Fortinet.NSE5_FAZ-6.2.v2021-05-16.q20

Exam Code:	NSE5_FAZ-6.2
Exam Name:	Fortinet NSE 5 - FortiAnalyzer 6.2
Certification Provider:	Fortinet
Free Question Number:	20
Version:	v2021-05-16
# of views:	453
# of Questions views:	4934
https://www.freecram.com/torrent/Fortinet.NSE5_FAZ-6.2.v2021-05-16.q20.html	

NEW QUESTION: 1
What FortiGate process caches logs when FortiAnalyzer is not reachable?
A. oftpd
B. logfiled
C. miglogd
D. sqlplugind
Answer: (SHOW ANSWER)

NEW QUESTION: 2
FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for analytics logs is 60 days.
What is the most likely problem?
A. Logs are rolling before the report is run
B. Quota enforcement is acting on analytical data before a report is complete
C. CPU resources are too high
D. Disk utilization for archive logs is set for 15 days
Answer: B (LEAVE A REPLY)

NEW QUESTION: 3
View the exhibit:

What does the 1000MB maximum for disk utilization refer to?

A. The disk quota for each device in the ADOM

B. The disk quota for the ADOM type

C. The disk quota for the FortiAnalyzer model

D. The disk quota for all devices in the ADOM

Answer: D (LEAVE A REPLY)

NEW QUESTION: 4

View the exhibit.

Why is the total quota less than the total system storage?

A. 3.6% of the system storage is already being used.

B. The logfiled process is just estimating the total quota

C. The oftpd process has not archived the logs yet

D. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files

Answer: D (LEAVE A REPLY)

NEW QUESTION: 5

You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used.

What does the disk quota refer to?

A. The maximum disk utilization for all devices in the ADOM

B. The maximum disk utilization for each device in the ADOM

C. The maximum disk utilization for the ADOM type

D. The maximum disk utilization for the FortiAnalyzer model

Answer: D (LEAVE A REPLY)

NEW QUESTION: 6

In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required? (Choose two.)

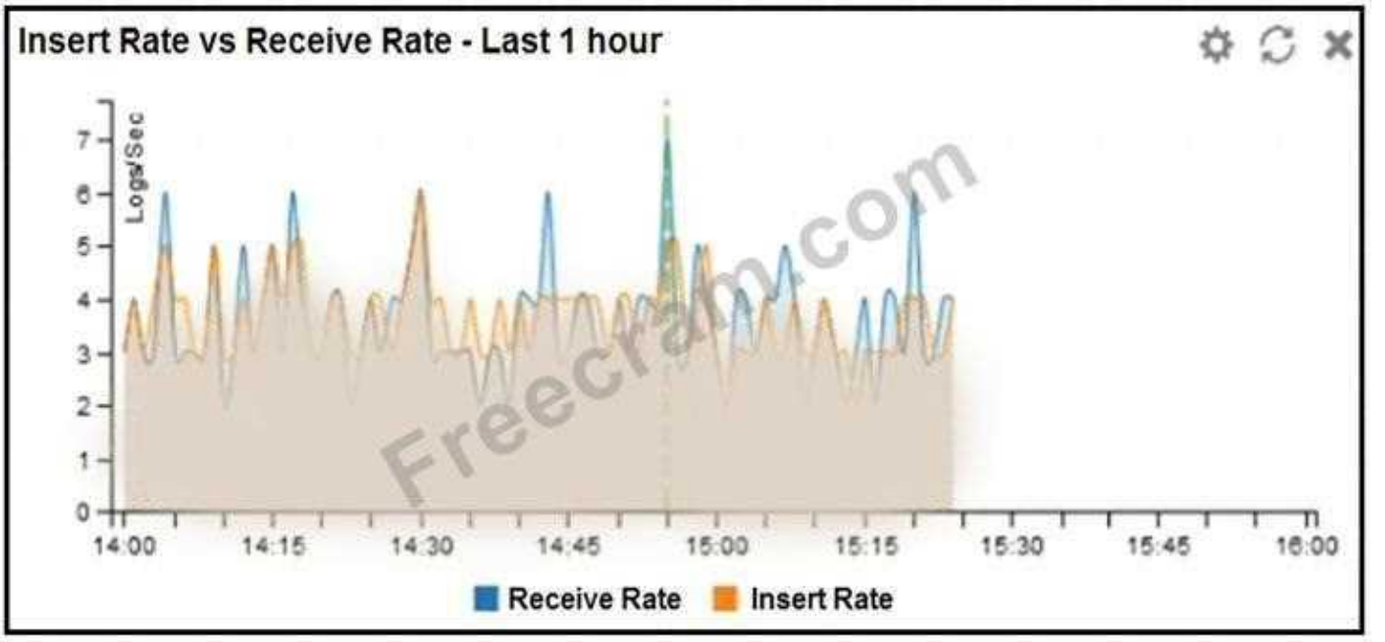
A. Remote logging must be enabled on FortiGate

