

# Fortinet

## Exam Questions NSE5\_FAZ-7.2

Fortinet NSE 5 - FortiAnalyzer 7.2



#### NEW QUESTION 1

What are two benefits of using fabric connectors? (Choose two.)

- A. They allow FortiAnalyzer to send logs in real-time to public cloud accounts.
- B. You do not need an additional license to send logs to the cloud platform.
- C. Fabric connectors allow you to improve redundancy.
- D. Using fabric connectors is more efficient than using third-party polling with API.

**Answer: AC**

#### NEW QUESTION 2

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 FortiAnalyzer
- 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 3

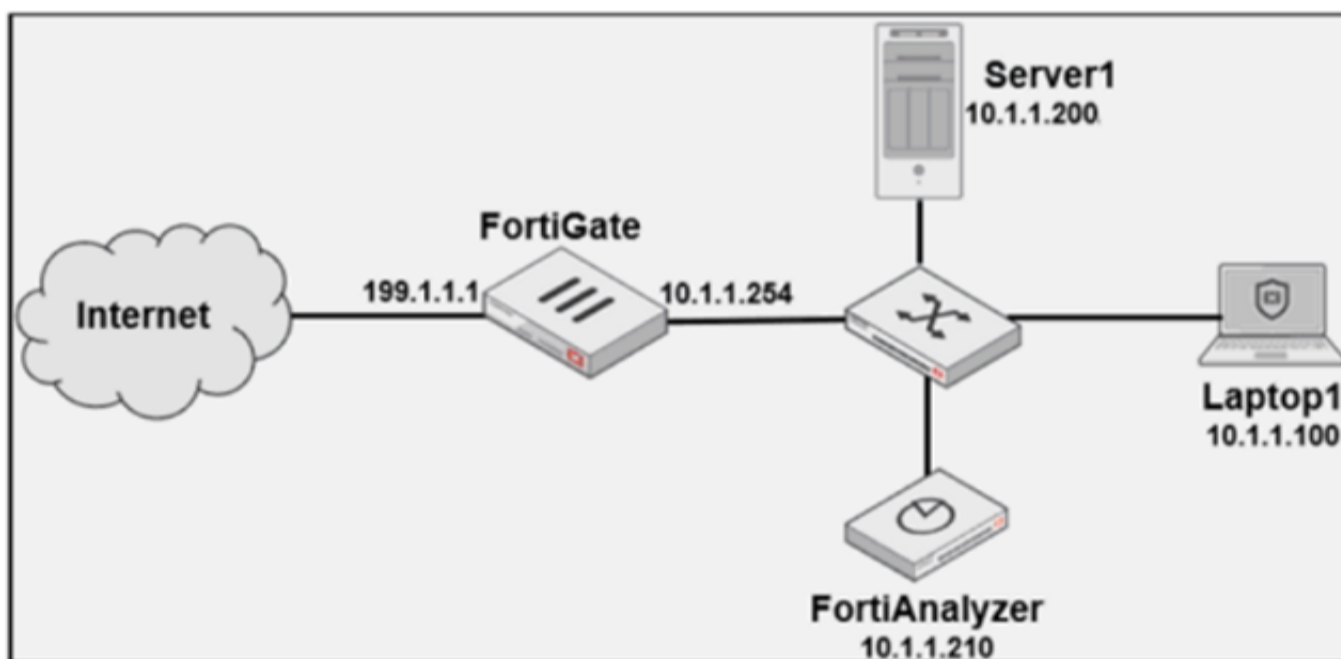
FortiAnalyzer centralizes which functions? (Choose three)

- A. Network analysis
- B. Graphical reporting
- C. Content archiving / data mining
- D. Vulnerability assessment
- E. Security log analysis / forensics

**Answer: BCE**

#### NEW QUESTION 4

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 5

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 6

If a hard disk fails on a FortiAnalyzer that supports software RAID, what should you do to bring the FortiAnalyzer back to functioning normally, without losing data?

