

Fortinet

Exam Questions NSE5_FAZ-7.0

Fortinet NSE 5 - FortiAnalyzer 7.0



NEW QUESTION 1

What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

- A. Chart Builder
- B. Export to Report Chart
- C. Dataset Library
- D. Custom View

Answer: B

NEW QUESTION 2

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 3

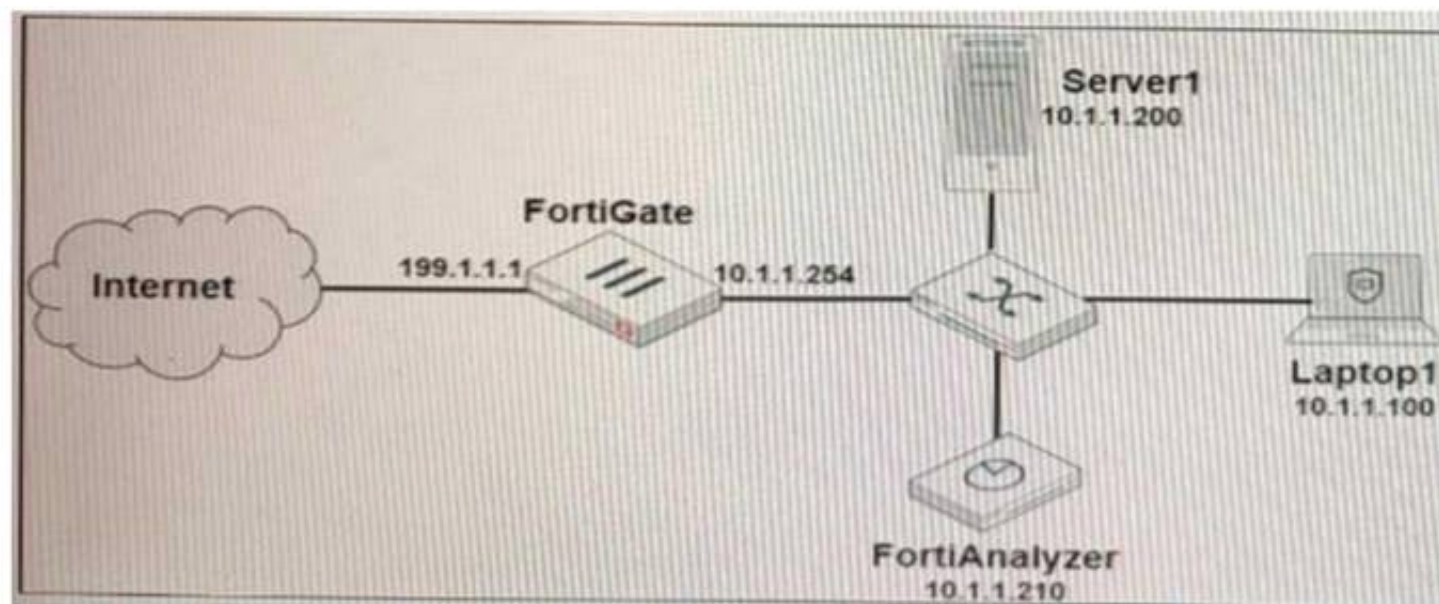
FortiAnalyzer uses the Optimized Fabric Transfer Protocok (OFTP) over SSL for what purpose?

- 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

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 5

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 6

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 7

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 8

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 9

What are offline logs on FortiAnalyzer?

- A. Compressed logs, which are also known as archive logs, are considered to be offline logs.
- B. When you restart FortiAnalyze
- C. all stored logs are considered to be offline logs.
- D. Logs that are indexed and stored in the SQL database.
- E. Logs that are collected from offline devices after they boot up.

Answer: A

NEW QUESTION 10

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 10

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 15

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 18

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 22

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 25

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 30

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 31

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

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

Answer: C

Explanation:

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

NEW QUESTION 35

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 38

Which two statements are true regarding the outbreak detection service? (Choose two.)

- A. New alerts are received by email.
- B. Outbreak alerts are available on the root ADOM only.
- C. An additional license is required.
- D. It automatically downloads new event handlers and reports.

Answer: CD

NEW QUESTION 43

After generating a report, you notice the information you were expecting to see is not included in it. What are two possible reasons for this scenario? (Choose two.)

- A. You enabled auto-cache with extended log filtering.
- B. The logfiled service has not indexed all the expected logs.
- C. The logs were overwritten by the data retention policy.
- D. The time frame selected in the report is wrong.

