Fortinet

Exam Questions NSE5_FAZ-7.2

Fortinet NSE 5 - FortiAnalyzer 7.2

NEW QUESTION 1
Which SQL query is in the correct order to query the database in the FortiAnslyzer?

A. SELECT devid FROM Slog GROOP BY devid WHERE * user' =* USERI'
B. SELECT devid WHERE 'u3er'='USERI' FROM $ log GROUP BY devid
C. SELECT devid FROM Slog- WHERE *user' =' USERI' GROUP BY devid
D. FROM Slog WHERE 'user* =' USERI' SELECT devid GROUP BY devid

Answer: C

Explanation:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 259: The main clauses FortiAnalyzer reports use are as follows:
•FROM
•WHERE
•GROUP BY
•ORDER BY
• LIMIT
• OFFSET
Accordingly, following the SELECT keyword, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide.

NEW QUESTION 2
What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

A. Chart Builder
B. Export to Report Chart
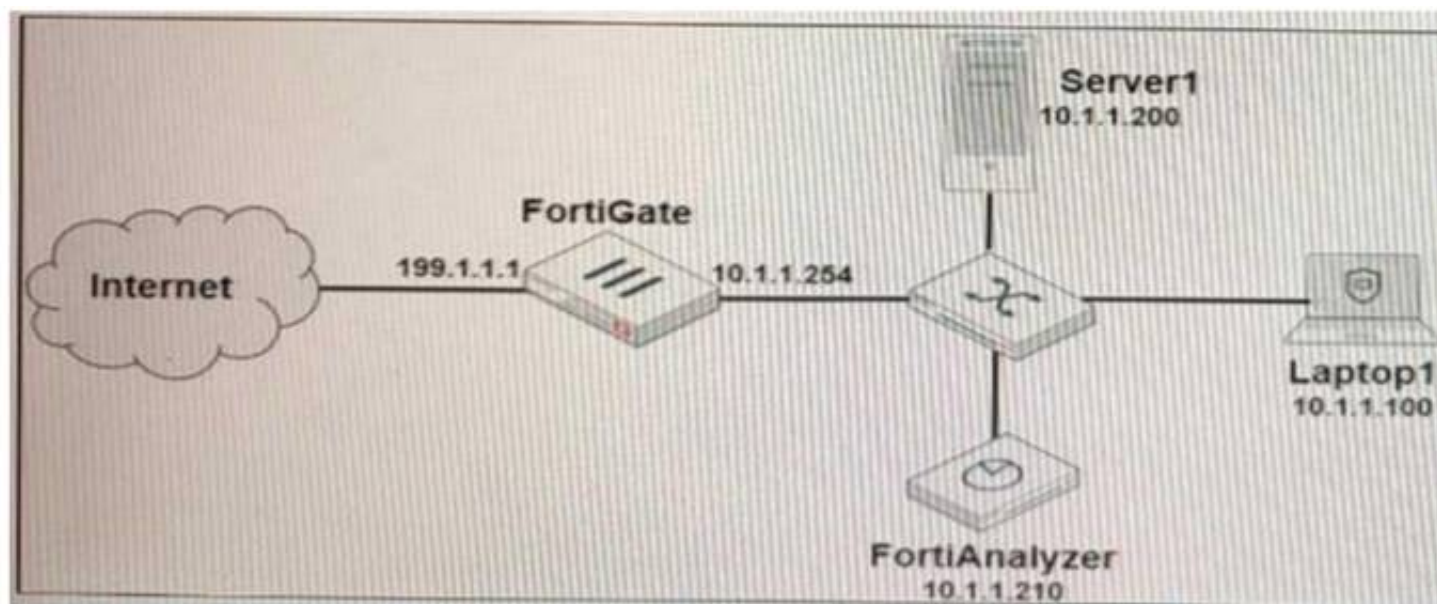C. Dataset Library
D. Custom View

Answer: B

NEW QUESTION 3
When working with FortiAnalyzer reports, what is the purpose of a dataset?

A. To provide the layout used for reports
B. To define the chart type to be used
C. To retrieve data from the database
D. To set the data included in templates

Answer: C

NEW QUESTION 4
Refer to the exhibit.

Laptopt is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin" and coming from Laptop1:
Which filter will achieve the desired result?

A. operation-login & performed_on=="GUI(10.1.1.100)" & user!=admin
B. operation-login & srcip==10.1.1.100 & dstip==10.1.1.210 & user==admin
C. operation-login & dstip==10.1.1.210 & userl-admin
D. operation-login & performed_on=="GUI(10.1.1.210)' & user!=admin

Answer: A

Explanation:
On there the task was to create a filter for failed logins from any other location but the local computer: "Add the text performed_on!~10.0.1.10. This includes any attempts coming from devices with an IP address that is not the one configured on the Local-Client computer."

NEW QUESTION 5

A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed by that rogue administrator on FortiAnalyzer.
What can you do on FortiAnalyzer to accomplish this?

A. Click FortiView and generate a report for that administrator.
B. Click Task Monitor and view the tasks performed by that administrator.
C. Click Log View and generate a report for that administrator.
D. View the tasks performed by the rogue administrator in Fabric View.

Answer: B

NEW QUESTION 6
What is the purpose of using prefilters when configuring event handlers?

