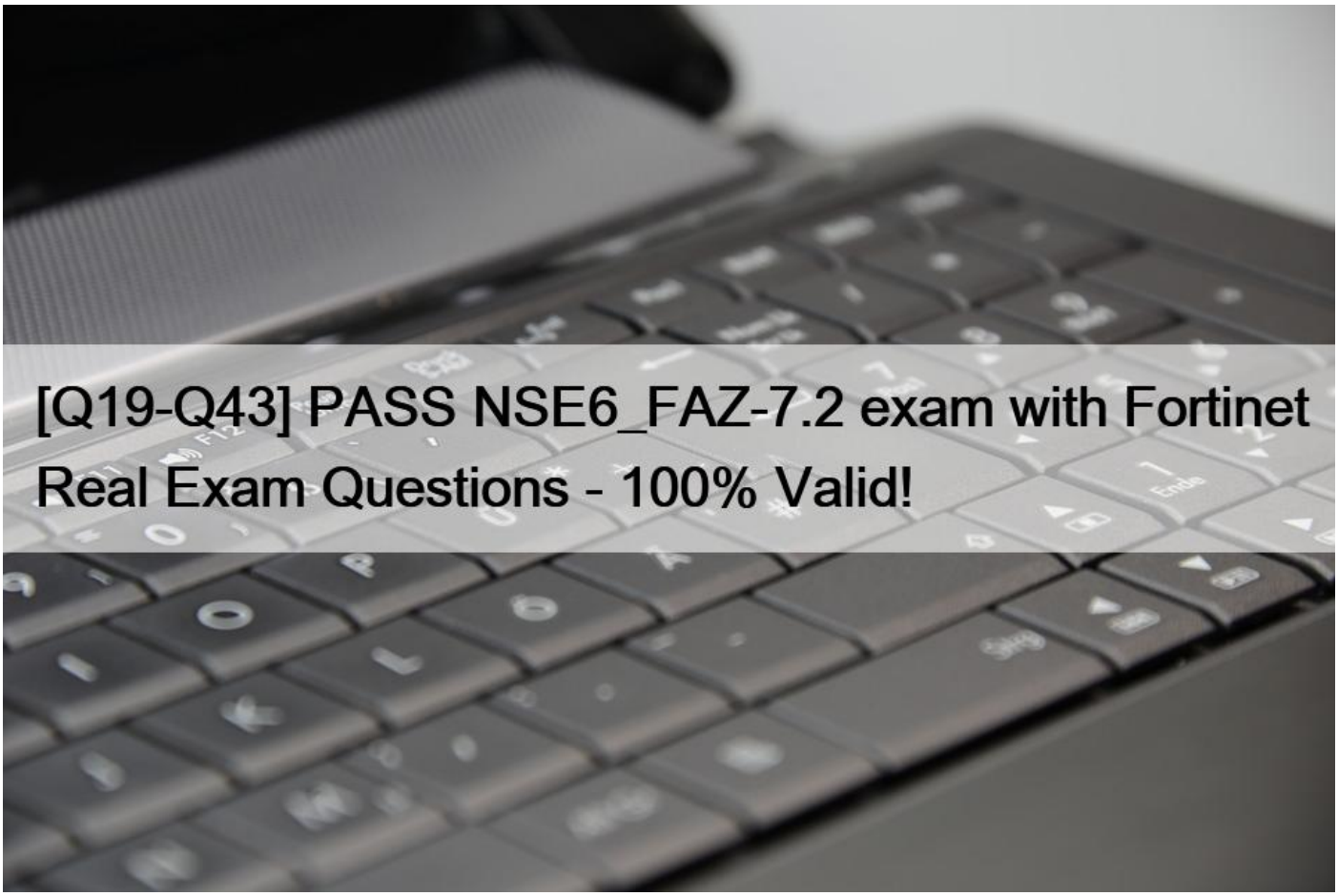
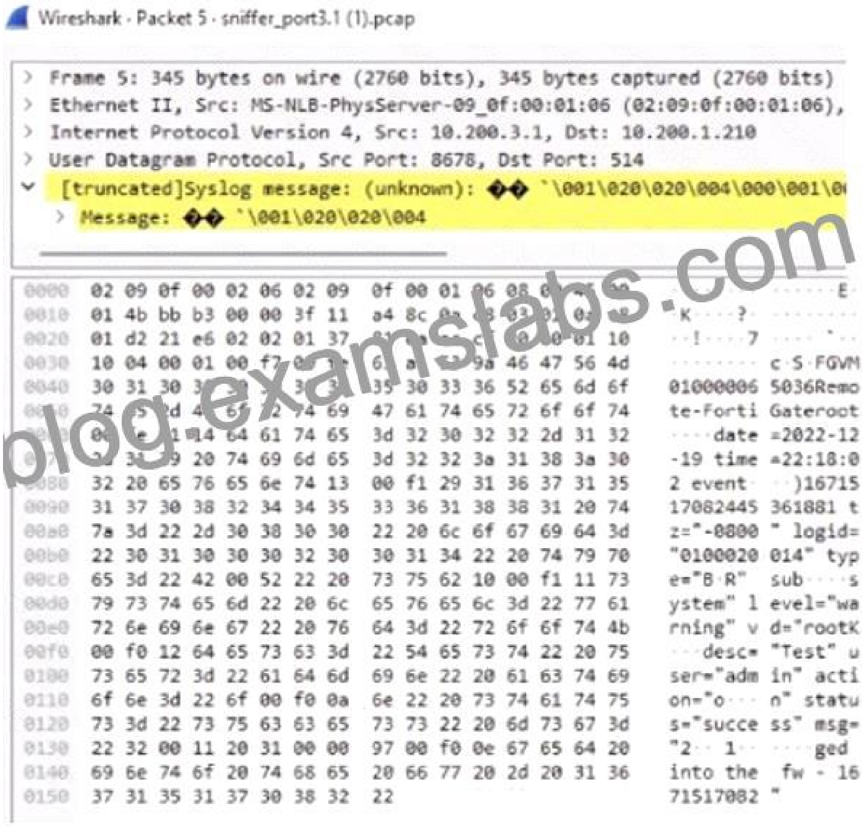
[Q19-Q43 PASS NSE6_FAZ-7.2 exam with Fortinet Real Exam Questions - 100% Valid!