- A. Hot swap the disk
- B. Replace the disk and rebuild the RAID manually
- C. Take no action if the RAID level supports a failed disk
- D. Shut down FortiAnalyzer and replace the disk

**Answer:** D

**Explanation:**

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiMana> If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the unit is still running – known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

**NEW QUESTION 7**

You've moved a registered logging device out of one ADOM and into a new ADOM. What happens when you rebuild the new ADOM database?

- A. FortiAnalyzer resets the disk quota of the new ADOM to default.
- B. FortiAnalyzer migrates archive logs to the new ADOM.
- C. FortiAnalyzer migrates analytics logs to the new ADOM.
- D. FortiAnalyzer removes logs from the old ADOM.

**Answer:** C

**Explanation:**

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD40383>

**NEW QUESTION 8**

Which statement is true when you are upgrading the firmware on an HA cluster made up of two FortiAnalyzer devices?

- A. First, upgrade the secondary device, and then upgrade the primary device.
- B. Both FortiAnalyzer devices will be upgraded at the same time.
- C. You can enable uninterruptible-upgrade so that the normal FortiAnalyzer operations are not interrupted while the cluster firmware upgrades.
- D. You can perform the firmware upgrade using only a console connection.

**Answer:** A

**Explanation:**

FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 64: To upgrade FortiAnalyzer HA cluster firmware:

- \* 1. Log in to each secondary device.
- \* 2. Upgrade the firmware of all secondary devices.
- \* 3. Wait for the upgrades to complete and verify that all secondary devices joined the cluster.
- \* 4. Verify that logs on all secondary devices are synchronized with the primary device.
- \* 5. Upgrade the primary device.

<https://docs.fortinet.com/document/fortianalyzer/7.2.0/upgrade-guide/262607/upgrading-fortianalyzer-firmware>

**NEW QUESTION 9**

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 / different config).

C) FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 147: Aggregation: Logs and content files stored and uploaded at scheduled time.

**NEW QUESTION 10**

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 10**

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 14

Which two methods are the most common methods to control and restrict administrative access on FortiAnalyzer? (Choose two.)

- A. Virtual domains
- B. Administrative access profiles
- C. Trusted hosts
- D. Security Fabric

**Answer:** BC

#### NEW QUESTION 19

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?

- A. FortiAnalyzer uses log fetching to retrieve the logs when back online
- B. FortiGate uses the miglogd process to cache the logs
- C. The logfiled process stores logs in offline mode
- D. Logs are dropped

**Answer:** B

#### Explanation:

If FortiAnalyzer becomes unavailable to FortiGate for any reason, FortiGate uses its *miglogd* process to cache the logs. There is a maximum value to the cache size, and the miglogd process will drop cached logs. When the connection between the two devices is restored, the miglogd process begins to send the cached logs to FortiAnalyzer. Therefore, the FortiGate buffer will keep logs long enough to sustain a reboot of your FortiAnalyzer (if you are upgrading the firmware, for example). But it is not intended for a lengthy FortiAnalyzer outage.

#### NEW QUESTION 20

Which two statements are true regarding ADOM modes? (Choose two.)

- A. You can only change ADOM modes through CLI.
- B. In normal mode, the disk quota of the ADOM is fixed and cannot be modified, but in advance mode, the disk quota of the ADOM is flexible because new devices are added to the ADOM.
- C. In an advanced mode ADO
- D. you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.
- E. Normal mode is the default ADOM mode.

**Answer:** CD

#### NEW QUESTION 24

Which two statements are true regardless of initial Logs sync and Log Data Sync for HA on FortiAnalyzer?

- A. By default, Log Data Sync is disabled on all backup devices.
- 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 rebuild the log database with the synchronized logs.

**Answer:** CD

#### NEW QUESTION 28

Logs are being deleted from one of your ADOMs earlier than 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://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 31

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 34**

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 39**

What happens when the IOC breach detection engine on FortiAnalyzer finds web logs that match a blocklisted IP address?