A. They limit which logs are checked for matches by the other filters.
B. They can filter the logs before they are processed by FortiAnalyzer
C. They download new filters to be used in event handlers.
D. They are common filters applied simultaneously to all event handlers.

Answer: A

NEW QUESTION 7
Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with SSL? (Choose two.)

A. SSL is the default setting.
B. SSL communications are auto-negotiated between the two devices.
C. SSL can send logs in real-time only.
D. SSL encryption levels are globally set on FortiAnalyzer.
E. FortiAnalyzer encryption level must be equal to, or higher than, FortiGate.

Answer: AD

NEW QUESTION 8
What must you consider when using log fetching? (Choose two.)

A. The fetch client can retrieve logs from devices that are not added to its local Device Manager
B. You can use filters to include only logs from a single device.
C. The fetching profile must include a user with the Super_User profile.
D. The archive logs retrieved from the server become archive logs in the client.

Answer: BC

NEW QUESTION 9
What are offline logs on FortiAnalyzer?

A. Compressed logs, which are also known as archive logs, are considered to be offline logs.
B. When you restart FortiAnalyze
C. all stored logs are considered to be offline logs.
D. Logs that are indexed and stored in the SQL database.
E. Logs that are collected from offline devices after they boot up.
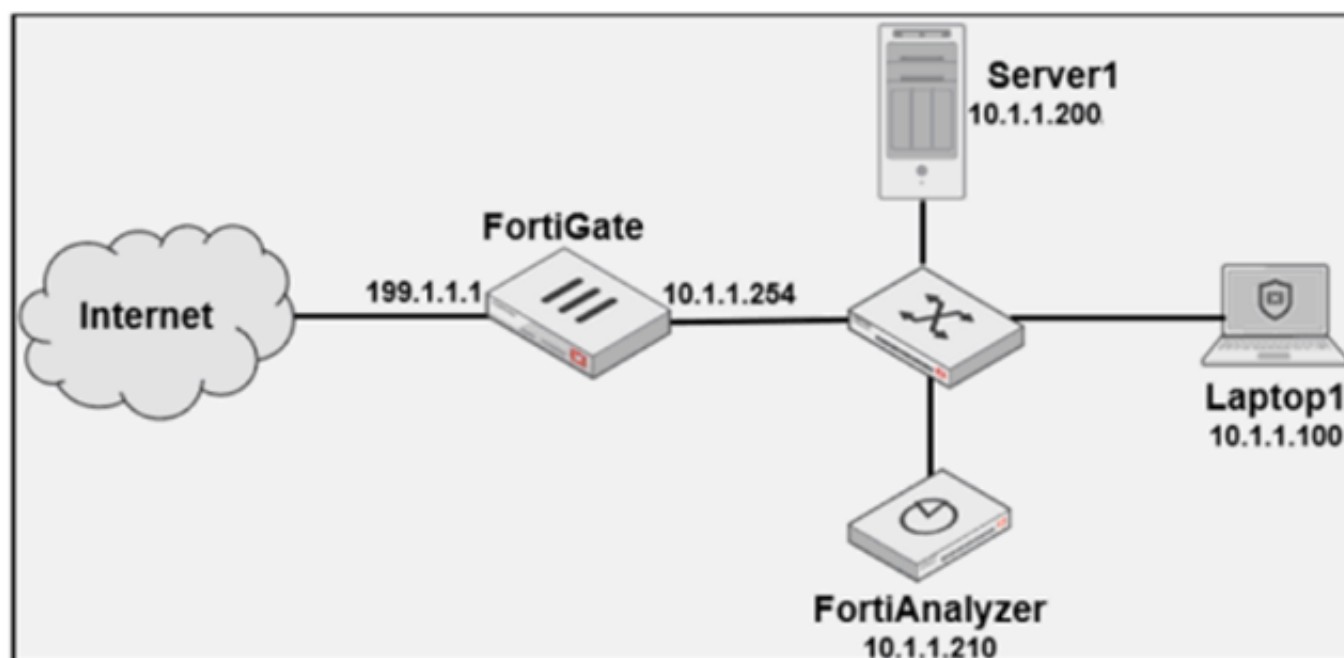
Answer: A

NEW QUESTION 10
Which item must you configure on FortiAnalyzer to email generated reports automatically?

A. Output profile
B. Report scheduling
C. SFTP server
D. SNMP server

Answer: A

NEW QUESTION 10
Refer to the exhibit.

Laptop1 is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin", and coming from Laptop1.
Which filter will achieve the desired result?

A. operation-login & dstip==10.1.1.210 & user!-admin
B. operation-login & srcip==10.1.1.100 & dstip==10.1.1.210 & user==admin
C. operation-login & performed_on=="GUI(10.1.1.210)" & user!=admin
D. operation-login & performed_on=="GUI(10.1.1.100)" & user!=admin

Answer: D

NEW QUESTION 15
An administrator has moved FortiGate A from the root ADOM to ADOM1. Which two statements are true regarding logs? (Choose two.)

A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.
B. Archived logs will be moved to ADOM1 from the root ADOM automatically.
C. Logs will be presented in both ADOMs immediately after the move.
D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the ADOM1 SQL database.

