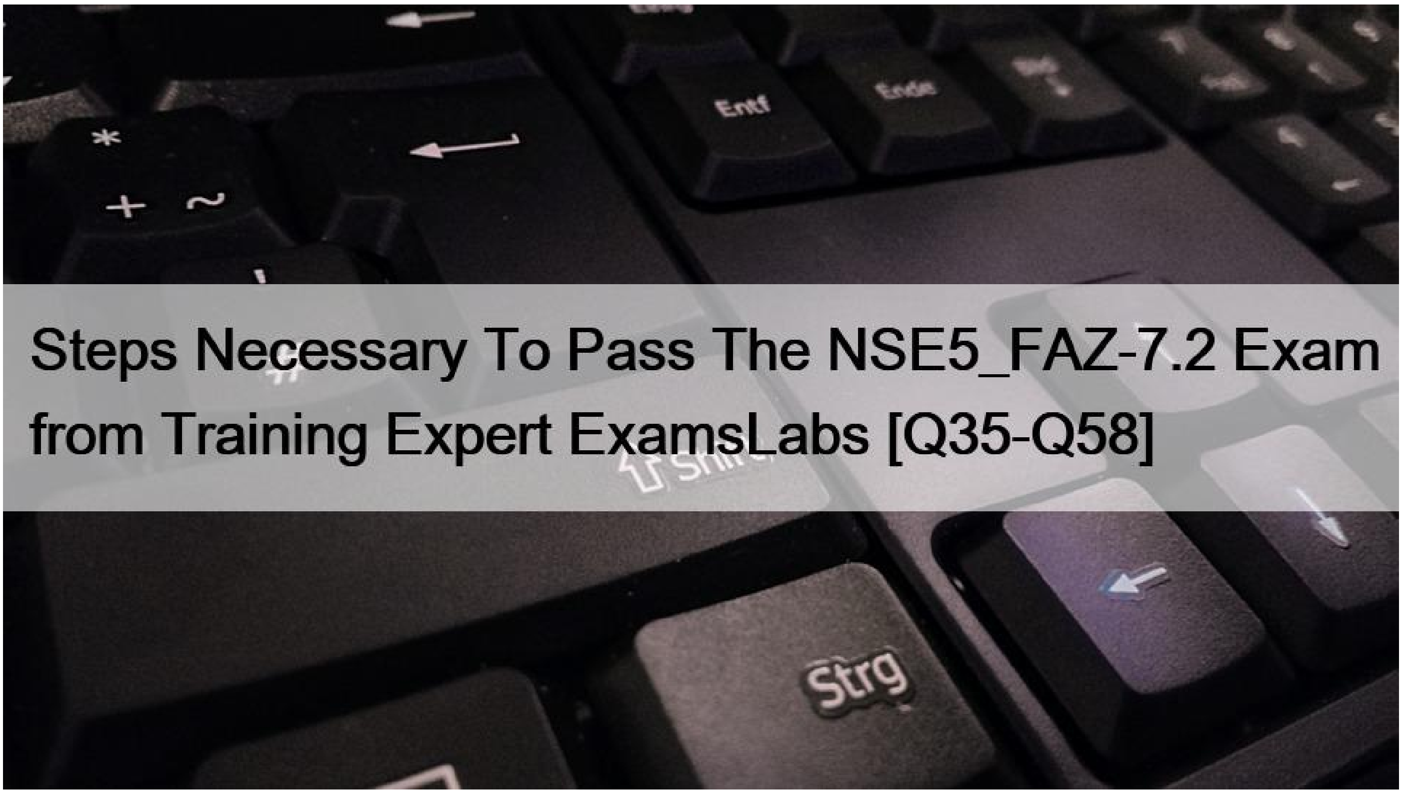
Steps Necessary To Pass The NSE5_FAZ-7.2 Exam from Training Expert ExamsLabs [Q35-Q58



Steps Necessary To Pass The NSE5_FAZ-7.2 Exam from Training Expert ExamsLabs
Valid Way To Pass NSE 5 Network Security Analyst's NSE5_FAZ-7.2 Exam

Fortinet NSE5_FAZ-7.2 exam is designed to test the knowledge and skills of cybersecurity professionals in using FortiAnalyzer 7.2 to collect, analyze, and report on security-related data. NSE5_FAZ-7.2 exam covers a wide range of topics, including FortiAnalyzer deployment, configuration, and administration, as well as log management, analysis, and reporting. NSE5_FAZ-7.2 exam also tests the ability of candidates to troubleshoot common issues and optimize FortiAnalyzer performance.

