from a Server Access Log showing a record for a request made to an AWS S3 bucket.

What does the first field starting with "385f9e" represent?

```
385f9ef91a82f8ca241dbb08d21b781846f4b75b73589dec7a054f8781cef6eb labresearch
[31/May/2021:14:18:38 +0000] 10.246.62.156 arn:aws:sts::305681518678:assumed-
role/AWSServiceRoleForConfig/AWSConfig-Describe RPB2PVAWY52G8J05
REST.GET.TAGGING - "GET /?tagging HTTP/1.1" 404 NoSuchTagSet 291 - 27 - "-"
"AWSConfig cfg/retry-mode/legacy" -
H9xRp+HGTSnP71vH9gG/9Bfs62jSbfE61nKRYcGBJ/0Y+Z1jBD1SNyqkaMIws3I9gon+w6kJBQY=
SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader labresearch.s3.us-east-
1.amazonaws.com TLSv1.2
```

- A. Bucket Owner
- B. Request ID
- C. Host ID
- D. Cipher Suite

Answer: B

2. Which is the effective access when aws user is assigned to an S3 bucket?

- A. A user must have an employee account
- B. A user must have an account under any AWS account
- C. A user must be under the same AWS account as the S3 bucket
- D. A user must have the AWS IAM role assigned

Answer: C

3. 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

4. An Azure blob is accessed using the link below.

What is the name of the blob container?

```
https://ex-storage.blob.core.windows.net/mymovies/mov1.avi
```

- A. ex-storage
- B. mov.avi
- C. mymovies
- D. blob.core

Answer: C

5. 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