Answer: BD

NEW QUESTION 17
How can you configure FortiAnalyzer to permit administrator logins from only specific locations?

A. Use static routes
B. Use administrative profiles
C. Use trusted hosts
D. Use secure protocols

Answer: C

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/186508/trusted-hosts

NEW QUESTION 18
Which two statements are true regarding the outbreak detection service? (Choose two.)

A. New alerts are received by email.
B. Outbreak alerts are available on the root ADOM only.
C. An additional license is required.
D. It automatically downloads new event handlers and reports.

Answer: CD

NEW QUESTION 23
Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two.)

A. Both modes, forwarding and aggregation, support encryption of logs between devices.
B. In aggregation mode, you can forward logs to syslog and CEF servers as well.
C. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
D. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.

Answer: AC

Explanation:
A) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 148: The log communication between devices can be protected by encryption, with the desired encryption level, using the commands shown on the slide. (You need to interpret this. "Real time" and "aggregation" is about the "moment" when Fortigate sends the logs. However, no matter the moment, Fortigate will upload logs encrypted or unencrypted based on previous / differente config).
C) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 147: Aggregation: Logs and content files stored and uploaded at scheduled time.

NEW QUESTION 24
What are two advantages of setting up fabric ADOM? (Choose two.)

A. It can be used for fast data processing and log correlation
B. It can be used to facilitate communication between devices in same Security Fabric
C. It can include all Fortinet devices that are part of the same Security Fabric
D. It can include only FortiGate devices that are part of the same Security Fabric

Answer: AC

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-a

NEW QUESTION 27
What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

A. The log file is stored as a raw log and is available for analytic support.
B. The log file rolls over and is archived.
C. The log file is purged from the database.
D. The log file is overwritten.

Answer: B

NEW QUESTION 32
For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

A. Principal
B. Service provider
C. Identity collector
D. Identity provider

Answer: BD

NEW QUESTION 35
In the FortiAnalyzer FortiView, source and destination IP addresses from FortiGate devices are not resolving to a hostname.
How can you resolve the source and destination IP addresses, without introducing any additional performance impact to FortiAnalyzer?

A. Resolve IP addresses on a per-ADOM basis to reduce delay on FortiView while IPs resolve
B. Configure # set resolve-ip enable in the system FortiView settings
C. Configure local DNS servers on FortiAnalyzer
D. Resolve IP addresses on FortiGate

Answer: D

Explanation:

https://packetplant.com/fortigate-and-fortianalyzer-resolve-source-and-destination-ip/
"As a best practice, it is recommended to resolve IPs on the FortiGate end. This is because you get both source and destination, and it offloads the work from FortiAnalyzer. On FortiAnalyzer, this IP resolution does destination IPs only"

NEW QUESTION 40
What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

A. Hot swap the disk.
B. There is no need to do anything because the disk will self-recover.
C. Run execute format disk to format and restart the FortiAnalyzer device.
D. Shut down FortiAnalyzer and replace the disk

Answer: A

Explanation:

https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/0700_RAID/0800_Swapping%20Disks.htm#:~:text=If

NEW QUESTION 41
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: AD

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 43
What is Log Insert Lag Time on FortiAnalyzer?

A. The number of times in the logs where end users experienced slowness while accessing resources.
B. The amount of lag time that occurs when the administrator is rebuilding the ADOM database.
C. The amount of time that passes between the time a log was received and when it was indexed on FortiAnalyzer.
D. The amount of time FortiAnalyzer takes to receive logs from a registered device

Answer: C

NEW QUESTION 47
Which two statement are true regardless initial Logs sync and Log Data Sync for Ha on FortiAnalyzer?

A. By default, Log Data Sync is disabled on all backup devise.
B. Log Data Sync provides real-time log synchronization to all backup devices.
C. With initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.
D. When Logs Data Sync is turned on, the backup device will reboot and then rebuilt the log database with the synchronized logs.

Answer: CD

NEW QUESTION 48
Which statement about the FortiSOAR management extension is correct?

A. It requires a FortiManager configured to manage FortiGate
B. It requires a dedicated FortiSOAR device or VM.
C. It does not include a limited trial by default.
D. It runs as a docker container on FortiAnalyzer

Answer: D

NEW QUESTION 49
On FortiAnalyzer, what is a wildcard administrator account?

A. An account that permits access to members of an LDAP group
B. An account that allows guest access with read-only privileges
C. An account that requires two-factor authentication
D. An account that validates against any user account on a FortiAuthenticator

Answer: A

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

NEW QUESTION 53
Logs are being deleted from one of your ADOMs earlier that the configured setting for archiving in your data policy. What is the most likely problem?

