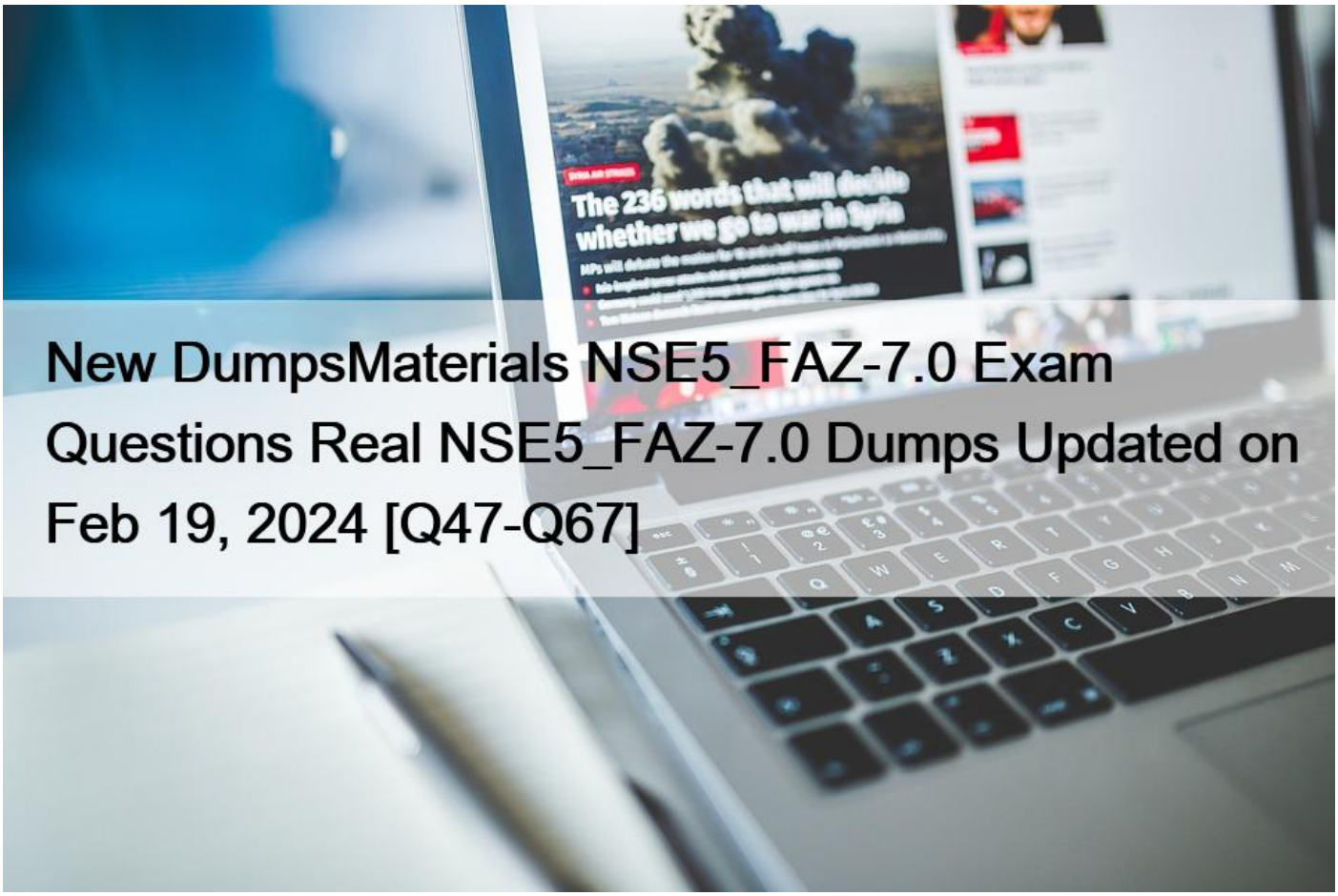
New DumpsMaterials NSE5_FAZ-7.0 Exam Questions Real NSE5_FAZ-7.0 Dumps Updated on Feb 19, 2024 [Q47-Q67