Answer: BC

NEW QUESTION 44

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 45

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 46

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 49

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 50

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 54

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 59

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 60

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 62

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 63

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 68

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 73

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 77

What is the purpose of trigger variables?

- A. To display statistics about the playbook runtime
- B. To use information from the trigger to filter the action in a task
- C. To provide the trigger information to make the playbook start running
- D. To store the start times of playbooks with On_Schedule triggers

Answer: B

NEW QUESTION 82

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 86

What is the purpose of a dataset query in FortiAnalyzer?

- A. It sorts log data into tables
- B. It extracts the database schema
- C. It retrieves log data from the database
- D. It injects log data into the database

Answer: C

NEW QUESTION 90

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 93

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

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 283: Note that macros are ADOM-specific and supported in FortiGate and FortiCarrier ADOMs only.

NEW QUESTION 95

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>
```

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 128: Are the device analytics logs required for reports in the new ADOM? If so, rebuild the new ADOM database

NEW QUESTION 100

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.

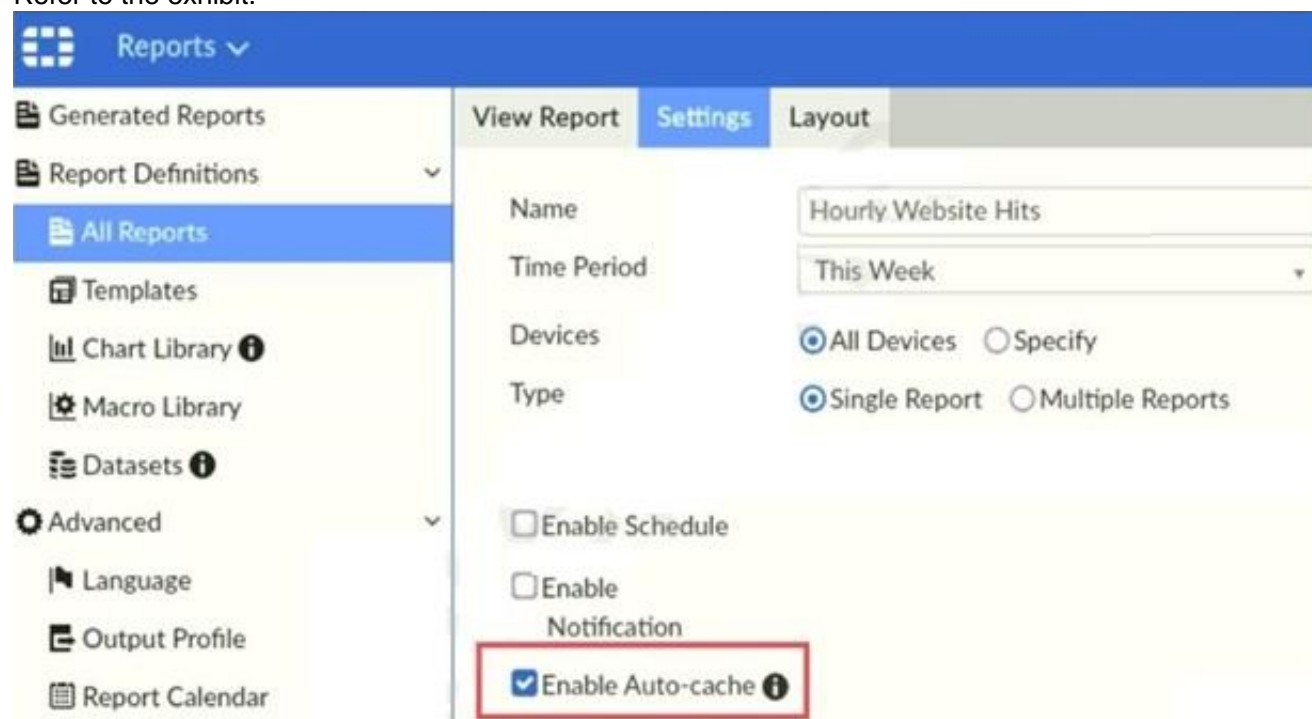
Answer: A

Explanation:

- Super_User, which, like in FortiGate, provides access to all device and system privileges.
 - Standard_User, which provides read and write access to device privileges, but not system privileges.
 - Restricted_User, which provides read access only to device privileges, but not system privileges. Access to the Management extensions is also removed.
 - No_Permissions_User, which provides no system or device privileges. Can be used, for example, to temporarily remove access granted to existing admins.
- FortiAnalyzer_7.0_Study_Guide-Online page 42

NEW QUESTION 103

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 104

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 106

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 109

Which statement correctly describes the management extensions available on FortiAnalyzer?

- A. Management extensions do not require additional licenses.
- B. Management extensions allow FortiAnalyzer to act as a ForbSIEM supervisor.
- C. Management extensions require a dedicated VM for best performance.