A. The total disk space is insufficient and you need to add other disk.
B. CPU resources are too high.
C. The ADOM disk quota is set too low based on log rates.
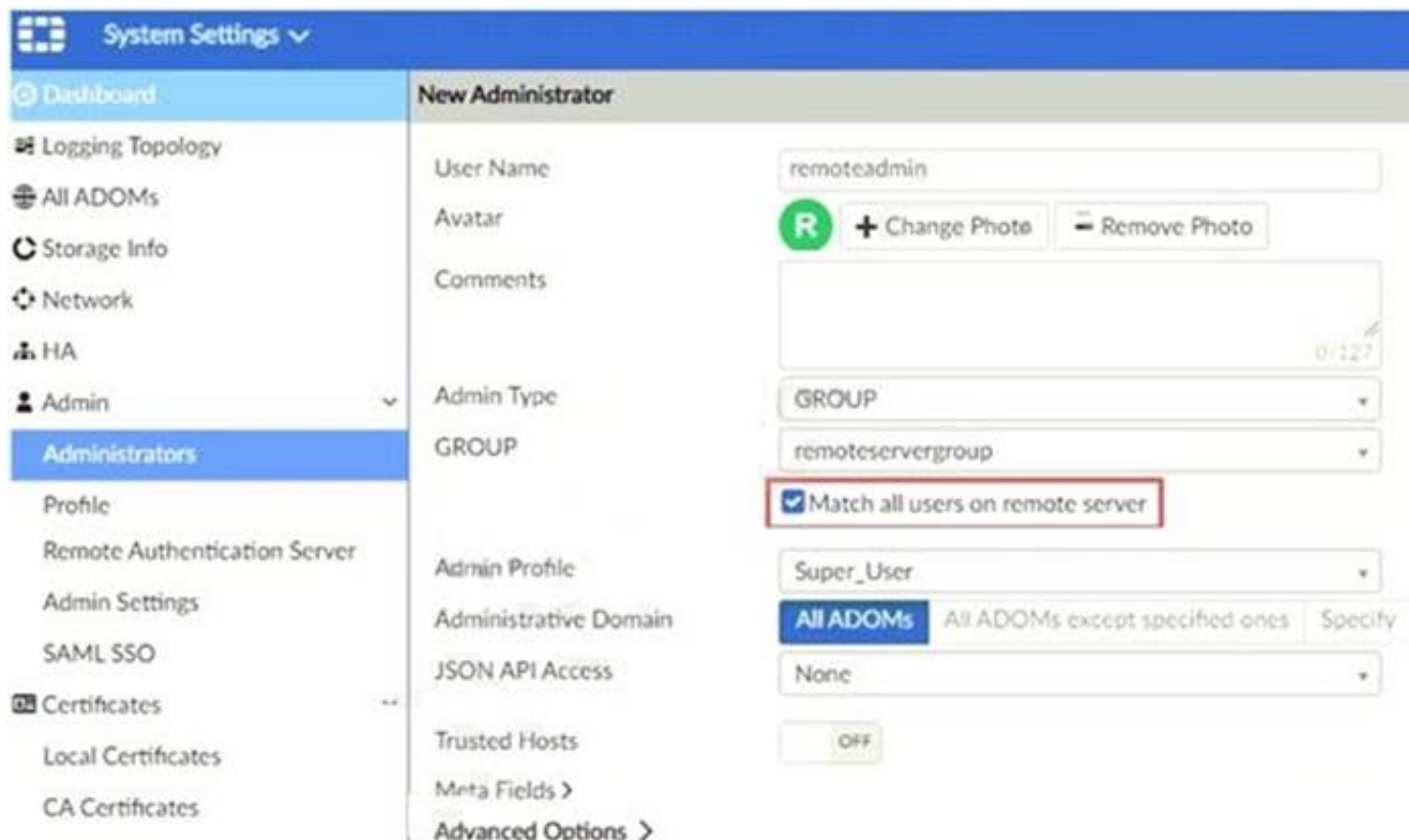D. Logs in that ADOM are being forwarded in real-time to another FortiAnalyzer device.

Answer: C

Explanation:
https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG FAZ/1100_Storage/0017_Deleted%20device%20logs.htm
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automatic-deletion

NEW QUESTION 55
Refer to the exhibit.

The exhibit shows "remoteservergroup" is an authentication server group with LDAP and RADIUS servers. Which two statements express the significance of enabling "Match all users on remote server" when
configuring a new administrator? (Choose two.)

A. It creates a wildcard administrator using LDAP and RADIUS servers.
B. Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.
C. Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at anytime.
D. It allows administrators to use two-factor authentication.

Answer: AB

NEW QUESTION 60
Which two statements about log forwarding are true? (Choose two.)

A. Forwarded logs cannot be filtered to match specific criteria.
B. Logs are forwarded in real-time only.
C. The client retains a local copy of the logs after forwarding.
D. You can use aggregation mode only with another FortiAnalyzer.

Answer: CD

Explanation:
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

NEW QUESTION 65
What is the purpose of trigger variables?

A. To display statistics about the playbook runtime
B. To use information from the trigger to filter the action in a task
C. To provide the trigger information to make the playbook start running
D. To store the start times of playbooks with On_Schedule triggers

Answer: B

NEW QUESTION 67
What can you do on FortiAnalyzer to restrict administrative access from specific locations?

A. Configure trusted hosts for that administrator.
B. Enable geo-location services on accessible interface.
C. Configure two-factor authentication with a remote RADIUS server.
D. Configure an ADOM for respective location.

Answer: A

NEW QUESTION 72
Which statement is true regarding Macros on FortiAnalyzer?

A. Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.
B. Macros are supported only on the FortiGate ADOM.
C. Macros are useful in generating excel log files automatically based on the reports settings.
D. Macros are predefined templates for reports and cannot be customized.