New DumpsMaterials NSE5_FAZ-7.0 Exam Questions| Real NSE5_FAZ-7.0 Dumps Updated on Feb 19, 2024
NSE5_FAZ-7.0 Braindumps – NSE5_FAZ-7.0 Questions to Get Better Grades

Fortinet NSE5_FAZ-7.0 certification exam consists of multiple-choice questions and simulations, which test the candidate's ability to configure and manage FortiAnalyzer 7.0. NSE5_FAZ-7.0 exam covers various topics, including the FortiAnalyzer 7.0 architecture, log collection, analysis, reporting, and troubleshooting. NSE5_FAZ-7.0 exam is designed to test the candidate's ability to deploy and manage FortiAnalyzer 7.0 in a real-world environment.

Q47. What are offline logs on FortiAnalyzer?
* Compressed logs, which are also known as archive logs, are considered to be offline logs.
* When you restart FortiAnalyzer. all stored logs are considered to be offline logs.
* Logs that are indexed and stored in the SQL database.
* Logs that are collected from offline devices after they boot up.

Reference:

Logs are received and saved in a log file on the FortiAnalyzer disks. Eventually, when the log file reaches a configured size, or at a set schedule, it is rolled over by being renamed. These files (rolled or otherwise) are known as archive logs and are considered offline so they don’t offer immediate analytic support. Combined, they count toward the archive quota and retention limits, and they are deleted based on the ADOM data policy. FortiAnalyzer_7.0_Study_Guide-Online page 140

Q48. You need to upgrade your FortiAnalyzer firmware.

What happens to the logs being sent to FortiAnalyzer from FortiGate during the time FortiAnalyzer is temporarily unavailable?
* FortiAnalyzer uses log fetching to retrieve the logs when back online
* FortiGate uses the miglogd process to cache the logs
* The logfiled process stores logs in offline mode
* Logs are dropped

Q49. For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:
* Use DNS
* Use host name resolution
* Use real-time forwarding
* Use an NTP server

Q50. What is the purpose of the following CLI command?

```
# configure system global
     set log-checksum md5
end
```

* To add a log file checksum
* To add the MD’s hash value and authentication code
* To add a unique tag to each log to prove that it came from this FortiAnalyzer
* To encrypt log communications

https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global

Q51. By default, what happens when a log file reaches its maximum file size?
* FortiAnalyzer overwrites the log files.
* FortiAnalyzer stops logging.
* FortiAnalyzer rolls the active log by renaming the file.
* FortiAnalyzer forwards logs to syslog.

Q52. Which two statements about log forwarding are true? (Choose two.)
* Forwarded logs cannot be filtered to match specific criteria.
* Logs are forwarded in real-time only.
* The client retains a local copy of the logs after forwarding.
* You can use aggregation mode only with another FortiAnalyzer.

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/420493/modes

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/621804/log-forwarding

Q53. What is the purpose of output variables?
* To store playbook execution statistics