B. Log encryption must be enabled

C. ADOMs must be enabled
D. FortiGate must be registered with FortiAnalyzer
Answer: (SHOW ANSWER)
Explanation
Pg 70: "after you add and register a FortiGate device with the FortiAnalyzer unit, you must also ensure that the FortiGate device is configured to send logs to the FortiAnalyzer unit." https://docs.fortinet.com/uploaded/files/4614/FortiAnalyzer-5.4.6-Administration%20Guide.pdf Pg 45: "ADOMs must be enabled to support the logging and reporting of NON-FORTIGATE devices, such as FortiCarrier, FortiClientEMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox."

NEW QUESTION: 7
Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally?
(Choose two.)
A. SFTP server
B. Mail server
C. Output profile
D. Report scheduling
Answer: (SHOW ANSWER)

NEW QUESTION: 8
Refer to the exhibit.



What does the data point at 14:55 tell you?
A. Logs are being dropped
B. The sqlplugind daemon is behind in log indexing by two logs
C. The received rate is almost at its maximum for this device
D. Raw logs are reaching FortiAnalyzer faster than they can be indexed

Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
What are the operating modes of FortiAnalyzer? (Choose two)
A. Manager
B. Standalone
C. Collector
D. Analyzer
Answer: (SHOW ANSWER)

NEW QUESTION: 10
What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons?
(Choose three)
A. RADIUS
B. Local
C. PKI
D. TACACS+
E. LDAP
Answer: (SHOW ANSWER)

NEW QUESTION: 11
Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?
A. To improve DNS response times
B. To use real-time forwarding
C. To resolve host names
D. To properly correlate logs
Answer: D (LEAVE A REPLY)

NEW QUESTION: 12
Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?
A. Log fetching
B. Log upload
C. Indicators of Compromise
D. Log forwarding an aggregation mode
Answer: A (LEAVE A REPLY)

NEW QUESTION: 13

After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the purpose of running the following CLI command?
execute sql-local rebuild-adom <new-ADOM-name>
A. To remove the analytics logs of the device from the old database
B. To migrate the archive logs to the new ADOM
C. To reset the disk quota enforcement to default
D. To populate the new ADOM with analytical logs for the moved device, so you can run reports
Answer: (SHOW ANSWER)

NEW QUESTION: 14
What statements are true regarding disk log quota? (Choose two)
A. The FortiAnalyzer stops logging once the disk log quota is met.
B. The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.
C. The FortiAnalyzer disk log quota is configurable, but has a minimum o 100mb a maximum based on the reserved system space.
D. The FortiAnalyzer automatically sets the disk log quota based on the device.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 15
Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)
A. Disk size
B. Total quota
C. License type
D. RAID level
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 16
For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:
A. Use real-time forwarding
B. Use host name resolution
C. Use DNS
D. Use an NTP server
Answer: (SHOW ANSWER)

NEW QUESTION: 17
What statements are true regarding FortiAnalyzer 's treatment of high availability (HA) dusters? (Choose two)
A. FortiAnalyzer receives logs from d devices in a duster.
B. FortiAnalyzer receives bgs only from the primary device in the cluster.
C. FortiAnalyzer only needs to know (he serial number of the primary device in the cluster-it automaticaly discovers the other devices.
D. FortiAnalyzer distinguishes different devices by their serial number.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
If you upgrade the FortiAnalyzer firmware, which report element can be affected?
A. Report settings
B. Output profiles
C. Report scheduling
D. Custom datasets
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19
You are using RAID with a FortiAnalyzer that supports software RAID, and one of the hard disks on FortiAnalyzer has failed.
What is the recommended method to replace the disk?
A. Clear all RAID alarms and replace the disk while FortiAnalyzer is still running
B. Downgrade your RAID level, replace the disk, and then upgrade your RAID level
C. Perform a hot swap
D. Shut down FortiAnalyzer and then replace the disk
Answer: (SHOW ANSWER)

NEW QUESTION: 20
What are two of the key features of FortiAnalyzer? (Choose two.)
A. Cloud-based management
B. Centralized log repository
C. Virtual domains (VDOMs)
D. Reports
Answer: (SHOW ANSWER)

Valid NSE5_FAZ-6.2 Dumps shared by Fast2test.com for Helping Passing NSE5_FAZ-6.2 Exam! Fast2test.com now offer the **newest NSE5_FAZ-6.2 exam dumps**, the Fast2test.com NSE5_FAZ-6.2 exam **questions have been updated** and **answers have been corrected** get the **newest** Fast2test.com NSE5_FAZ-6.2 dumps with Test Engine here: https://www.fast2test.com/NSE5_FAZ-6.2-premium-file.html (**68** Q&As Dumps, **30%OFF Special Discount: freecram**)