

Exam Questions NSE5_FAZ-7.0

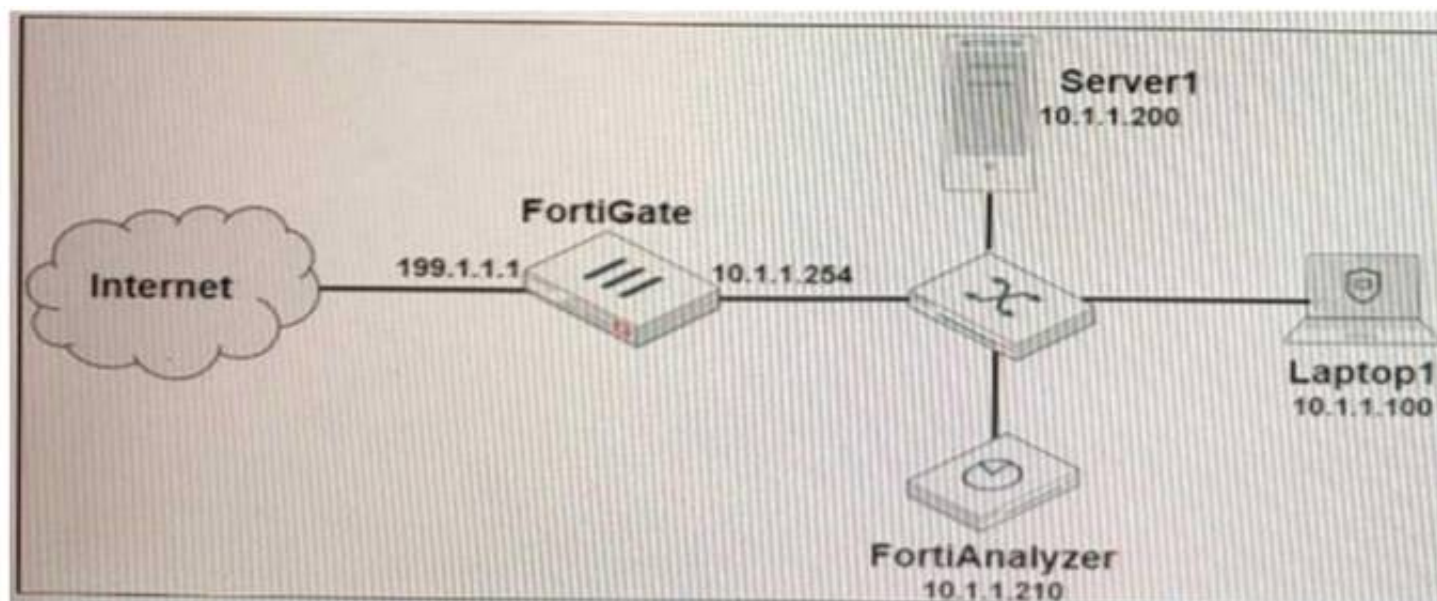
Fortinet NSE 5 - FortiAnalyzer 7.0

https://www.2passeasy.com/dumps/NSE5_FAZ-7.0/



NEW QUESTION 1

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=="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 & user!=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 2

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 3

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 4

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 5

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

Explanation:

To prevent logs from being tampered with while in storage, you can add a log checksum using the config system global command. You can configure FortiAnalyzer to record a log file hash value, timestamp, and authentication code when the log is rolled and archived and when the log is uploaded (if that feature is enabled). This can also help against man-in-the-middle only for the transmission from FortiAnalyzer to an SSH File Transfer Protocol (SFTP) server during log upload.
FortiAnalyzer_7.0_Study_Guide-Online page 149

NEW QUESTION 6

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: AC

Explanation:

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

NEW QUESTION 7

Which statement about sending notifications with incident updates is true?

- A. Notifications can be sent only when an incident is created or deleted.
- B. You must configure an output profile to send notifications by email.
- C. Each incident can send notifications to a single external platform.
- D. Each connector used can have different notification settings.

Answer: D

NEW QUESTION 8

Which statement describes online logs on FortiAnalyzer?

- A. Logs that reached a specific size and were rolled over
- B. Logs that can be used to create reports
- C. Logs that can be viewed using Log Browse
- D. Logs that are saved to disk, compressed, and available in FortiView

Answer: C

NEW QUESTION 9

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 10

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 10

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 13

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 18

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 22

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 27

What can the CLI command # diagnose test application oftpd 3 help you to determine?