- A. The endpoint is marked as Compromised and optionally, can be put in quarantine.
- B. optionally, can be put in quarantine.
- C. FortiAnalyzer flags the associated host for further analysis.
- D. A new Infected entry is added for the corresponding endpoint.
- E. The detection engine classifies those logs as Suspicious

**Answer:** A

**NEW QUESTION 42**

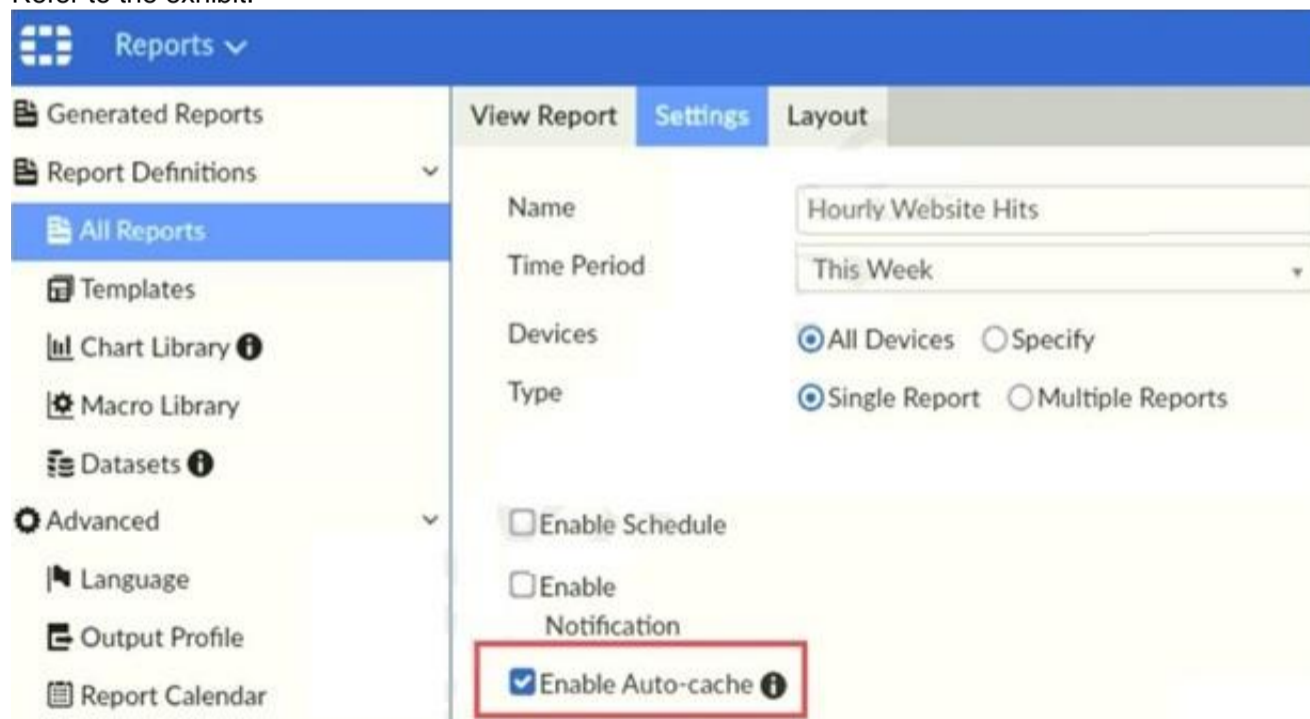
What is the purpose of a predefined template on the FortiAnalyzer?

- 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 47**

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 52

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 54

Refer to the exhibit.

