

NSE5_FAZ-7.0 Dumps

Fortinet NSE 5 - FortiAnalyzer 7.0

https://www.certleader.com/NSE5_FAZ-7.0-dumps.html



NEW QUESTION 1

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 2

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 3

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 4

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 5

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 6

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 7

View the exhibit.

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 8

Which SQL query is in the correct order to query the database in the FortiAnalyzer?

- 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

NEW QUESTION 9

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: D

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

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 15

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

NEW QUESTION 18

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 22

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 23

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 28

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 30

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 31

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 public cloud accounts like Amazon S3, Azure Blob, and Google Cloud.

Answer: AD

NEW QUESTION 36

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 41

Refer to the exhibit.

Laptop 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=10.1.1.2.10 & user1—admin

Answer: C

NEW QUESTION 44

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 48

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 49

How are logs forwarded when FortiAnalyzer is using aggregation mode?

- A. Logs are forwarded as they are received and content files are uploaded at a scheduled time.
- B. Logs and content files are stored and uploaded at a scheduled time.
- C. Logs are forwarded as they are received.
- D. Logs and content files are forwarded as they are received.

Answer: B

Explanation:

<https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/> <https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes>

NEW QUESTION 50

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 55

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 56

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: D

NEW QUESTION 61

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: C

NEW QUESTION 63

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 65

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:

NEW QUESTION 69

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 74

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 76

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 77

How do you restrict an administrator's access to a subset of your organization's ADOMs?

- A. Set the ADOM mode to Advanced
- B. Assign the ADOMs to the administrator's account
- C. Configure trusted hosts
- D. Assign the default Super_User administrator profile

Answer: B

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigning-administrators-to>

NEW QUESTION 82

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 85

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 88

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 92

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.
- B. ADOM mode should be set to advanced, in order to register the FortiClient EMS device.
- C. ADOMs are not enabled on FortiAnalyzer.
- D. A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.

Answer: C

NEW QUESTION 95

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 97

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 98

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 102

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://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automatic-deletion>

NEW QUESTION 103

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

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

Answer: D

NEW QUESTION 104

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 109

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 111

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 114

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 117

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 119

Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

- A. FROM
- B. LIMIT
- C. WHERE
- D. ORDER BY

Answer: A

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 123

An administrator fortinet, is able to view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mail server that can be used to send email.

What could be the problem?

- A. Fortinet is assigned the Standard_ User administrator profile.
- B. A trusted host is configured.
- C. ADOM mode is configured with Advanced mode.
- D. Fortinet is assigned the Restricted_ User administrator profile.

Answer: A

NEW QUESTION 125

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 128

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 129

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 130

In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results. Similarly, which feature you can use for FortiView?

- A. Export to Report Chart
- B. Export to PDF
- C. Export to Chart Builder
- D. Export to Custom Chart

Answer: A

NEW QUESTION 131

.....

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-7.0 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE5_FAZ-7.0-dumps.html