Answer: A

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

NEW QUESTION 74
Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)

A. 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.
B. Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.
C. Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.
D. 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.

Answer: BD

NEW QUESTION 77
What is the purpose of a predefined template on the FortiAnalyzer?

A. It can be edited and modified as required
B. It specifies the report layout which contains predefined texts, charts, and macros
C. It specifies report settings which contains time period, device selection, and schedule
D. It contains predefined data to generate mock reports

Answer: B

NEW QUESTION 78
Refer to the exhibit.
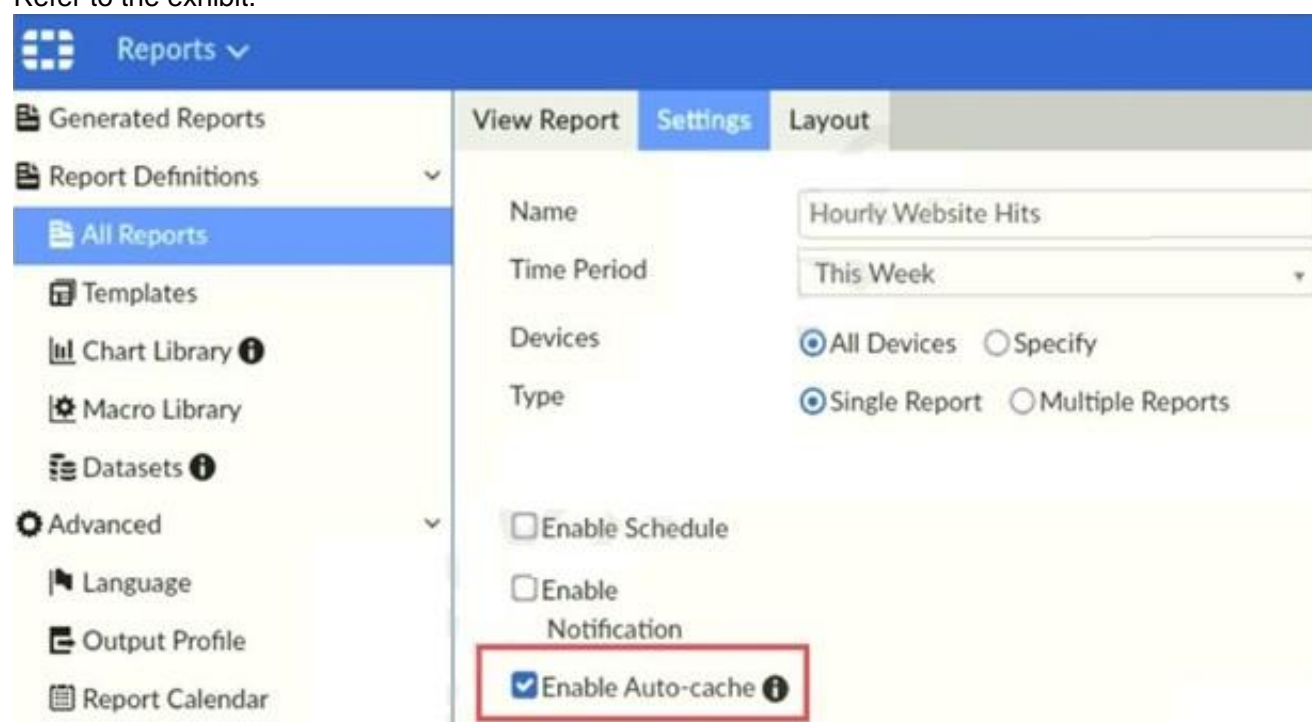
Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)

A. Report size will be optimized to conserve disk space on FortiAnalyzer.
B. Reports will be cached in the memory.
C. This feature is automatically enabled for scheduled reports.
D. Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

Answer: CD

Explanation:
"Enable auto-cache in the report settings to boost the reporting performance and reduce report generation time. Scheduled reports have auto-cache enabled already."
FortiAnalyzer_7.0_Study_Guide-Online page 306

NEW QUESTION 83
Which daemon is responsible for enforcing raw log file size?

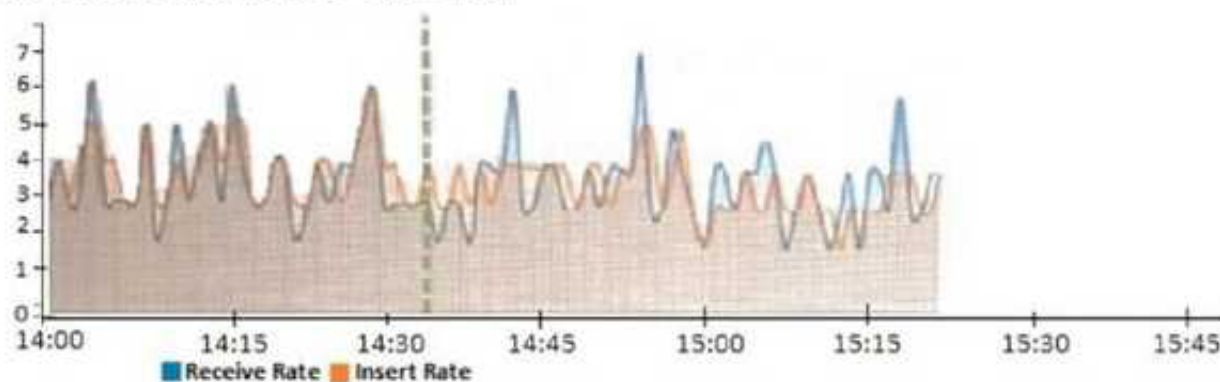A. logfiled
B. oftpd
C. sqlplugind
D. miglogd

Answer: A

NEW QUESTION 85
View the exhibit.