PASS NSE6_FAZ-7.2 exam with Fortinet Real Exam Questions - 100% Valid!
Actual NSE6_FAZ-7.2 Exam Recently Updated Questions with Free Demo

NO.19 Refer to the exhibit.



Which image corresponds to the packet capture shown in the exhibit?

*


*


*


The exhibit shows a packet capture with a syslog message containing a log event from a FortiGate device. This log event includes several details such as the date, time, and event message. The corresponding image that matches this packet capture would be the one which shows that the FortiGate device has logs being received in real-time, as indicated by the highlighted section in the packet capture where it mentions “real-time”.

Therefore, Option A is the correct answer because it shows logs with “Real Time” status for the FortiGate-VM64 device, indicating that this FortiAnalyzer is currently receiving real-time logs from the device, matching the activity in the packet capture.References:Based on the provided exhibits and the real-time logging information, correlated with the knowledge from the FortiAnalyzer 7.2 Administrator documentation regarding log reception and device management.

NO.20 Refer to the exhibit.

Based on the partial outputs displayed in the exhibit, which devices are ready to be configured as peers in an HA cluster?

* FortiAnalyzer1 and FortiAnalyzer3
* FortiAnalyzer1 and FortiAnalyzer2
* These devices cannot participate in the same cluster.
* FortiAnalyzer2 and FortiAnalyzer3

Based on the provided exhibit, which shows partial outputs of the system status and global settings for FortiAnalyzer devices, the devices cannot be configured as peers in an HA (High Availability) cluster. This is indicated by the HA Mode status being set to ‘Stand Alone’ for the displayed FortiAnalyzer device. For devices to be part of an HA cluster, they would need to havecompatible HA configurations, and usually, they should not be in ‘Stand Alone’ mode. Additionally, the exhibit only shows information for one FortiAnalyzer, so it cannot be determined if there is another device ready to form an HA cluster with it.

NO.21 What is true about FortiAnalyzer reports?