- A. What devices and IP addresses are connecting to FortiAnalyzer
- B. What logs, if any, are reaching FortiAnalyzer
- C. What ADOMs are enabled and configured
- D. What devices are registered and unregistered

Answer: A

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/395556/test#test_application

NEW QUESTION 30

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 34

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 39

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

- A. When in collector mode, FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.
- B. Collector mode is the default operating mode.
- C. When in collector mod
- D. FortiAnalyzer supports event management and reporting features.
- E. By deploying different FortiAnalyzer devices with collector and analyzer mode in a network, you can improve the overall performance of log receiving, analysis, and reporting

Answer: AD

NEW QUESTION 41

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 42

Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

- A. FortiView
- B. Event Management
- C. Device Manger
- D. Reporting

Answer: B

NEW QUESTION 45

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 48

Refer to the exhibit.

The screenshot shows the 'New Administrator' configuration page in FortiAnalyzer. The 'User Name' is 'remoteadmin'. The 'Admin Type' is 'GROUP'. The 'GROUP' dropdown is set to 'remoteservergroup'. The checkbox 'Match all users on remote server' is checked and highlighted with a red box. Other fields include 'Admin Profile' (Super_User), 'Administrative Domain' (All ADOMs), 'JSON API Access' (None), 'Trusted Hosts' (OFF), and 'Meta Fields' (Advanced Options).

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 50

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 55

How can you attach a report to an incident?

- A. By attaching it to an event handler alert
- B. By editing the settings of the desired report
- C. From the properties of an existing incident
- D. Saving it in JSON format, and then importing it

Answer: C

NEW QUESTION 58

Why run the command diagnose sql status sqlplugind?

- A. To list the current SQL processes running
- B. To check what is the database log insertion status
- C. To display the SOL query connections and hcache status
- D. To view the current hcache size

Answer: C

NEW QUESTION 62

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 65

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 67

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: D

Explanation:

You can add more than one fabric connector, each with the same or different notification settings. The receiving side of the connector must be configured for the notifications to be sent successfully.

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 34: Fabric connectors also enable FortiAnalyzer to send notifications to ITSM platforms when a new incident is created or for any subsequent updates.

NEW QUESTION 71

What are the operating modes of FortiAnalyzer? (Choose two)

- A. Standalone
- B. Manager
- C. Analyzer
- D. Collector

Answer: CD

NEW QUESTION 74

How does FortiAnalyzer retrieve specific log data from the database?

- A. SQL FROM statement
- B. SQL GET statement
- C. SQL SELECT statement
- D. SQL EXTRACT statement