Insert Rate vs Receive Rate - Last 1 hour

What does the data point at 14:35 tell you?

A. FortiAnalyzer is dropping logs.
B. FortiAnalyzer is indexing logs faster than logs are being received.
C. FortiAnalyzer has temporarily stopped receiving logs so older logs' can be indexed.
D. The sqlplugind daemon is ahead in indexing by one log.

Answer: B

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-wi

NEW QUESTION 89
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. Shut down FortiAnalyzer and then replace the disk
B. Downgrade your RAID level, replace the disk, and then upgrade your RAID level
C. Clear all RAID alarms and replace the disk while FortiAnalyzer is still running
D. Perform a hot swap

Answer: A

Explanation:

supports hot swapping on hardware RAID only, so it is recommended that on FortiAnalyzer devices with software RAID you should shutdown FortiAnalyzer prior to exchanging the hard disk.

https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta-

NEW QUESTION 92
A play book contains five tasks in total. An administrator executed the playbook and four out of five tasks finished successfully, but one task failed. What will be the status of the playbook after its execution?

A. Success
B. Failed
C. Running
D. Upstream_failed

Answer: B

Explanation:
Playbook jobs that include one or more failed tasks are labeled as Failed in Playbook Monitor. FortiAnalyzer_7.0_Study Guide page No: 247
Playbook jobs that include one or more failed tasks are labeled as Failed in Playbook Monitor. A failed status, however, does not mean that all tasks failed. Some individual actions may have been completed successfully.

NEW QUESTION 95
Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

A. License type
B. Disk size
C. Total quota
D. RAID level

Answer: BD

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

NEW QUESTION 96
Consider the CLI command:

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

What is the purpose of the command?

A. To add a unique tag to each log to prove that it came from this FortiAnalyzer
B. To add the MD5 hash value and authentication code
C. To add a log file checksum
D. To encrypt log communications

Answer: C

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/849211/global

NEW QUESTION 97
On the RAID management page, the disk status is listed as Initializing.
What does the status Initializing indicate about what the FortiAnalyzer is currently doing?

A. FortiAnalyzer is ensuring that the parity data of a redundant drive is valid
B. FortiAnalyzer is writing data to a newly added hard drive to restore it to an optimal state
C. FortiAnalyzer is writing to all of its hard drives to make the array fault tolerant
D. FortiAnalyzer is functioning normally

Answer: C

NEW QUESTION 102
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?

A. Running
B. Failed
C. Upstream_failed
D. Success

Answer: B

NEW QUESTION 105
Which two statements are true regarding fabric connectors? (Choose two.)

A. Configuring fabric connectors to send notification to ITSM platform upon incident creation Is more efficient than third-party information from the FortiAnalyzer API.
B. Fabric connectors allow to save storage costs and improve redundancy.
C. Storage connector service does not require a separate license to send logs to cloud platform.
D. Cloud-Out connections allow you to send real-time logs to pubic cloud accounts like Amazon S3, Azure Blob , and Google Cloud.

Answer: AD

NEW QUESTION 106
View the exhibit.


```
Total Quota Summary:
        Total Quota      Allocated    Available    Allocate%
         63.7GB            12.7GB        51.0GB         19.9%

System Storage Summary:
        Total      Used        Available        Use%
        78.7GB     2.9GB          75.9GB         3.6%

Reserved space: 15.0GB (19.0% of total space).
```

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

A. 3.6% of the system storage is already being used.
B. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files
C. The oftpd process has not archived the logs yet
D. The logfiled process is just estimating the total quota

Answer: B

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

NEW QUESTION 111
Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

A. System information
B. Logs from registered devices
C. Report information
D. Database snapshot

Answer: AC

Explanation:
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.

NEW QUESTION 112
Which two methods can you use to send event notifications when an event occurs that matches a configured event handler? (Choose two.)

A. SMS
B. Email
C. SNMP
D. IM

Answer: BC

NEW QUESTION 113
What statements are true regarding FortiAnalyzer 's treatment of high availability (HA) dusters? (Choose two)

A. FortiAnalyzer distinguishes different devices by their serial number.
B. FortiAnalyzer receives logs from d devices in a duster.
C. FortiAnalyzer receives bgs only from the primary device in the cluster.
D. FortiAnalyzer only needs to know (he serial number of the primary device in the cluster-it automaticaly discovers the other devices.

Answer: AB

NEW QUESTION 118
What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

A. The size of newly generated reports is optimized to conserve disk space.
B. FortiAnalyzer local cache is used to store generated reports.
C. When new logs are received, the hard-cache data is updated automatically.
D. The generation time for reports is decreased.

Answer: CD

NEW QUESTION 120
What is the recommended method of expanding disk space on a FortiAnalyzer VM?