Q35. Which statement describes online logs on FortiAnalyzer?
* Logs that reached a specific size and were rolled over
* Logs that can be used to create reports
* Logs that can be viewed using Log Browse
* Logs that are saved to disk, compressed, and available in FortiView

Q36. 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

Q37. 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>
* To reset the disk quota enforcement to default
* To remove the analytics logs of the device from the old database
* To migrate the archive logs to the new ADOM
* To populate the new ADOM with analytical logs for the moved device, so you can run reports
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 128: Are the device analytics logs required for reports in the new ADOM? If so, rebuild the new ADOM database

Q38. How can you attach a report to an incident?
* By attaching it to an event handler alert
* By editing the settings of the desired report
* From the properties of an existing incident
* Saving it in JSON format, and then importing it

Q39. 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&#8217;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

Q40. What are two benefits of using fabric connectors? (Choose two.)
* They allow FortiAnalyzer to send logs in real-time to public cloud accounts.
* You do not need an additional license to send logs to the cloud platform.
* Fabric connectors allow you to improve redundancy.
* Using fabric connectors is more efficient than using third-party polling with API.

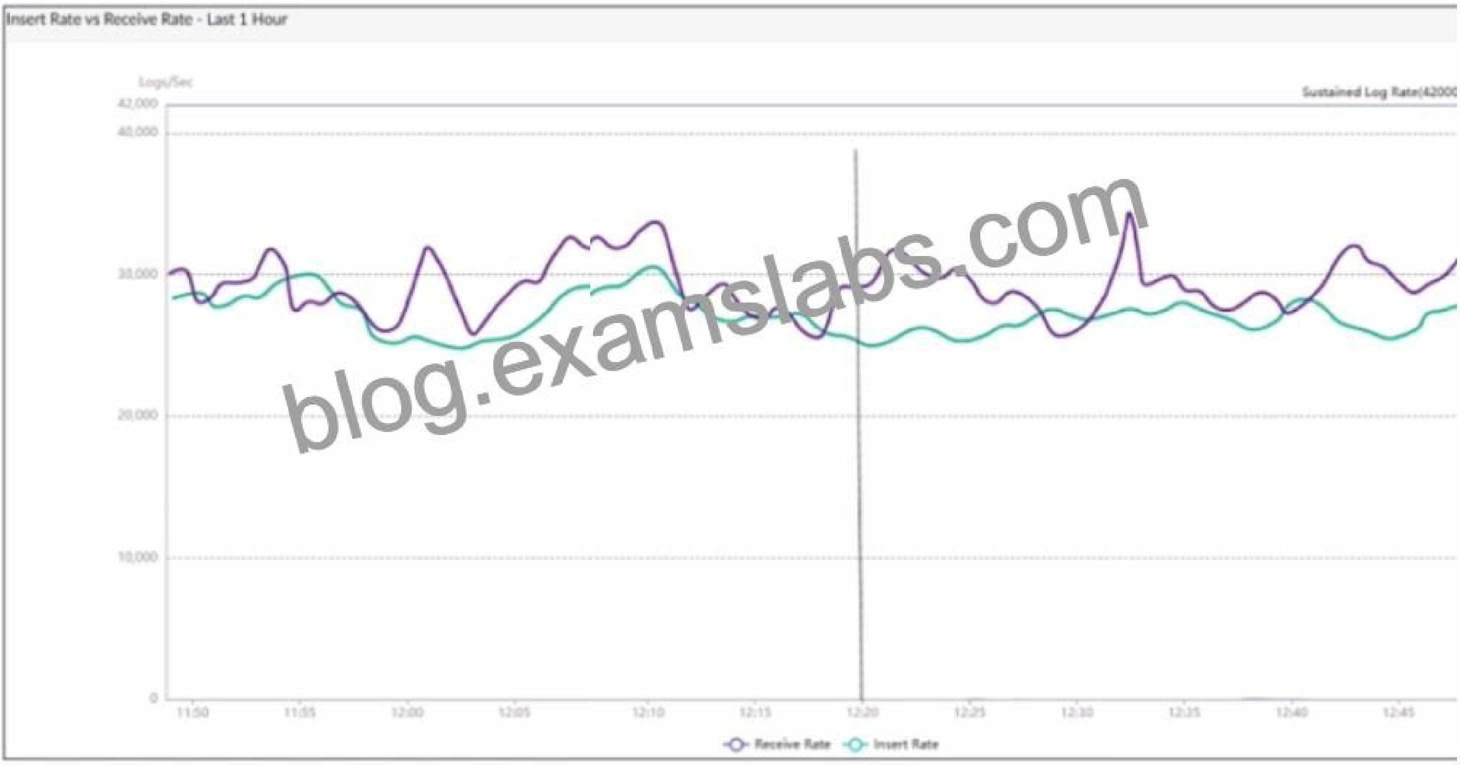
Q41. What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)
* The size of newly generated reports is optimized to conserve disk space.
* FortiAnalyzer local cache is used to store generated reports.
* When new logs are received, the hard-cache data is updated automatically.
* The generation time for reports is decreased.

