

Fortinet

Exam Questions NSE5_FAZ-7.2

Fortinet NSE 5 - FortiAnalyzer 7.2



NEW QUESTION 1

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

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 259: The main clauses FortiAnalyzer reports use are as follows:

- FROM
- WHERE
- GROUP BY
- ORDER BY
- LIMIT
- OFFSET

Accordingly, following the SELECT keyword, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide.

NEW QUESTION 2

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

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

Answer: A

NEW QUESTION 3

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 4

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 5

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

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

Answer: A

NEW QUESTION 6

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.

NEW QUESTION 7

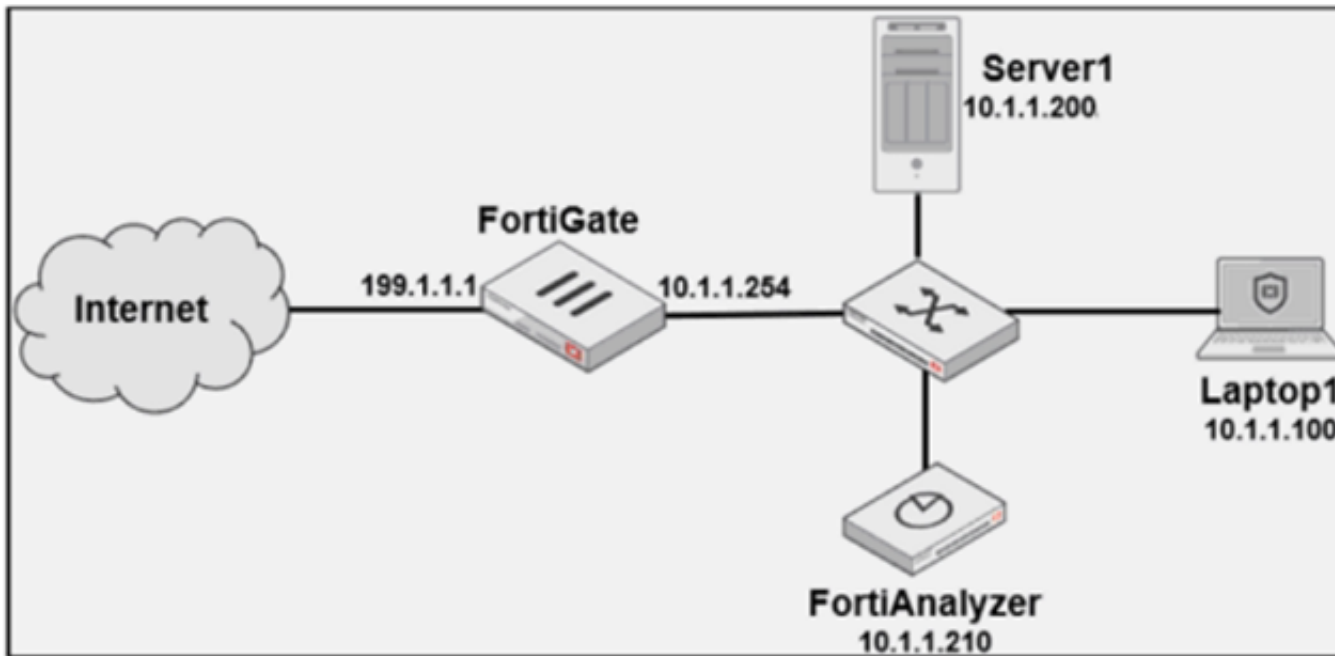
Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

- A. Antivirus logs
- B. Web filter logs
- C. IPS logs
- D. Application control logs

Answer: B

NEW QUESTION 8

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 9

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 10

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

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: BD

Explanation:

Option B is correct because you must establish an IPsec tunnel ID and pre-shared key to secure the communication between FortiAnalyzer and FortiGate with IPsec12. The tunnel ID is a unique identifier for each tunnel and the pre-shared key is a secret passphrase that authenticates the peers.

Option D is correct because IPsec is only enabled through the CLI on FortiAnalyzer1. You cannot configure IPsec settings through the GUI on FortiAnalyzer.

NEW QUESTION 11

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 13

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

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

Answer: A

Explanation:

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

NEW QUESTION 14

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 17

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

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

Answer: CD

NEW QUESTION 20

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 22

Refer to the exhibit.

