

## NSE5\_FAZ-7.2 Dumps

### Fortinet NSE 5 - FortiAnalyzer 7.2

[https://www.certleader.com/NSE5\\_FAZ-7.2-dumps.html](https://www.certleader.com/NSE5_FAZ-7.2-dumps.html)



**NEW QUESTION 1**

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:** 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 2**

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 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**

Which two statements express the advantages of grouping similar reports? (Choose two.)

- A. Improve report completion time.
- B. Conserve disk space on FortiAnalyzer by grouping multiple similar reports.
- C. Reduce the number of hcache tables and improve auto-hcache completion time.
- D. Provides a better summary of reports.

**Answer:** AC

**NEW QUESTION 5**

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 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**

What are two of the key features of FortiAnalyzer? (Choose two.)

- A. Centralized log repository
- B. Cloud-based management
- C. Reports
- D. Virtual domains (VDOMs)

**Answer:** AC

#### NEW QUESTION 8

Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?

- A. To properly correlate logs
- B. To use real-time forwarding
- C. To resolve host names
- D. To improve DNS response times

**Answer:** A

#### Explanation:

- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server for proper log correlation

#### NEW QUESTION 9

Which statement is true about sending notifications with incident updates?

- A. Notifications can be sent only when an incident is updated or deleted.
- B. If you use multiple fabric connectors, all connectors must have the same notification settings
- C. Notifications can be sent only by email.
- D. You can send notifications to multiple external platforms

**Answer:** A

#### NEW QUESTION 10

What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

**Answer:** D

#### NEW QUESTION 10

Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

- A. ADOMs are enabled by default.
- B. ADOMs constrain other administrator's access privileges to a subset of devices in the device list.
- C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
- D. All administrators can create ADOMs--not just the admin administrator.

**Answer:** BC

#### NEW QUESTION 11

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 15

View the exhibit:

Data Policy

Keep Logs for Analytics: 60 Days

Keep Logs for Archive: 365 Days

Disk Utilization

Maximum Allowed: 1000 MB

Analytics: Archive: 70%

Alert and Delete When Usage Reaches: 90%

Out of Available: 62.8 GB

☐ 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 19

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>

- A. To reset the disk quota enforcement to default
- B. To remove the analytics logs of the device from the old database
- C. To migrate the archive logs to the new ADOM
- D. To populate the new ADOM with analytical logs for the moved device, so you can run reports

**Answer: D**

**Explanation:**

- Are the device's analytics logs required for reports in the *new* ADOM? If so, rebuild the new ADOM database:  
# exe sql-local rebuild-adom <new-ADOM-name>

#### NEW QUESTION 24

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: AB**

#### NEW QUESTION 29

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 30

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 35

Refer to the exhibit.



The screenshot shows the 'Cluster Settings' page in FortiAnalyzer. The 'Operation Mode' is set to 'High Availability'. The 'Preferred Role' is 'Primary'. The 'Cluster Virtual IP' section shows 'Interface' as 'port1' and 'IP Address' as '192.168.101.222'. The 'Cluster Settings' section includes 'Peer IP and Peer SN' with 'Peer IP' as '10.0.1.210' and 'Peer SN' as 'FAZ-VM0000065040'. Other settings include 'Group Name' as 'NSE5', 'Group ID' as '1', 'Password' as a masked field, 'Heart Beat Interval' as '10' seconds, 'Failover Threshold' as '30', 'Priority' as '120', and 'Log Data Sync' is disabled.

