Fortinet

FCSS_ADA_AR-6.7
FCSS - Advanced Analytics 6.7 Architect

- **Up to Date products, reliable and verified.**
- **Questions and Answers in PDF Format.**

Full Version Features:

- **90 Days Free Updates**
- **30 Days Money Back Guarantee**
- **Instant Download Once Purchased**
- **24 Hours Live Chat Support**

For More Information:

https://www.testsexpert.com/

- **Product Version**

Latest Version: 6.0

Question: 1

What is the estimated time that it would take for the collector to reach the maximum buffer size for a 2000 EPS license?
Response:

A. 13.88 hours
B. 27.77 hours
C. 55.55 hours
D. 9.25 hours

Answer: A

Question: 2

During which time period is the license enforcement performed on the number of events received?
Response:

A. Events received every minute
B. Events received every two minutes
C. Events received every three minutes
D. Events received every second

Answer: C

Question: 3

How often do collectors upload data to the Supervisor?
(Choose two.)
Response:

A. Every 20 MB for low EPS environment
B. Every 5 seconds for low EPS environment
C. Every 10 MB for high EPS environment
D. Every 10 seconds for high EPS environment

Answer: B,C

Question: 4

A service provider purchased a licensed EPS of 520 and the total unused events is 72,000. Calculate the total amount of allowed events for the next 3-minute interval.
Response:

A. 192,456
B. 192,442
C. 192,446
D. 192,450

Answer: A

Question: 5

Where can you define automated remediation on FortiSIEM?
Response:

A. Integration policy
B. Notification policy
C. Authentication policy
D. Remediation policy

Answer: B

Question: 6

Which two things should you take into consideration before scaling collectors at a customer site? (Choose two.)
Response:

A. Direct log collection
B. Performance monitoring and SIEM collection jobs
C. The types of operating systems running in the network
D. The complexity of the network

Answer: A,B

Question: 7

What are the two SQLite databases that are used for baseline data?
(Choose two.)
Response:

A. Profile database
B. Event database
C. Weekly database
D. Daily database

Answer: A,D

Question: 8

What is recommended method of adding workers to a FortiSIEM cluster?
Response:

A. Add a worker every 25,000 EPS
B. Add a worker every 20,000 EPS
C. Add a worker every 10,000 EPS
D. Add a worker every 15,000 EPS

Answer: C

Question: 9

What are two reasons that agents maintain communication with the supervisor after registration?
(Choose two.)
Response:

A. To report incoming EPS value
B. To report logs and events
C. To report health and its status
D. To collect new agent template

Answer: C,D

Question: 10

Which function of Linux is used by FortiSIEM for collecting logs?
Response:

A. aureport

B. ausearch
C. autrace
D. auditd

Answer: D

For More Information – **Visit link below:**

https://www.testsexpert.com/

16$ Discount Coupon: 9M2GK4NW

Features:

- Money Back Guarantee……..……...…. 

- 100% Course Coverage…… 

- 90 Days Free Updates…… 

- Instant Email Delivery after Order……