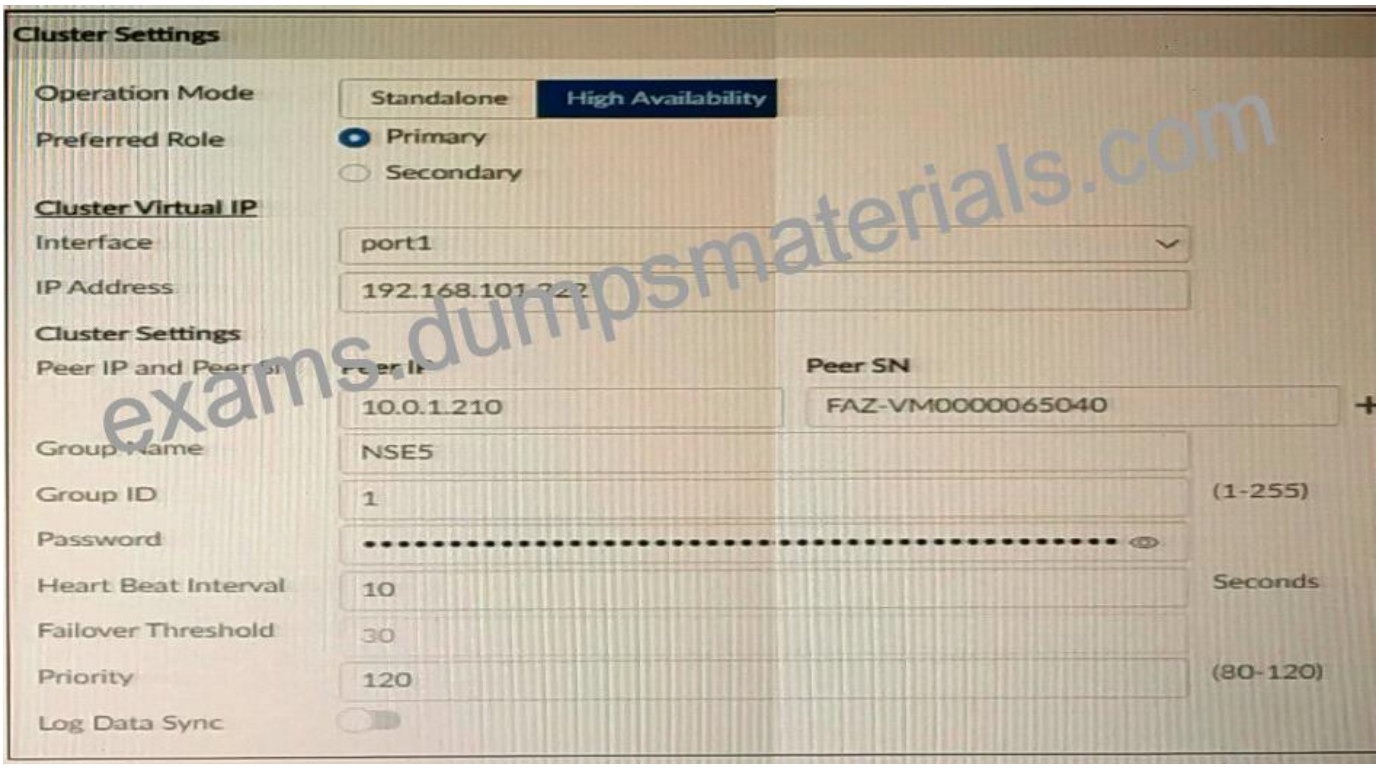
* To use the output of the previous task as the input of the current task
* To display details of the connectors used by a playbook
* To save all the task settings when a playbook is exported

Q54. What statements are true regarding disk log quota? (Choose two)
* The FortiAnalyzer stops logging once the disk log quota is met.
* The FortiAnalyzer automatically sets the disk log quota based on the device.
* The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.
* The FortiAnalyzer disk log quota is configurable, but has a minimum o 100mb a maximum based on the reserved system space.

Q55. Which statement is true regarding Macros on FortiAnalyzer?
* Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.
* Macros are supported only on the FortiGate ADOM.
* Macros are useful in generating excel log files automatically based on the reports settings.
* Macros are predefined templates for reports and cannot be customized.

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 283: Note that macros are ADOM-specific and supported in FortiGate and FortiCarrier ADOMs only.

Q56. Refer to the exhibit.



The image displays the configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster.

What can you conclude from the configuration displayed?
* This FortiAnalyzer will join to the existing HA cluster as the primary.
* This FortiAnalyzer is configured to receive logs in its port1.
* This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.

* After joining to the cluster, this FortiAnalyzer will keep an updated log database.