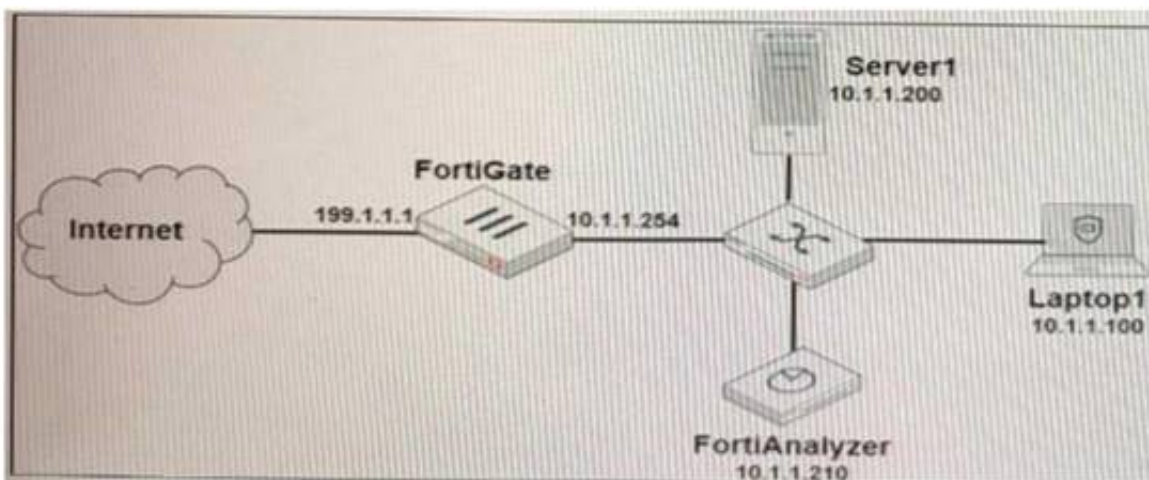
The image displays the configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster. What can you conclude from the configuration displayed?

- A. This FortiAnalyzer will join to the existing HA cluster as the primary.
- B. This FortiAnalyzer is configured to receive logs in its port1.
- C. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
- D. After joining to the cluster, this FortiAnalyzer will keep an updated log database.

**Answer: D**

#### NEW QUESTION 40

Refer to the exhibit.



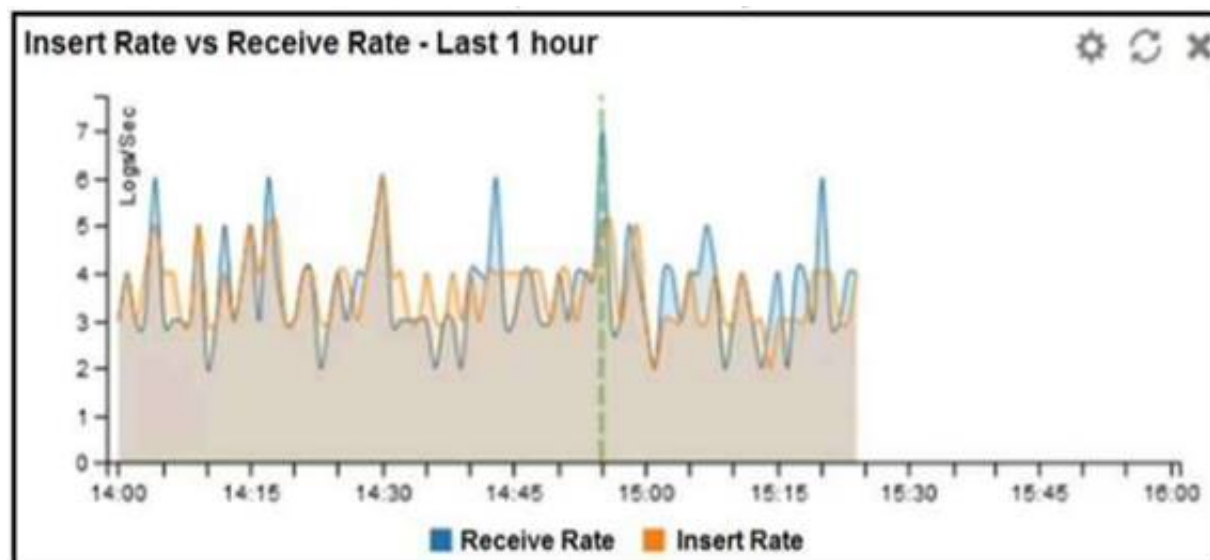
Laptop1 is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin" and coming from Laptop1: Which filter will achieve the desired result?

- A. operation—login & performed\_on==BGUI(10.1.1.100)" & user!=admin
- B. operation—login & srcip=10.1.1.100 & dstip==10.1.1.210 & user=admin
- C. operation—login & performed1\_on=,'GUI(10.1.1.210)" & user!=admin
- D. operation—login & dstip=10.1.1.210 & user1—admin

**Answer: C**

#### NEW QUESTION 45

Refer to the exhibit.



What does the data point at 14:55 tell you?