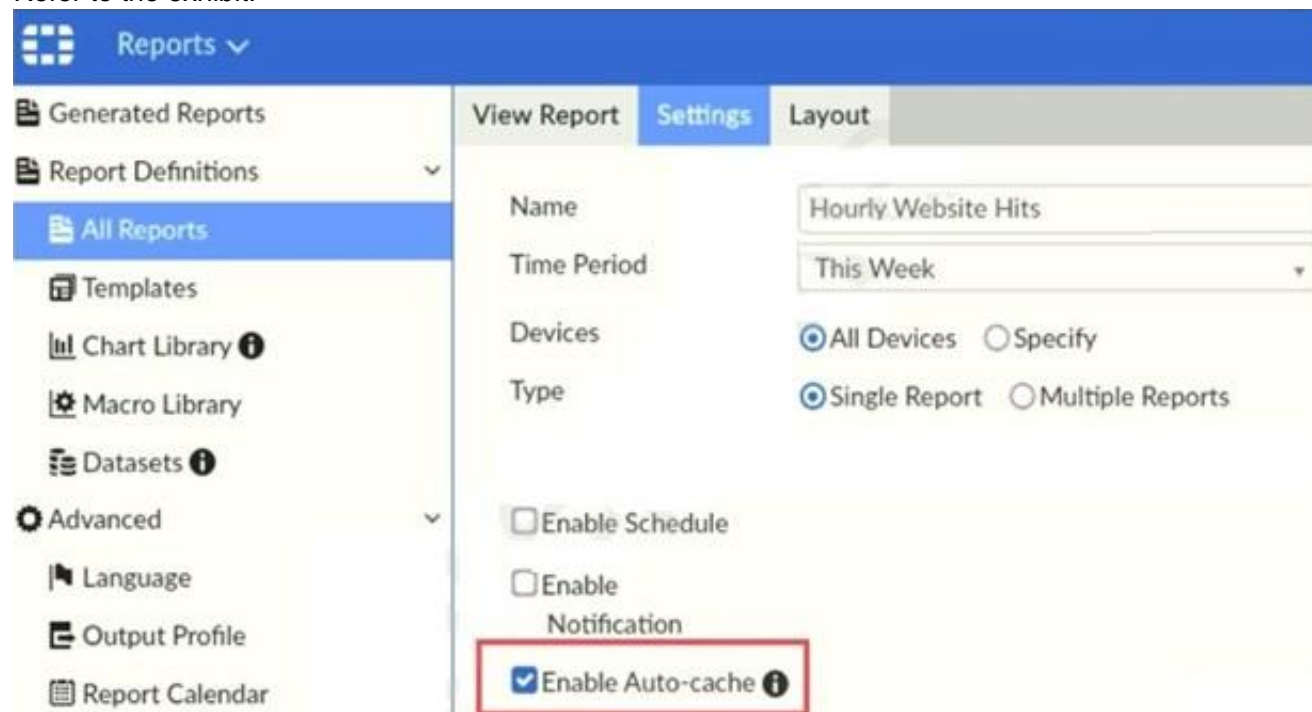
Answer: A

Explanation:

<https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/137bb60e-ff37-11e8-8524-f8bc1258b8>

NEW QUESTION 79

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 80

Which daemon is responsible for enforcing raw log file size?

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

Answer: A

NEW QUESTION 83

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 84

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 86

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 87

If you upgrade the FortiAnalyzer firmware, which report element can be affected?

- A. Custom datasets
- B. Report scheduling
- C. Report settings
- D. Output profiles

Answer: A

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/upgrade-guide/669300/checking-reports>

NEW QUESTION 88

Refer to the exhibit.

The screenshot shows the 'Cluster Settings' configuration page in FortiAnalyzer. The 'Operation Mode' is set to 'High Availability'. The 'Preferred Role' is set to 'Primary'. The 'Cluster Virtual IP' section shows 'Interface' as 'port1' and 'IP Address' as '192.168.101.222'. The 'Cluster Settings' section shows 'Peer IP and Peer SN' with 'Peer IP' as '10.0.1.210' and 'Peer SN' as 'FAZ-VM0000065040'. The 'Group Name' is 'NSE5', 'Group ID' is '1', 'Password' is masked, 'Heart Beat Interval' is '10' seconds, 'Failover Threshold' is '30', 'Priority' is '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: B

Explanation:

"If the preferred role is Primary, then this unit becomes the primary unit if it is configured first in a new HA cluster. If there is an existing primary unit, then this unit becomes a secondary unit." (<https://docs.fortinet.com/document/fortianalyzer/7.0.5/administration-guide/275104>)

NEW QUESTION 89

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 93

The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device. What can be the reason for this failure?

- A. FortiAnalyzer is in an HA cluster.

- Answer: C**

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 & Canada) Disk Usage : Free 43.60GB, Total 58.80GB File System : Ext4 License Status : Valid </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 & Canada) Disk Usage : Free 12.98GB, Total 79.80GB File System : Ext4 License Status : Valid </pre>
<pre> 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 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 task-list-size : 2000 webbservice-proto : tlsv1.3 tlsv1.2 </pre>

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

Answer: C

- 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

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

visit - <https://www.2PassEasy.com>

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 107

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 111

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 112

Refer to the exhibit.

Event	Event Status	Event Type	Count	Severity
✓ 151.101.54.62 (1)				
Insecure SSL Connection blocked from 10.0.3.20	Mitigated	⚙️ SSL	1	🟢 Low