<pre>FortiAnalyzer1# get system status Platform Type       : FAZVM64-KVM Platform Full Name  : FortiAnalyzer-VM64-KVM Version             : v7.2.1-build1215 220809 (GA) Serial Number       : FAZ-VM0000065040 BIOS version        : 04000002 Hostname            : FortiAnalyzer1 Max Number of Admin Domains : 5 Admin Domain Configuration : Enabled FIPS Mode           : Disabled HA Mode             : Stand Alone Branch Point        : 1215 Release Version Information : GA Time Zone           : (GMT-8:00) Pacific Time (US &amp; Canada) Disk Usage           : Free 43.60GB, Total 58.80GB File System          : Ext4 License Status       : Valid  FortiAnalyzer1# get system global adom-mode           : normal adom-select         : enable adom-status         : enable console-output      : standard country-flag        : enable enc-algorithm       : high ha-member-auto-grouping : enable hostname            : FortiAnalyzer2 log-checksum        : md5 log-forward-cache-size : 5 log-mode            : analyzer longitude           : (null) max-aggregation-tasks : 0 max-running-reports : 1 oftp-ssl-protocol   : tlsv1.2 ssl-low-encryption  : disable ssl-protocol        : tlsv1.3 tlsv1.2                     : 2000                     : tlsv1.3 tlsv1.2</pre>	<pre>FortiAnalyzer3# get system status Platform Type       : FAZVM64-KVM Platform Full Name  : FortiAnalyzer-VM64-KVM Version             : v7.2.1-build1215 220809 (GA) Serial Number       : FAZ-VM0000065042 BIOS version        : 04000002 Hostname            : FortiAnalyzer3 Max Number of Admin Domains : 5 Admin Domain Configuration : Enabled FIPS Mode           : Disabled HA Mode             : Stand Alone Branch Point        : 1215 Release Version Information : GA Time Zone           : (GMT-8:00) Pacific Time (US &amp; Canada) Disk Usage           : Free 12.98GB, Total 79.80GB File System          : Ext4 License Status       : Valid  FortiAnalyzer3# get system global adom-mode           : normal adom-select         : enable adom-status         : enable console-output      : standard country-flag        : enable enc-algorithm       : high ha-member-auto-grouping : enable hostname            : FortiAnalyzer3 log-checksum        : md5 log-forward-cache-size : 5 log-mode            : analyzer longitude           : (null) max-aggregation-tasks : 0 max-running-reports : 5 oftp-ssl-protocol   : tlsv1.2 ssl-low-encryption  : disable ssl-protocol        : tlsv1.3 tlsv1.2                     : 2000                     : tlsv1.3 tlsv1.2 web-service-proto    : tlsv1.3 tlsv1.2</pre>
--	---

Based on the partial outputs displayed, which devices can be members of a FortiAnalyzer Fabric?

- A. FortiAnalyzer1 and FortiAnalyzer3
- B. FortiAnalyzer1 and FortiAnalyzer2
- C. All devices listed can be members
- D. FortiAnalyzer2 and FortiAnalyzer3

Answer: C

## NEW QUESTION 55

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 56

An administrator has moved FortiGate A from the root ADOM to ADOM1. However, the administrator is not able to generate reports for FortiGate A in ADOM1. What should the administrator do to solve this issue?

- A. Use the execute sql-local rebuild-db command to rebuild all ADOM databases.
- B. Use the execute sql-local rebuild-adom ADOM1 command to rebuild the ADOM database.
- C. Use the execute sql-report run ADOM1 command to run a report.
- D. Use the execute sql-local rebuild-adom root command to rebuild the ADOM database.

**Answer:** B

#### NEW QUESTION 61

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 62

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 67

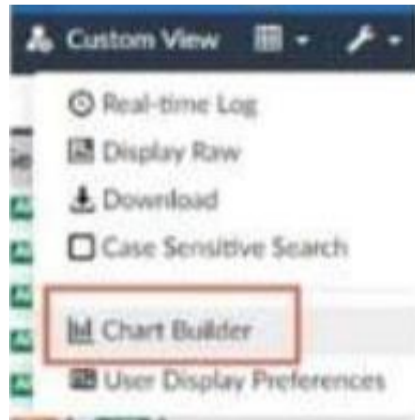
What statements are true regarding disk log quota? (Choose two)

- A. The FortiAnalyzer stops logging once the disk log quota is met.
- B. The FortiAnalyzer automatically sets the disk log quota based on the device.
- C. The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.
- D. The FortiAnalyzer disk log quota is configurable, but has a minimum of 100mb and a maximum based on the reserved system space.