- A. The received rate is almost at its maximum for this device
- B. The sqlplugind daemon is behind in log indexing by two logs
- C. Logs are being dropped

D. Raw logs are reaching FortiAnalyzer faster than they can be indexed

**Answer:** D

#### NEW QUESTION 49

Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

- A. FortiAnalyzer HA can function without VRR
- B. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
- C. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
- D. All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
- E. FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

**Answer:** BC

#### NEW QUESTION 51

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

#### NEW QUESTION 54

What purposes does the auto-cache setting on reports serve? (Choose two.)

- A. To reduce report generation time
- B. To automatically update the hcache when new logs arrive
- C. To reduce the log insert lag rate
- D. To provide diagnostics on report generation time

**Answer:** AB

#### NEW QUESTION 55

What is the purpose of output variables?

- A. To store playbook execution statistics
- B. To use the output of the previous task as the input of the current task
- C. To display details of the connectors used by a playbook
- D. To save all the task settings when a playbook is exported

**Answer:** A

#### NEW QUESTION 57

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

- A. FortiAnalyzer provides the ability to create custom reports.
- B. FortiAnalyzer allows 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 59

Refer to the exhibits.

Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Handler	Tags
> MS-ISLdr:HTF:Information Disclosure (2)	Mitigated	IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
> PHPURL:Code:Injection (2)	Mitigated	IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
> 91.189.92.18 (1)	Mitigated	SSL	1	Low	2 hours ago	2 hours ago	Default-Risky-Destination-Detection-By-Threat	Risky, SSL
> HTTP:Request:URI:Directory Traversal (2)	Mitigated	IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
> Apache.Expect:Header:XSS (2)	Mitigated	IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat	
✓ 10.0.1.19 (7)							Default-Malicious-Code-Detection-By-Endpoint	Intrusion, Signature
Internal Intrusion MS-ISLdr:HTF:Information Disclosure	Mitigated	IPS	2	Medium	2021-12-01 21:32:31	2021-12-01 21:32:41	Default-Risky-Destination-Detection-By-Endpoint	Risky, SSL
Internal Intrusion PHPURL:Code:Injection (2)	Mitigated	IPS	2	Medium	2021-12-01 21:32:11	2021-12-01 21:32:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion, Signature
Insecure SSL connection blocked	Mitigated	SSL	5	Low	2021-12-01 21:32:01	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion, Signature
Internal Intrusion HTTP:Request:URI:Directory Traversal	Mitigated	IPS	2	Medium	2021-12-01 21:31:51	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion, Signature
Internal Intrusion Apache.Expect:Header:XSS	Mitigated	IPS	2	Medium	2021-12-01 21:31:31	2021-12-01 21:31:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion, Signature
✓ 10.200.1.254 (6)								
Internal Intrusion MS-ISLdr:HTF:Information Disclosure	Mitigated	IPS	2	Medium	2021-12-01 21:32:31	2021-12-01 21:32:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion, Signature
Internal Intrusion PHPURL:Code:Injection (2)	Mitigated	IPS	2	Medium	2021-12-01 21:32:11	2021-12-01 21:32:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion, Signature
Internal Intrusion HTTP:Request:URI:Directory Traversal	Mitigated	IPS	2	Medium	2021-12-01 21:31:51	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion, Signature
Internal Intrusion Apache.Expect:Header:XSS	Mitigated	IPS	2	Medium	2021-12-01 21:31:31	2021-12-01 21:31:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion, Signature
Internal Intrusion HTTP:Request:URI:Directory Traversal	Mitigated	IPS	2	Medium	2021-12-01 21:31:51	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion, Signature
Internal Intrusion Apache.Expect:Header:XSS	Mitigated	IPS	2	Medium	2021-12-01 21:31:31	2021-12-01 21:31:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion, Signature
Internal Intrusion Nmap:Web:Scanner:detected	Unmitigated	IPS	21	High	2021-12-01 21:31:11	2021-12-01 21:32:06	Default-Malicious-Code-Detection-By-Endpoint	Intrusion, Signature





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:** C

#### NEW QUESTION 62

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 64

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 68

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 73

What is required to authorize a FortiGate on FortiAnalyzer using Fabric authorization?

- A. A FortiGate ADOM
- B. The FortiGate serial number
- C. A pre-shared key
- D. Valid FortiAnalyzer credentials

**Answer:** C

#### NEW QUESTION 75

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:** C

#### NEW QUESTION 78

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 79

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 80

Which daemon is responsible for enforcing raw log file size?