A. From the VM host manager, add an additional virtual disk and use the #execute lvm extend <disk number> command to expand the storage
B. From the VM host manager, expand the size of the existing virtual disk
C. From the VM host manager, expand the size of the existing virtual disk and use the # execute format disk command to reformat the disk
D. From the VM host manager, add an additional virtual disk and rebuild your RAID array

Answer: A

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD40848

NEW QUESTION 124
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 each device in the ADOM
B. The maximum disk utilization for the FortiAnalyzer model
C. The maximum disk utilization for the ADOM type
D. The maximum disk utilization for all devices in the ADOM

Answer: D

NEW QUESTION 126
An administrator has configured the following settings: config system fortiview settings
set resolve-ip enable end
What is the significance of executing this command?

A. Use this command only if the source IP addresses are not resolved on FortiGate.
B. It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.
C. You must configure local DNS servers on FortiGate for this command to resolve IP addresses on Forti Analyzer.
D. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

Answer: D

NEW QUESTION 128
Refer to the exhibit.

Which statement is correct regarding the event displayed?

A. The security risk was blocked or dropped.
B. The security event risk is considered open.
C. An incident was created from this event.
D. The risk source is isolated.

Answer: A

Explanation:
Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not.
The possible statuses are:
Unhandled: The security event risk is not mitigated or contained, so it is considered open. Contained: The risk source is isolated.
Mitigated: The security risk is mitigated by being blocked or dropped. (Blank): Other scenarios.
FortiAnalyzer_7.0_Study_Guide-Online pag. 206

NEW QUESTION 129
When you perform a system backup, what does the backup configuration contain? (Choose two.)

A. Generated reports
B. Device list
C. Authorized devices logs
D. System information

Answer: BD

Explanation:
https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400_execute/backup.htm

NEW QUESTION 130
Which statements are correct regarding FortiAnalyzer reports? (Choose two)

A. FortiAnalyzer provides the ability to create custom reports.
B. FortiAnalyzer glows you to schedule reports to run.
C. FortiAnalyzer includes pre-defined reports only.
D. FortiAnalyzer allows reporting for FortiGate devices only.

Answer: AB

NEW QUESTION 134
Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?

A. Log upload
B. Indicators of Compromise
C. Log forwarding an aggregation mode
D. Log fetching

Answer: D

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetcher-management

NEW QUESTION 139
What does the disk status Degraded mean for RAID management?

A. One or more drives are missing from the FortiAnalyzer uni
B. The drive is no longer available to the operating system.
C. The FortiAnalyzer device is writing to all the hard drives on the device in order to make the array fault tolerant.
D. The FortiAnalyzer device is writing data to a newly added hard drive in order to restore the hard drive to an optimal state.
E. The hard driveIs no longer being used by the RAID controller

Answer: D

NEW QUESTION 141
Which two statements are correct regarding the export and import of playbooks? (Choose two.)

A. You can export only one playbook at a time.
B. You can import a playbook even if there is another one with the same name in the destination.
C. Playbooks can be exported and imported only within the same FortiAnaryzer.
D. A playbook that was disabled when it was exported, will be disabled when it is imported.

Answer: BD

Explanation:
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.

NEW QUESTION 143
What are analytics logs on FortiAnalyzer?

A. Log type Traffic logs.
B. Logs that roll over when the log file reaches a specific size.
C. Logs that are indexed and stored in the SQL.
D. Raw logs that are compressed and saved to a log file.

Answer: C

NEW QUESTION 147
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. Quota enforcement is acting on analytical data before a report is complete
B. Logs are rolling before the report is run
C. CPU resources are too high
D. Disk utilization for archive logs is set for 15 days

Answer: B

NEW QUESTION 151
In FortiAnalyzer's FormView, source and destination IP addresses from FortiGate devices are not resolving to a hostname. How can you resolve the source and destination IPs, without introducing any additional performance impact to FortiAnalyzer?

A. Configure local DNS servers on FortiAnalyzer
B. Resolve IPs on FortiGate
C. Configure # set resolve-ip enable in the system FortiView settings
D. Resolve IPs on a per-ADOM basis to reduce delay on FortiView while IPs resolve

Answer: B

NEW QUESTION 156
Refer to the exhibit.
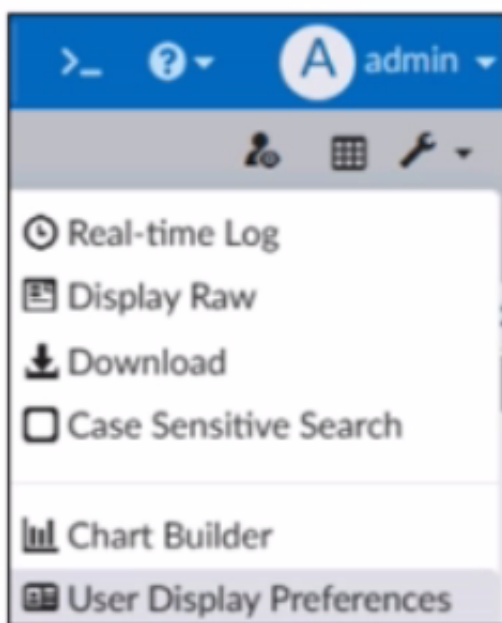
What is the purpose of using the Chart Builder feature on FortiAnalyzer?