**Answer:** CD

#### NEW QUESTION 68

Refer to the exhibit.



What is the purpose of using the Chart Builder feature on FortiAnalyzer?

- A. In Log View, this feature allows you to build a dataset and chart automatically, based on the filtered search results.
- B. In Log View, this feature allows you to build a chart and chart automatically, on the top 100 log entries.
- C. This feature allows you to build a chart under FortiView.
- D. You can add charts to generated reports using this feature.

**Answer:** A

#### NEW QUESTION 71

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 76

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 79

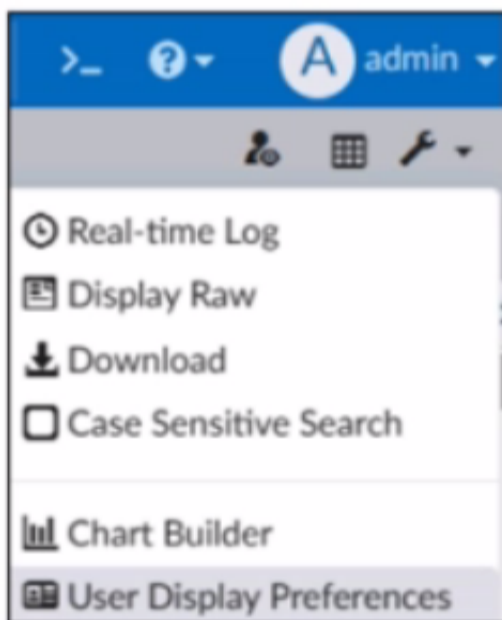
Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally? (Choose two.)

- A. Mail server
- B. Output profile
- C. SFTP server
- D. Report scheduling

**Answer: AB**

#### NEW QUESTION 84

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 89

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%	
Alert and Delete When Usage Reaches	90%		

☐ Modify

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 90

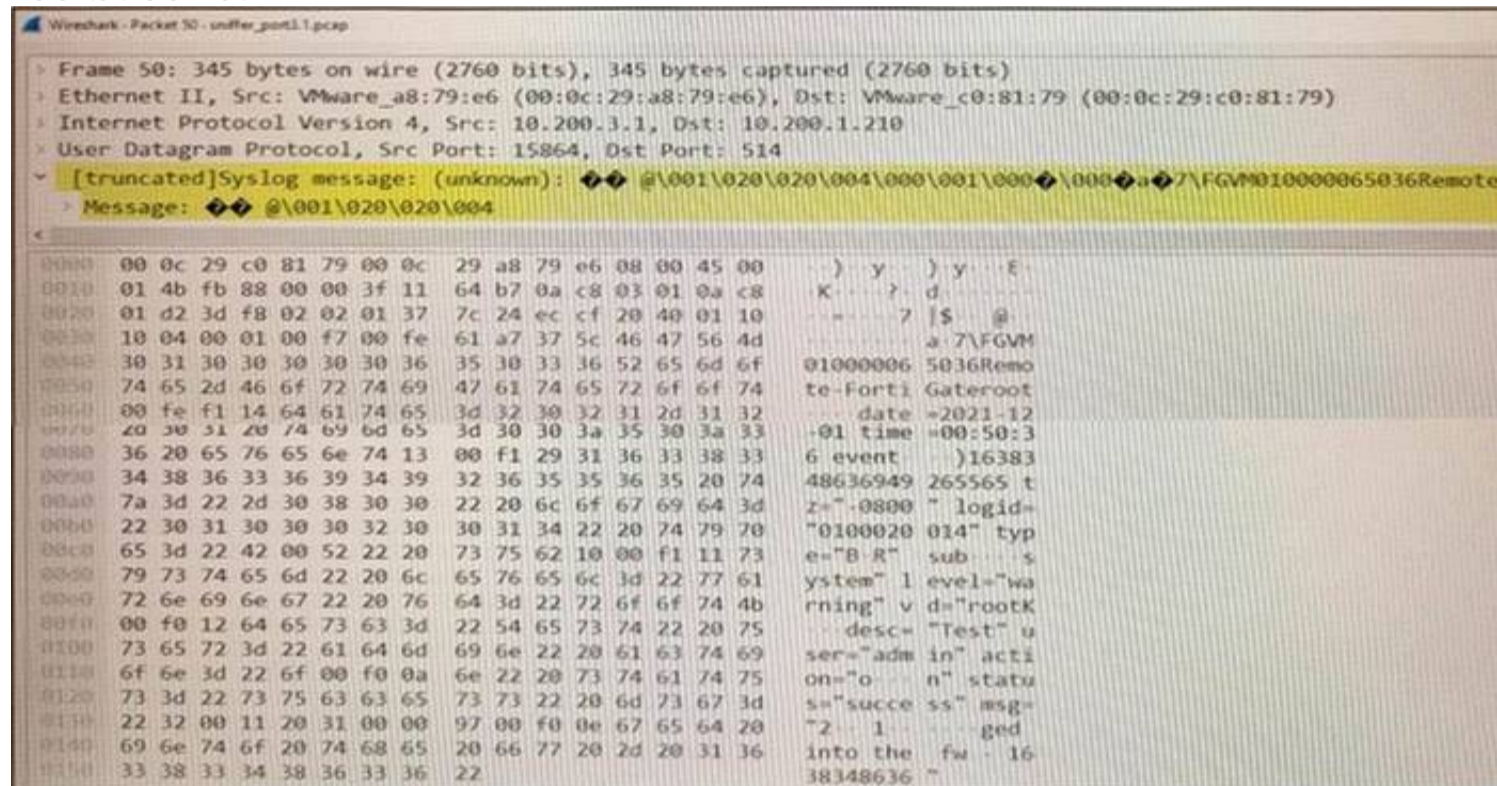
Why must you wait for several minutes before you run a playbook that you just created?