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 115

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 120

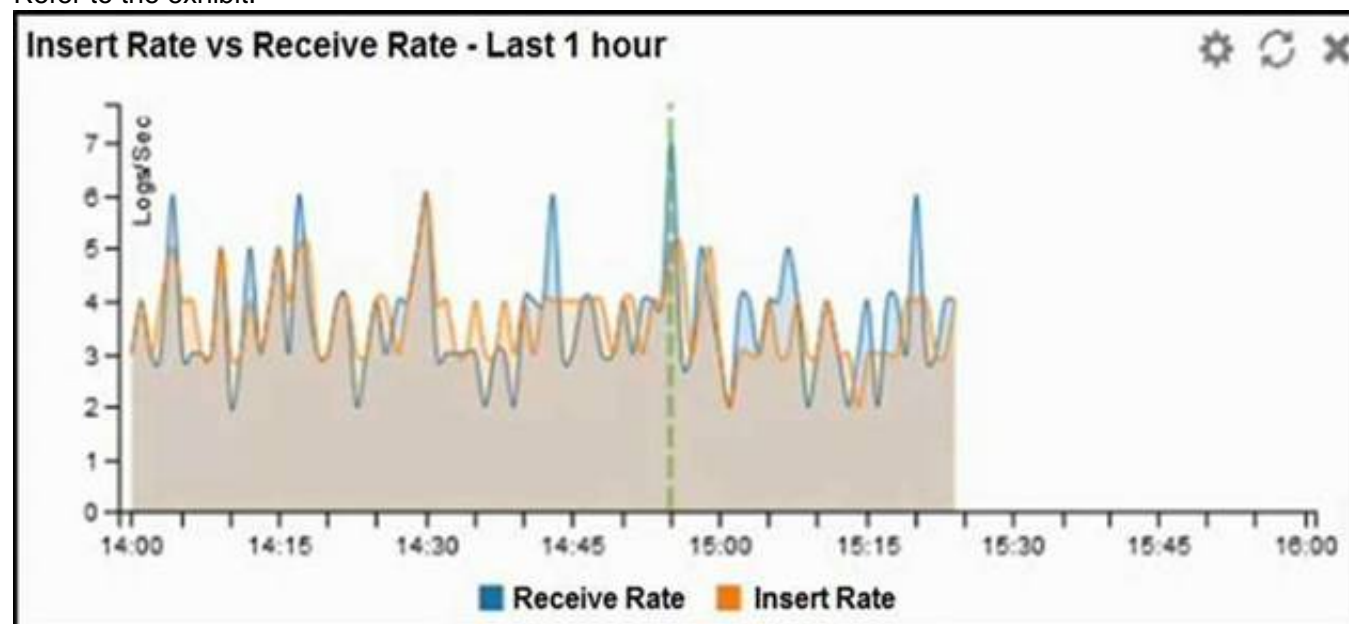
What purposes does the auto-cache setting on reports serve? (Choose two.)

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

Answer: AB

NEW QUESTION 124

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 129

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 131

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 drive is no longer being used by the RAID controller

Answer: D

NEW QUESTION 135

For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:

- A. Use DNS
- B. Use host name resolution
- C. Use real-time forwarding
- D. Use an NTP server

Answer: D

NEW QUESTION 137

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

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 141

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 146

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 150

An administrator has configured the following settings:

```
config system global
set log-checksum md5-auth
end
```

What is the significance of executing this command?

- A. This command records the log file MD5 hash value.
- B. This command records passwords in log files and encrypts them.
- C. This command encrypts log transfer between FortiAnalyzer and other devices.
- D. This command records the log file MD5 hash value and authentication code.

Answer: D

NEW QUESTION 154

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: B

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 242: Output variables allow you to use the output from a preceding task as an input to the current task.
"Output variables allow you to use the output from a preceding task as an input to the current task." FortiAnalyzer_7.0_Study_Guide-Online page 242

NEW QUESTION 155

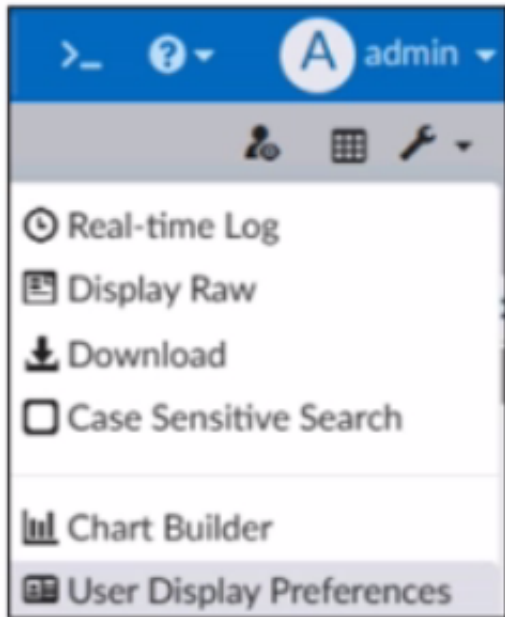
In FortiAnalyzer's FormView, source and destination IP addresses from FortiGate devices are not resolving to a hostname. How can you resolve the source and destination IPs, without introducing any additional performance impact to FortiAnalyzer?