Q57. On FortiAnalyzer, what is a wildcard administrator account?
* An account that permits access to members of an LDAP group
* An account that allows guest access with read-only privileges
* An account that requires two-factor authentication
* An account that validates against any user account on a FortiAuthenticator

https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/747268/configuring-wildcard-admin-accounts

Q58. Which statement is true regarding Macros on FortiAnalyzer?
* Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.
* Macros are supported only on the FortiGate ADOM.
* Macros are useful in generating excel log files automatically based on the reports settings.
* Macros are predefined templates for reports and cannot be customized.

Q59. FortiAnalyzer centralizes which functions? (Choose three)
* Network analysis
* Graphical reporting
* Content archiving / data mining
* Vulnerability assessment
* Security log analysis / forensics

Q60. View the exhibit:

What does the 1000MB maximum for disk utilization refer to?
* The disk quota for the FortiAnalyzer model
* The disk quota for all devices in the ADOM
* The disk quota for each device in the ADOM
* The disk quota for the ADOM type

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-policy

Q61. What FortiGate process caches logs when FortiAnalyzer is not reachable?
* logfiled
* sqlplugind
* oftpd
* miglogd

Q62. Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)
* License type
* Disk size

* Total quota
* RAID level

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

Q63. Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec? (Choose two.)
* Must configure the FortiAnalyzer end of the tunnel only–the FortiGate end is auto-negotiated.
* Must establish an IPsec tunnel ID and pre-shared key.
* IPsec cannot be enabled if SSL is enabled as well.
* IPsec is only enabled through the CLI on FortiAnalyzer.

Q64. Which statement correctly describes the management extensions available on FortiAnalyzer?
* Management extensions do not require additional licenses.
* Management extensions allow FortiAnalyzer to act as a ForbSIEM supervisor.
* Management extensions require a dedicated VM for best performance.
* Management extensions may require a minimum number of CPU cores to run.

Q65. Which two statements are correct regarding the export and import of playbooks? (Choose two.)
* You can export only one playbook at a time.
* You can import a playbook even if there is another one with the same name in the destination.
* Playbooks can be exported and imported only within the same FortiAnaryzer.
* A playbook that was disabled when it was exported, will be disabled when it is imported.

If the imported playbook has the same name as an existing one, FortiAnalyzer will create a new name that includes a timestamp to avoid conflicts.

Playbooks are imported with the same status they had (enabled or disabled) when they were exported.

Playbooks set to run automatically should be exported while they are disabled to avoid unintended runs on the destination.

Q66. 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?
* Quota enforcement is acting on analytical data before a report is complete
* Logs are rolling before the report is run
* CPU resources are too high
* Disk utilization for archive logs is set for 15 days

Q67. Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec? (Choose two.)
* Must configure the FortiAnalyzer end of the tunnel only–the FortiGate end is auto-negotiated.
* Must establish an IPsec tunnel ID and pre-shared key.
* IPsec cannot be enabled if SSL is enabled as well.
* IPsec is only enabled through the CLI on FortiAnalyzer.

Option B is correct because you must establish an IPsec tunnel ID and pre-shared key to secure the communication between FortiAnalyzer and FortiGate with IPsec12. The tunnel ID is a unique identifier for each tunnel and the pre-shared key is a secret passphrase that authenticates the peers.

Option D is correct because IPsec is only enabled through the CLI on FortiAnalyzer1. You cannot configure IPsec settings through the GUI on FortiAnalyzer.

Fortinet NSE5_FAZ-7.0 certification is suitable for network administrators, security analysts, and other IT professionals who want to demonstrate their expertise in managing and analyzing network security logs. Fortinet NSE 5 - FortiAnalyzer 7.0 certification is also beneficial for those who want to enhance their career prospects in the network security industry.

NSE5_FAZ-7.0 Exam Dumps - Try Best NSE5_FAZ-7.0 Exam Questions:
https://www.dumpsmaterials.com/NSE5_FAZ-7.0-real-torrent.html]