- D. Management extensions may require a minimum number of CPU cores to run.

Answer: D

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. 189.

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 189: Review the hardware requirements before you enable a management extension application. Some of them require a minimum amount of memory or a minimum number of CPU cores.

NEW QUESTION 113

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 118

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 123

A playbook contains five tasks in total. An administrator runs the playbook and four out of five tasks finish successfully, but one task fails. What will be the status of the playbook after it is run?

- A. Running
- B. Failed

- C. Upstream_failed
- D. Success

Answer: B

NEW QUESTION 125

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 129

You created a playbook on FortiAnalyzer that uses a FortiOS connector

When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?

- A. FortiAnalyzer Event Handler
- B. Incoming webhook
- C. FortiOS Event Log
- D. Fabric Connector event

Answer: B

Explanation:

"One possible scenario is shown on the slide:

- * 1. Traffic flows through the FortiGate
- * 2. FortiGate sends logs to FortiAnalyzer
- * 3. FortiAnalyzer detects some suspicious traffic and generates an event
- * 4. The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate so that it runs an automation stitch
- * 5. FortiGate runs the automation stitch with the corrective or preventive actions" FortiAnalyzer_7.0_Study_Guide-Online page 228

In order to see the actions related to the FOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on the FortiGate side.

FortiAnalyzer_7.0_Study Guide page no 233

NEW QUESTION 132

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 134

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 : tls1.2 ssl-low-encryption : disable ssl-protocol : tls1.3 tls1.2 : 2000 : tls1.3 tls1.2	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 : tls1.2 ssl-low-encryption : disable ssl-protocol : tls1.3 tls1.2 task-list-size : 2000 web-service-proto : tls1.3 tls1.2
---	--

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 135

What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

- 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

NEW QUESTION 137

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 142

What statements are true regarding FortiAnalyzer's treatment of high availability (HA) clusters? (Choose two)

- A. FortiAnalyzer distinguishes different devices by their serial number.
- B. FortiAnalyzer receives logs from all devices in a cluster.
- C. FortiAnalyzer receives logs only from the primary device in the cluster.
- D. FortiAnalyzer only needs to know the serial number of the primary device in the cluster-it automatically discovers the other devices.

Answer: AB

NEW QUESTION 143

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 147

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 150

What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

Answer: D

NEW QUESTION 154