- 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 158

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 162

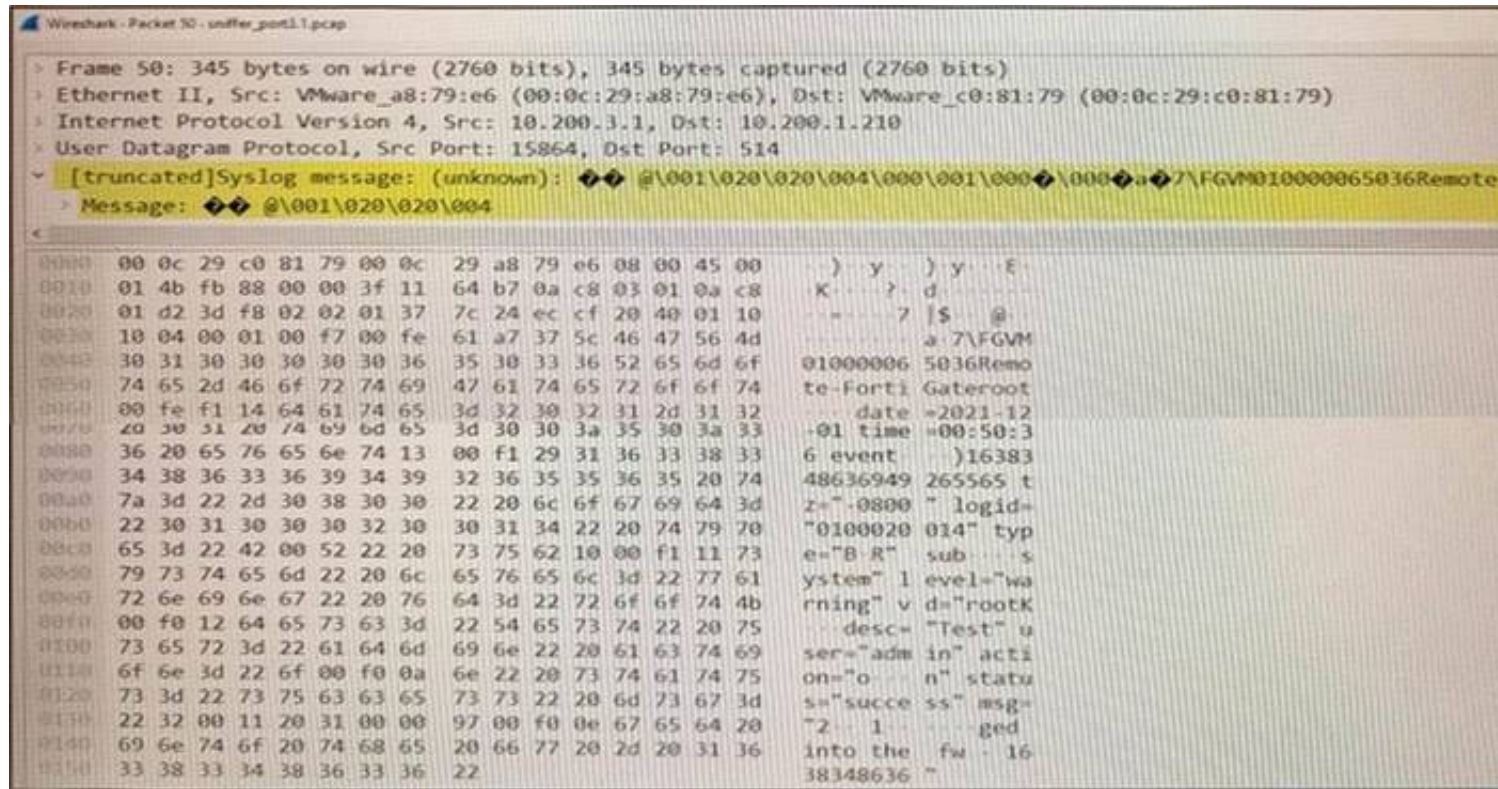
FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for analytics logs is 60 days. What is the most likely problem?

- 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 163

Refer to the exhibit.



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

A)

Device Manager					
+ Add Device ✎ Edit 🗑 Delete More ▾ ⚙ Column Settings ▾					
<input type="checkbox"/>	▲ Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote- Fortigate	10.200.3.1	FortiGate-VM64	  Real Time	0

B)

Device Manager					
+ Add Device Edit Delete More Column Settings					
<input type="checkbox"/>	▲ Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-Fortigate	10.200.3.1	FortiGate-VM64	Real Time	0

C)

Device Manager					
+ Add Device Edit Delete More Column Settings					
<input type="checkbox"/>	▲ Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-Fortigate	10.200.3.1	FortiGate-VM64	Real Time	0

D)

Device Manager					
+ Add Device Edit Delete More Column Settings					
<input type="checkbox"/>	▲ Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-Fortigate	10.200.3.1	FortiGate-VM64	Real Time	0

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

Answer: C

NEW QUESTION 167

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE5_FAZ-7.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE5_FAZ-7.0 Product From:

https://www.2passeasy.com/dumps/NSE5_FAZ-7.0/

Money Back Guarantee

NSE5_FAZ-7.0 Practice Exam Features:

- * NSE5_FAZ-7.0 Questions and Answers Updated Frequently
- * NSE5_FAZ-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE5_FAZ-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE5_FAZ-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year