* When you enable auto-cache, reports are scheduled by default.
* Reports can be saved in a CSV format.
* You require an output profile before reports are generated.
* The reports from one ADOM are available for all ADOMs.

For FortiAnalyzer reports, an output profile must be configured before reports can be generated and sent to an external server or system. This output profile determines how the reports are distributed, whether by email, uploaded to a server, or any other supported method. The options such as auto-cache, saving reports in CSV format, or reports availability across different ADOMs are separate features/settings and not directly related to the requirement of having an output profile for report generation.

NO.22 Which two statements are true regarding the log synchronization states for HA on FortiAnalyzer? (Choose two.)

* When Log Data Sync is turned on, the backup device reboots and then rebuilds the log database with the synchronized logs.
* By default. Log Data Sync is disabled on all backup devices.
* With Initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.

* Log Data Sync provides real-time log synchronization to all backup devices.

For HA on FortiAnalyzer, Log Data Sync ensures real-time log synchronization among all cluster members, including backup devices. This feature is enabled by default. The Initial Logs Sync state is triggered when a new unit is added to an HA cluster, where the primary unit synchronizes its logs with the newly added unit.

After the initial synchronization, the secondary unit reboots and rebuilds its log database with the synchronized logs.References:FortiAnalyzer 7.2 Administrator Guide, “Log synchronization” section.

NO.23 Which statement is true about using aggregation mode on FortiAnalyzer?

* Aggregation mode supports log filters.
* Aggregation mode can work with syslog servers.
* In aggregation mode, logs and content files are forwarded in real time.
* Aggregation mode can be configured only on the CLI.

In aggregation mode, FortiAnalyzer stores logs received from devices and forwards them at a specified time each day to avoid duplication. It is specifically designed to work between two FortiAnalyzer units and does not support syslog or CEF servers. Additionally, aggregation mode configurations are limited to CLI commandslog-forwardandlog-forward-service.References:FortiAnalyzer 7.2 Administrator Guide,

“Aggregation” and “CLI Commands for Aggregation Mode” sections.

NO.24 After you have moved a registered logging device out of one ADOM and into a new ADOM, you run the following command: execute sql-local rebuild-adom <new-ADOM-name> What is the purpose of running this CLI command?

* To reset the ADOM disk quota enforcement to its default value
* 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
* To remove the analytics logs of the device from the old database

When you move a registered logging device from one ADOM (Administrative Domain) to another in FortiAnalyzer, it’s essential to ensure that the analytical logs for the moved device are available in the new ADOM to maintain continuity in reporting and log analysis. The commandexecute sql-local rebuild-adom < new-ADOM-name>is used specifically for this purpose. Running this command populates the new ADOM with the analytical logs of the moved device, enabling you to generate accurate and comprehensive reports based on the historical data of the device in its new ADOM context. This process ensures that the transition of devices between ADOMs does not lead to a loss of analytical insight or reporting capabilities for the device’s traffic and events.

NO.25 What areanalytics logs on FortiAnalyzer?

* Logs that are compressed and saved to a log file
* Logs that roll over when the log file reaches a specific size
* Logs thatare indexed and stored in the SQL
* Logs classified as type Traffic, or type Security

On FortiAnalyzer, analytics logs refer to the logs that have been processed, indexed, and then stored in the SQL database. This process allows for efficient data retrieval and analytics. Unlike basic log storage, which might involve simple compression and storage in a file system, analytics logs in FortiAnalyzer undergo an indexing process. This enables advanced features such as quick search, report generation, and detailed analysis, making it easier for administrators to gain insights into network activities and security incidents.References:FortiAnalyzer 7.2 Administrator Guide – “Log Management” and “Data Analytics” sections.

NO.26 Which two statements are true regarding FortiAnalyzer system backups? (Choose two.)

* Existing reports can be included in the backup files.
* The system reserves at least 5% to 20% disk space for backup files.
* Scheduled system backups can be configured only from the CLI.

* Backup files can be uploaded to SCP and SFTP servers.