A. To add a new chart under FortiView to be used in new reports
B. To build a dataset and chart automatically, based on the filtered search results
C. To add charts directly to generate reports in the current ADOM
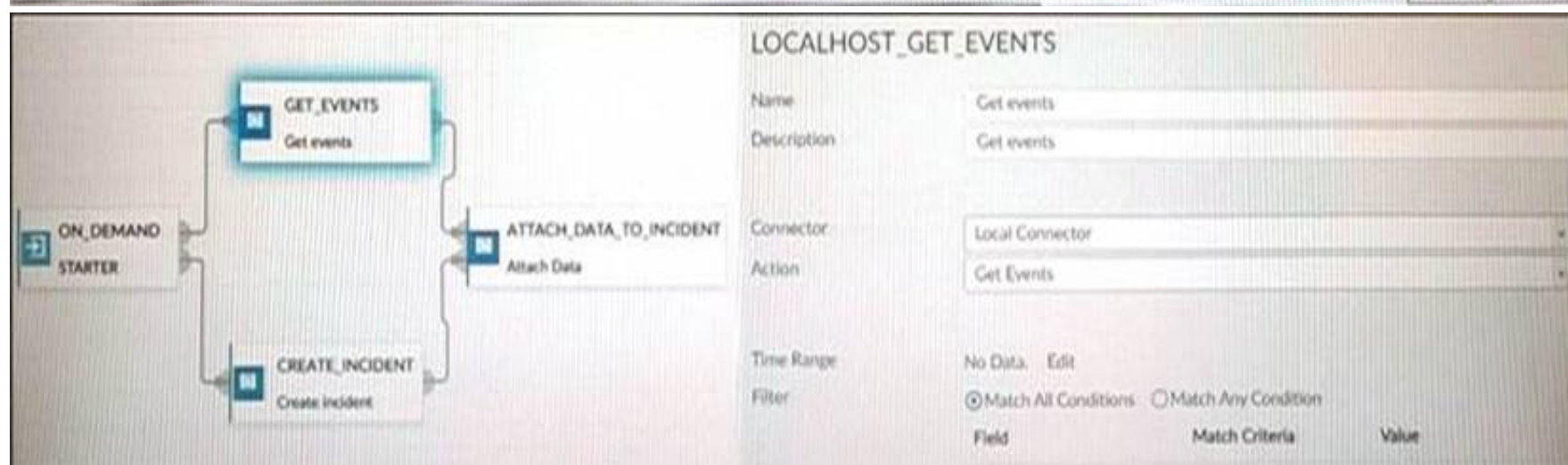D. To build a chart automatically based on the top 100 log entries

Answer: B

NEW QUESTION 158
Refer to the exhibits.

How many events will be added to the incident created after running this playbook?

A. Ten events will be added.
B. No events will be added.
C. Five events will be added.
D. Thirteen events will be added.

Answer: A

NEW QUESTION 159
Which log will generate an event with the status Contained?

A. An IPS log with action=pass.
B. A WebFilter log with action=dropped.
C. An AV log with action=quarantine.
D. An AppControl log with action=blocked.

Answer: C

NEW QUESTION 162
What is the purpose of the following CLI command?

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

A. To add a log file checksum
B. To add the MD's hash value and authentication code
C. To add a unique tag to each log to prove that it came from this FortiAnalyzer
D. To encrypt log communications

Answer: A

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

NEW QUESTION 164
Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

A. Incidents dashboards
B. Threat hunting
C. FortiView Monitor
D. Outbreak alert services

Answer: B

Explanation:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 217: Threat hunting consists in proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach will help administrator find any threats that might have eluded detection by the current security solutions or configurations.

NEW QUESTION 169
View the exhibit:

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

A. The disk quota for the FortiAnalyzer model
B. The disk quota for all devices in the ADOM
C. The disk quota for each device in the ADOM
D. The disk quota for the ADOM type

Answer: B

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

NEW QUESTION 173
If the primary FortiAnalyzer in an HA cluster fails, how is the new primary elected?

A. The configured IP address is checked first.
B. The active port number is checked first.
C. The firmware version is checked first.
D. The configured priority is checked first

Answer: D

Explanation:
In the case of a primary device failure, FortiAnalyzer HA uses the following rules to select a new primary:
• All cluster devices are assigned a priority from 80 to 120. The default priority is 100. If the primary device becomes unavailable, the device with the highest priority is selected as the new primary device. For example, a device with a priority of 110 is selected over a device with a priority of 100.
• If multiple devices have the same priority, the device whose primary IP address has the greatest value is selected as the new primary device. For example, 123.45.67.124 is selected over 123.45.67.123.
• If a new device with a higher priority or a greater value IP address joins the cluster, the new device does not replace (or pre-empt) the current primary device automatically.
FortiAnalyzer_7.0_Study_Guide-Online page 62

NEW QUESTION 177
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE5_FAZ-7.2 Practice Exam Features:

* NSE5_FAZ-7.2 Questions and Answers Updated Frequently

* NSE5_FAZ-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE5_FAZ-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE5_FAZ-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_FAZ-7.2 Practice Test Here](https://www.certshared.com/exam/NSE5_FAZ-7.2/)