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

**Answer:** A

#### NEW QUESTION 81

Which daemon is responsible for enforcing the log file size?

- A. sqlplugind
- B. logfiled
- C. miglogd
- D. ofrpd

**Answer:** B

#### NEW QUESTION 84

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 FortiAnalyzer.
- D. A playbook that was disabled when it was exported, will be disabled when it is imported.

**Answer:** BD

#### NEW QUESTION 86

Which two purposes does the auto cache setting on reports serve? (Choose two.)

- A. It automatically updates the hcache when new logs arrive.
- B. It provides diagnostics on report generation time.
- C. It reduces the log insert lag rate.
- D. It reduces report generation time.

**Answer:** AD



**NEW QUESTION 88**

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 91**

For which two purposes would you use the command set log checksum? (Choose two.)

- A. To help protect against man-in-the-middle attacks during log upload from FortiAnalyzer to an SFTP server
- B. To prevent log modification or tampering
- C. To encrypt log communications
- D. To send an identical set of logs to a second logging server

**Answer:** AB

**NEW QUESTION 94**

FortiAnalyzer uses the Optimized Fabric Transfer Protocok (OFTP) over SSL for what purpose?

- A. To upload logs to an SFTP server
- B. To prevent log modification during backup
- C. To send an identical set of logs to a second logging server
- D. To encrypt log communication between devices

**Answer:** D

**NEW QUESTION 97**

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec? (Choose two.)

- A. Must configure the FortiAnalyzer end of the tunnel only--the FortiGate end is auto-negotiated.
- B. Must establish an IPsec tunnel ID and pre-shared key.
- C. IPsec cannot be enabled if SSL is enabled as well.
- D. IPsec is only enabled through the CLI on FortiAnalyzer.

**Answer:** C

**NEW QUESTION 102**

What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)

- A. RADIUS
- B. Local
- C. LDAP
- D. PKI
- E. TACACS+

**Answer:** ACE

**NEW QUESTION 105**

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

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

**Answer:** BC

**NEW QUESTION 110**

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 112**

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 117**

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 119**

What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server? (Choose two.)

- A. SFTP, FTP, or SCP server
- B. Mail server
- C. Output profile
- D. Report scheduling

**Answer:** BC

**Explanation:**

<https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creating-output-profiles>

**NEW QUESTION 121**

By default, what happens when a log file reaches its maximum file size?

- A. FortiAnalyzer overwrites the log files.
- B. FortiAnalyzer stops logging.
- C. FortiAnalyzer rolls the active log by renaming the file.
- D. FortiAnalyzer forwards logs to syslog.

**Answer:** C

**NEW QUESTION 126**

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 131**

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 133**

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 134**

Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate to FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

- A. A local wildcard administrator account
- B. A remote LDAP server
- C. A trusted host profile that restricts access to the LDAP group
- D. An administrator group

**Answer:** AB

**NEW QUESTION 136**

What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)

- A. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
- B. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer.
- C. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date.
- D. Make sure all endpoints are reachable by FortiAnalyzer.

**Answer:** BC

**NEW QUESTION 137**

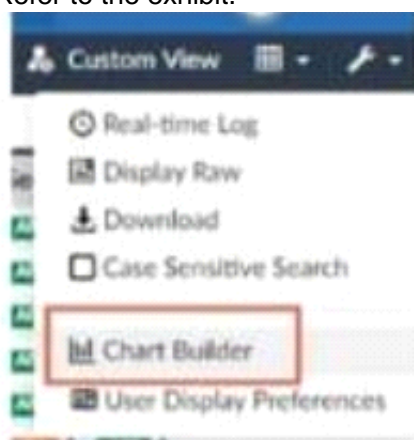
What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

- A. Log correlation
- B. Host name resolution
- C. Log collection
- D. Real-time forwarding

**Answer:** A

**NEW QUESTION 142**

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 143**

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 146**

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 147**

.....



## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your NSE5\_FAZ-7.2 Exam with Our Prep Materials Via below:**

[https://www.certleader.com/NSE5\\_FAZ-7.2-dumps.html](https://www.certleader.com/NSE5_FAZ-7.2-dumps.html)