Vendor:GIAC

Exam Code:GCFR

Exam Name:GIAC Cloud Forensics Responder (GCFR)

Version: Demo

QUESTION 1

What Amazon EC2 instance prefix should be monitored to detect potential crypto mining?

A. C

B. P

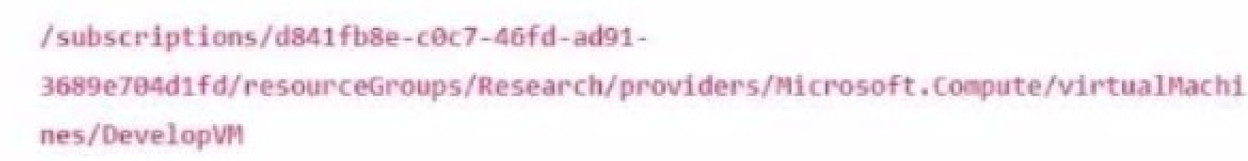
C. R

D. I

Correct Answer: B

QUESTION 2

The Azure URI for the Develop VM is shown below. What will change in the notation when referencing the VM\\'s OS disk?



```
/subscriptions/d841fb8e-c0c7-46fd-ad91-
3689e704d1fd/resourceGroups/Research/providers/Microsoft.Compute/virtualMachi
nes/DevelopVM
```

A. Resource Type

B. Provider

C. Resource Group

D. Subscription ID

Correct Answer: A

QUESTION 3

Which of the following Windows agents would need to be configured on an Azure VM for an investigator to query Its operating system logs sent to Azure Storage?

A. Azure Monitor

B. Diagnostic Extension

C. Dependency

D. Log Analytics

Correct Answer: B

QUESTION 4

Which is a limitation of AWS Lambdas?

A. Functions must run in less than 15 minutes

B. They can be quite costly to operate

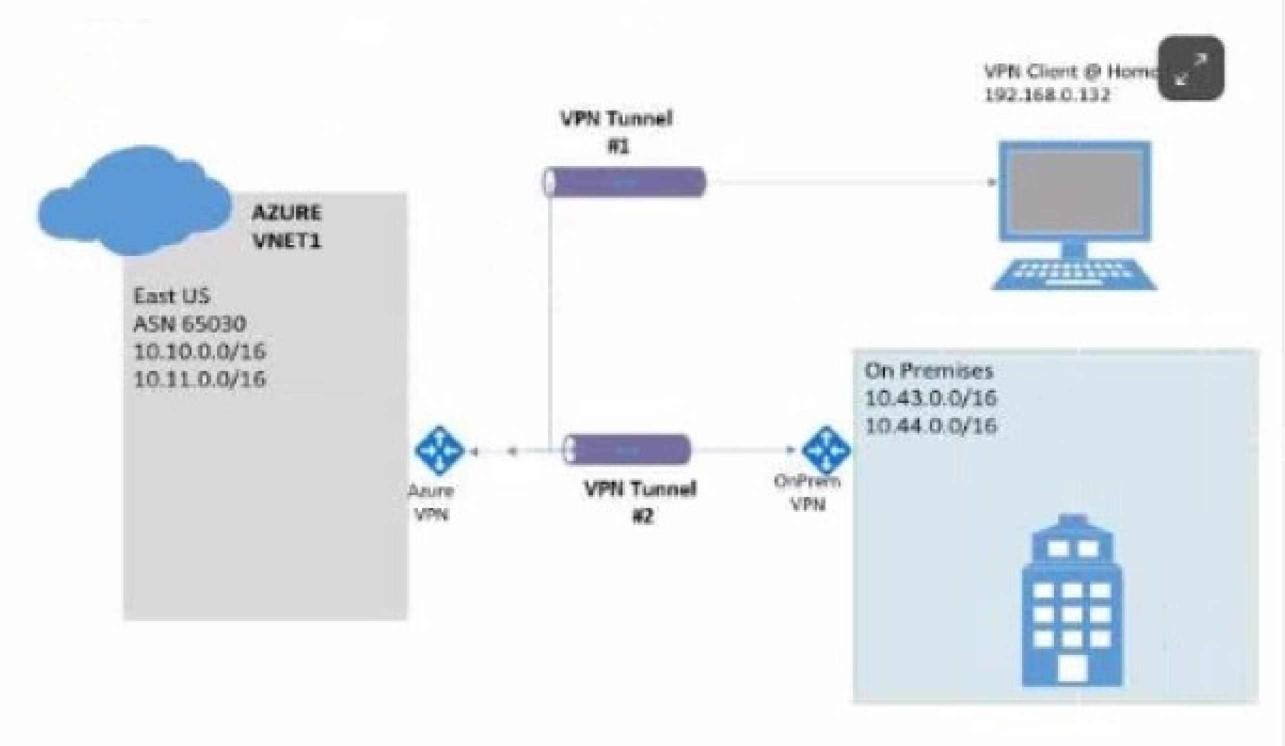
C. Managing systems can be time consuming

D. They only support up to 256 MB of storage

Correct Answer: A

QUESTION 5

Communication between the VPN client and Azure VNet1via VPN Tunnel #1 is using which of the following connections?



A. Point-to-site VPN

B. IPSec

Correct Answer: A

QUESTION 6

Which AWS authentication method provides temporary, limited privilege credentials for 1AM users or federated users?

A. lAMRole

B. API Key

C. SAML Token

Correct Answer: A

QUESTION 7

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

Correct Answer: C

QUESTION 8

Which of the following is available with the free tier of service for CloudTrail?

A. Single trail of management events delivered to Amazon

B. Access to data-related API Cloud Trail events

C. Access to CloudTrail Insights to detect anomalies

D. Default trail maintained by AWS for more than 90 days

Correct Answer: A

QUESTION 9

What information do AWS VPC flow logs collect?

A. Details of all traffic transmitted in or out of the VPC

B. Traffic between end point and load balancer interfaces

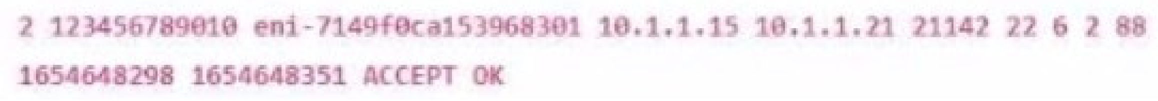
C. Contents of network traffic

D. Length of network connections

Correct Answer: A

QUESTION 10

What type of AWS log is the following snippet an example of?



```
2 123456789010 eni-7149f0ca153968301 10.1.1.15 10.1.1.21 21142 22 6 2 88
1654648298 1654648351 ACCEPT OK
```

A. Web Application firewall Log

B. VPC Flow Log

C. Load Balancer Log

D. Route 53 Query Log

Correct Answer: B

QUESTION 11

What is the maximum file size for Azure Page Blob storage?

A. 10.25 TB

B. 10.25 TB

C. 8TB

D. 7TB

Correct Answer: C

QUESTION 12

Access Kibana via http://10.0.1.7:5601 and use theazure-* index pattern. Between March 31st, 2021 and April 3rd, 2021, how many virtual machines were created that use a Linux operating system?

A. 4

B. 6

C. 5

D. 2

E. 3

F. 8

G. 7

H. 9

I. 1

J. 10

Correct Answer: B