- A. FortiAnalyzer needs that time to parse the new playbook.
- B. FortiAnalyzer needs that time to back up the current playbooks.
- C. FortiAnalyzer needs that time to ensure there are no other playbooks running.
- D. FortiAnalyzer needs that time to debug the new playbook.

**Answer: A**

#### NEW QUESTION 91

Refer to the exhibit.



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

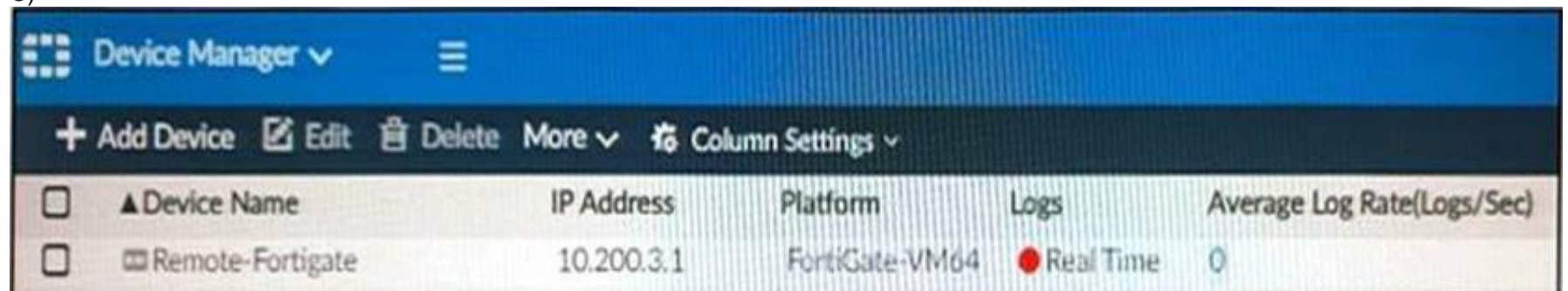
A)



B)



C)



D)



- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer:** C

**NEW QUESTION 92**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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](#)**