The screenshot shows the 'New Administrator' configuration page in FortiAnalyzer. The left sidebar contains navigation options: Dashboard, Logging Topology, All ADOMs, Storage Info, Network, HA, Admin, Administrators (selected), Profile, Remote Authentication Server, Admin Settings, SAML SSO, Certificates, Local Certificates, and CA Certificates. The main form fields include: User Name (remoteadmin), Avatar (with a green 'R' icon and buttons for Change Photo and Remove Photo), Comments (empty text area), Admin Type (GROUP), GROUP (remoteservergroup), Match all users on remote server (checked and highlighted with a red box), Admin Profile (Super_User), Administrative Domain (All ADOMs), JSON API Access (None), Trusted Hosts (OFF), Meta Fields, and 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 27

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 32

Which two actions should an administrator take 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. Make sure all endpoints are reachable by FortiAnalyzer.
- C. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer device.
- D. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up to date.

Answer: AD

Explanation:

In order to configure IOC, you require the following:

- A one-year subscription to IOC. Note that FortiAnalyzer does include an evaluation license, but it is restrictive and only meant to give you an idea of how the feature works.
 - A web filter services subscription on FortiGate device(s)
 - Web filter policies on FortiGate device(s) that send traffic to FortiAnalyzer Compromised Hosts or Indicators of Compromise service (IOC) is a licensed feature.
- To view Compromised Hosts, you must turn on the UTM web filter of FortiGate devices and subscribe your FortiAnalyzer unit to FortiGuard to keep its local threat database synchronized with the FortiGuard threat database. See Subscribing FortiAnalyzer to FortiGuard.

Ref :

<https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/137635/viewing-compromised-host>

NEW QUESTION 36

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 37

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 38

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 39

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 41

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 43

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 44

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 47

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

- A. Configuring fabric connectors to send notification to ITSM platform upon incident creation is more efficient than third-party information from the FortiAnalyzer

- API.
- B. Fabric connectors allow to save storage costs and improve redundancy.
- C. Storage connector service does not require a separate license to send logs to cloud platform.
- D. Cloud-Out connections allow you to send real-time logs to pubic cloud accounts like Amazon S3, Azure Blob , and Google Cloud.

Answer: AD

NEW QUESTION 49

Refer to the exhibit.

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 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 task-list-size : 2000 webservice-proto : tlsv1.3 tlsv1.2	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 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 webservice-proto : tlsv1.3 tlsv1.2
--	--

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 50

What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

Answer: D

NEW QUESTION 52

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 o 100mb a maximum based on the reserved system space.

Answer: CD

NEW QUESTION 57

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 58

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 61

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 66

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: D

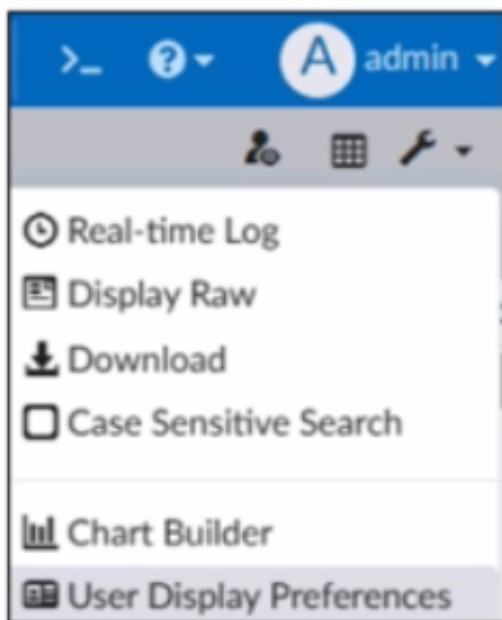
Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 93: The fourth method uses the Fortinet Security Fabric authorization process. This method requires that both FortiGate and FortiAnalyzer are running version 7.0.1 or higher. It is also required that the FortiGate administrator has valid credentials to log in on FortiAnalyzer and complete the registration.

<https://docs.fortinet.com/document/fortianalyzer/7.2.1/administration-guide/13897/adding-a-fortigate-using-secu>

NEW QUESTION 67

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 70

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

NSE5_FAZ-7.2 Practice Exam Features:

- * NSE5_FAZ-7.2 Questions and Answers Updated Frequently
- * NSE5_FAZ-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE5_FAZ-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE5_FAZ-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_FAZ-7.2 Practice Test Here](#)