FortiAnalyzer allows for the inclusion of existing reports in the backup files, providing a comprehensive backup of configurations and data. Additionally, the backup files can be configured to be uploaded to SCP and SFTP servers, ensuring secure transfer and offsite storage of backup data. This can be configured both in the GUI and the CLI, providing flexibility in how backups are scheduled and managed.References:FortiAnalyzer

7.4.1 Administration Guide, “Scheduling automatic backups” section.

NO.27 An administrator, fortinet, can view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mail server that can be used to send alert emails.

What can be the problem?

* ADOM mode is configured with Advanced mode.
* fortinet is assigned the Standard_User administrative profile.
* A trusted host is configured.
* fortinet is assigned Restricted_User administrative profile.

If the administrator “fortinet” can view logs and perform device management tasks but cannot create a mail server for alert emails, it is likely due to the administrative profile assigned to them. The Standard_User administrative profile may restrict certain administrative functions, such as creating mail servers. To perform all administrative tasks, including creating mail servers, a higher privilege profile, such as Super_Admin, might be required.References:FortiAnalyzer 7.2 Administrator Guide, “Mail Server” section.

NO.28 Which statement is true about ADOMs?

* When a FortiAnalyzer Fabric is implemented, the default ADOM mode is set to advanced.
* A fabric ADOM can include all the device types supported by FortiAnalyzer.
* You can change the ADOM mode only through the GUI.
* In normal mode, you cannot change the disk quota of the ADOM after its creation.

Regarding ADOMs (Administrative Domains) in FortiAnalyzer, a fabric ADOM is capable of including all device types that FortiAnalyzer supports. This is part of the flexibility offered by ADOMs to manage and report on logs from various devices within a Fortinet security fabric. ADOMs can be enabled to support non-FortiGate devices as well, and the root ADOM in Fabric ADOMs provides visibility into all Security Fabric devices. Additionally, it should be noted that in normal mode, you cannot assign different FortiGate VDOMs to different ADOMs, while in advanced mode, you can, which provides a more granular control over the log data from individual VDOMs.References:FortiAnalyzer 7.4.1 Administration Guide, “ADOMs” and

“ADOM device modes” sections.

NO.29 Which two statements about FortiAnalyzer operating modes are true? (Choose two.)

* When in collector mode. FortiAnalyzer offloads the log receiving task to the analyzer.
* Analyzer mode is the default operating mode.
* For the collector, you should allocate most of the disk space to analytics logs.
* When in analyzer mode. FortiAnalyzer supports event management and reporting features.

The default operating mode for FortiAnalyzer is analyzer mode. In this mode, FortiAnalyzer provides full functionality for event management and reporting features. This mode is intended for environments where comprehensive analysis and reporting are required. It allows FortiAnalyzer to collect, analyze, and store logs, as well as generate reports and manage events.References:FortiAnalyzer 7.4.1 Administration Guide,

“Operating modes” section.

NO.30 Which two of the available registration methods place the device automatically in its assigned ADOM?

(Choose two.)
* Request from the device
* Serial number
* Fabric Authorization
* Pre-shared key

The registration methods that automatically place a device in its assigned ADOM are using the serial number and fabric authorization. When devices are added to FortiAnalyzer using these methods, they are automatically placed in the appropriate ADOM, which could be a defaultADOM based on the device type or a predefined ADOM based on the serial number or fabric authorization. This simplifies the management of devices and their logs by organizing them into their respective ADOMs from the moment they are registered.References:FortiAnalyzer 7.4.1 Administration Guide, “Default device type ADOMs” and

“Assigning devices to an ADOM” sections.

NO.31 Which two methods can you use to restrict administrative access on FortiAnalyzer? (Choose two.)
* Use administrator profiles.
* Configure trusted hosts.
* Fabric connectors to external LDAP servers.
* Limit access to specific virtual domains.

To restrict administrative access on FortiAnalyzer, two effective methods are using administrator profiles and configuring trusted hosts. Administrator profiles allow for defining the level of access and permissions for different administrators, controlling what each administrator can seeand do within the FortiAnalyzer unit.

Configuring trusted hosts enhances security by limiting administrative access to specified IP addresses, ensuring that administrators can only connect from approved locations or networks, thus preventing unauthorized access from outside specified subnets or IP addresses.References:FortiAnalyzer 7.4.1 Administration Guide, “Administrators” and “Trusted hosts” sections.