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 156

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

- A. FortiAnalyzer provides the ability to create custom reports.
- B. FortiAnalyzer glows 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 161

What are analytics logs on FortiAnalyzer?

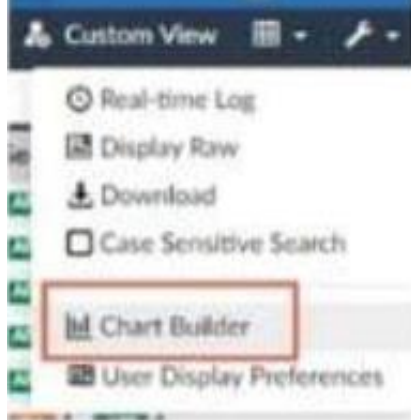
- A. Log type Traffic logs.
- B. Logs that roll over when the log file reaches a specific size.
- C. Logs that are indexed and stored in the SQL.

D. Raw logs that are compressed and saved to a log file.

Answer: C

NEW QUESTION 163

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 167

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 172

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

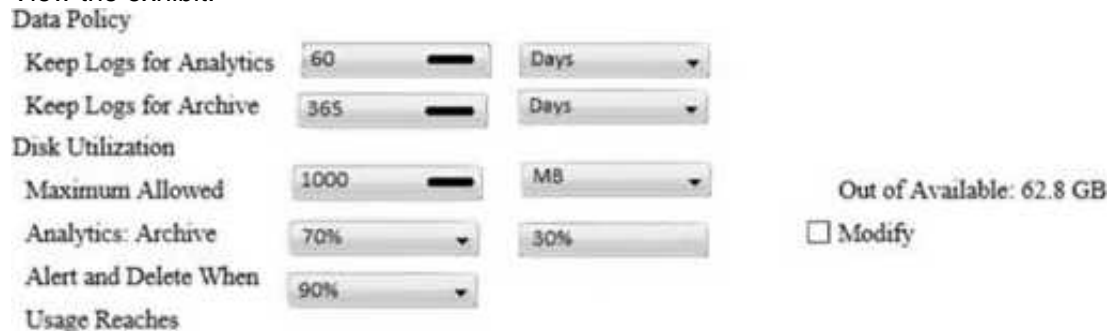
Answer: B

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 176

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 180

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 184

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 189

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?

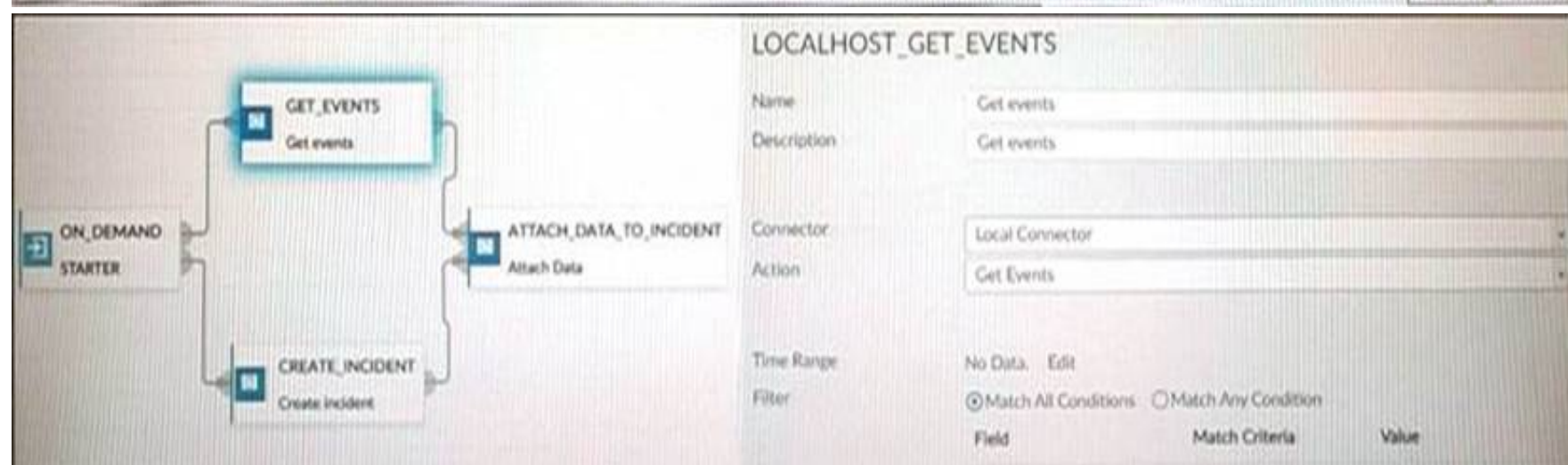
- A. Quota enforcement is acting on analytical data before a report is complete
- B. Logs are rolling before the report is run
- C. CPU resources are too high
- D. Disk utilization for archive logs is set for 15 days

Answer: B

NEW QUESTION 191

Refer to the exhibits.

Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Handler	Tags
> MS.IIS.bdir.HTR.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	5	Low	2 hours ago	2 hours ago	Default-Risky-Destination-Detection-By-Threat	Risky SSL
> HTTP.RequestURL.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	
✓ 10.0.1.10 (7)							Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion MS.IIS.bdir.HTR.Informati...	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 bl...	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.RequestURL.Direct...	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.XS...	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.IIS.bdir.HTR.Informati...	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 bl...	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.RequestURL.Direct...	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.XS...	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.Password.Access blocke...	Mitigated	IPS	2	Medium	2021-12-01 21:31:11	2021-12-01 21:31:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Nikto.Web.Scanner.detect...	Unmitigated	IPS	21	High	2021-12-01 21:31:11	2021-12-01 21:32:36	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: A

NEW QUESTION 193

Which log will generate an event with the status Contained?

- A. An IPS log with action=pass.
- B. A WebFilter log with action=dropped.
- C. An AV log with action=quarantine.
- D. An AppControl log with action=blocked.

Answer: C

NEW QUESTION 198

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

NSE5_FAZ-7.0 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

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_FAZ-7.0 Practice Test Here](#)