Q42. Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec? (Choose two.)
* Must configure the FortiAnalyzer end of the tunnel only&#8211;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.

Q43. Refer to the exhibit.



What does the data point at 12:20 indicate?

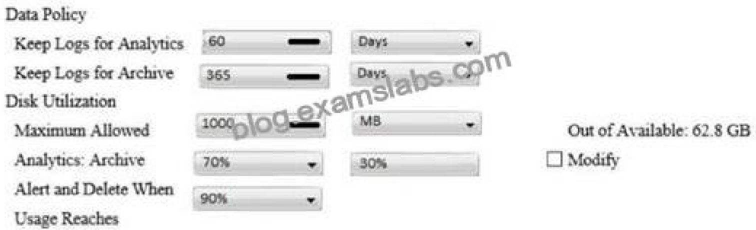
- The performance of FortiAnalyzer is below the baseline.
- FortiAnalyzer is using its cache to avoid dropping logs.
- The log insert lag time is increasing.
- The sqlplugind service is caught up with new logs.

Q44. 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

Q45. View the exhibit:



Data Policy
Keep Logs for Analytics 60 Days
Keep Logs for Archive 365 Days
Disk Utilization
Maximum Allowed 1000 MB Out of Available: 62.8 GB
Analytics: Archive 70% 30% □ Modify
Alert and Delete When Usage Reaches 90%

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

Q46. 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?
* Shut down FortiAnalyzer and then replace the disk
* Downgrade your RAID level, replace the disk, and then upgrade your RAID level
* Clear all RAID alarms and replace the disk while FortiAnalyzer is still running
* Perform a hot swap
https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta-p/194997?externalID=FD41397#:~:text=If%20a%20hard%20disk%20on,process%20known%20as%20hot%20swapping

Q47. What are two of the key features of FortiAnalyzer? (Choose two.)
* Centralized log repository
* Cloud-based management
* Reports
* Virtual domains (VDOMs)

Q48. Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?
* Log upload
* Indicators of Compromise
* Log forwarding an aggregation mode
* Log fetching
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetcher-management

Q49. What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)
* RADIUS
* Local
* LDAP
* PKI
* TACACS+

Q50. Which two actions should an administrator take to view Compromised Hosts on FortiAnalyzer? (Choose two.)
* Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
* Make sure all endpoints are reachable by FortiAnalyzer.
* Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer device.
* Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up to date.
In order to configure IOC, you require the following:

* A one-year subscription to IOC. Note that FortiAnalyzer does include an evaluation license, but it is restrictive and only meant to give you an idea of how the feature works.

* A web filter services subscription on FortiGate device(s)

* Web filter policies on FortiGate device(s) that send traffic to FortiAnalyzer Compromised Hosts or Indicators of Compromise service (IOC) is a licensed feature.

To view Compromised Hosts, you must turn on the UTM web filter of FortiGate devices and subscribe your FortiAnalyzer unit to FortiGuard to keep its local threat database synchronized with the FortiGuard threat database. See Subscribing FortiAnalyzer to FortiGuard.

Ref : https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/137635/viewing-compromised-hosts

Q51. 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.

Q52. Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)
* FortiAnalyzer HA can function without VRRP. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
* FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
* All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
* FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.
Reference:

FortiAnalyzer HA implementation works only in networks where Virtual Router Redundancy Protocol (VRRP) is permitted. Therefore it may not be supported by some public cloud infrastructures.

Q53. Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)
* A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.
* Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.
* Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.
* Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.
Reference:

Using FortiAnalyzer, you can enable log fetching. This allows FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer, which you can then run queries or reports on for forensic analysis.

The FortiAnalyzer device that fetches logs operates as the fetch client, and the other FortiAnalyzer device that sends logs operates as the fetch server. Log fetching can happen only between two FortiAnalyzer devices, and both of them must be running the same firmware version. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end.

FortiAnalyzer_7.0_Study_Guide-Online pag. 168

Q54. A playbook contains five tasks in total. An administrator runs the playbook and four out of five tasks finish successfully, but one task fails. What will be the status of the playbook after it is run?
* Running
* Failed
* Upstream_failed
* Success

Q55. The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device.

What can be the reason for this failure?
* FortiAnalyzer is in an HA cluster.
* ADOM mode should be set to advanced, in order to register the FortiClient EMS device.
* ADOMs are not enabled on FortiAnalyzer.
* A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.

Q56. Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)
* System information
* Logs from registered devices
* Report information
* Database snapshot
What does the System Configuration backup include?

System information, such as the device IP address and administrative user information.

Device list, such as any devices you configured to allow log access.

Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

FortiAnalyzer_7.0_Study_Guide-Online pag. 29

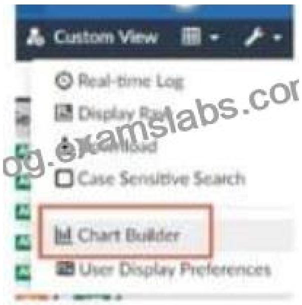
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 29: What does the System Configuration backup include?

* System information, such as the device IP address and administrative user information

* Device list, such as any devices you configured to allow log access

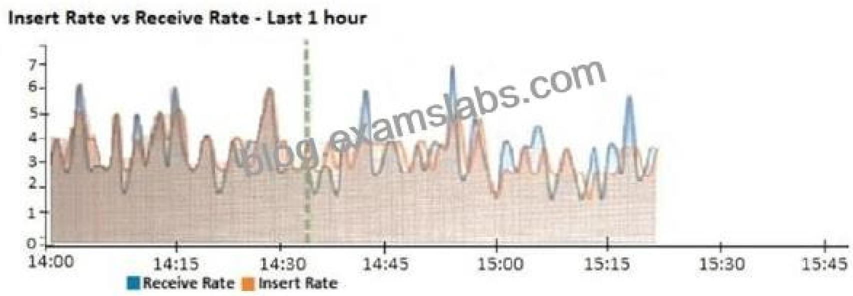
* Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

Q57. Refer to the exhibit.



What is the purpose of using the Chart Builder feature on FortiAnalyzer?
* In Log View, this feature allows you to build a dataset and chart automatically, based on the filtered search results.
* In Log View, this feature allows you to build a chart and chart automatically, on the top 100 log entries.
* This feature allows you to build a chart under FortiView.
* You can add charts to generated reports using this feature.

Q58. View the exhibit.



What does the data point at 14:35 tell you?
* FortiAnalyzer is dropping logs.
* FortiAnalyzer is indexing logs faster than logs are being received.
* FortiAnalyzer has temporarily stopped receiving logs so older logs&#8217; can be indexed.
* The sqlplugind daemon is ahead in indexing by one log.
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-widget

The Fortinet NSE 5 - FortiAnalyzer 7.2 Analyst certification exam covers a wide range of topics, including FortiAnalyzer deployment, configuration, management, and troubleshooting. It also covers topics such as data analysis, report generation, and event management. NSE5_FAZ-7.2 exam is designed to test the candidate's ability to work with FortiAnalyzer 7.2 in a real-world environment.

All NSE5_FAZ-7.2 Dumps and Fortinet NSE 5 - FortiAnalyzer 7.2 Analyst Training Courses:
https://www.examslabs.com/Fortinet/NSE-5-Network-Security-Analyst/best-NSE5_FAZ-7.2-exam-dumps.html]