

## Exam Questions NSE5\_FAZ-7.0

Fortinet NSE 5 - FortiAnalyzer 7.0

[https://www.2passeasy.com/dumps/NSE5\\_FAZ-7.0/](https://www.2passeasy.com/dumps/NSE5_FAZ-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

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 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

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 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.  
FortiAnalyzer\_7.0\_Study\_Guide-Online page 149

#### NEW QUESTION 7

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 8

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 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 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 10

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 11

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 14

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 15

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 18

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 21

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 26

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 28

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 33

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 38**

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 41**

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 44**

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 45**

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

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

**Answer:** C

**Explanation:**

[https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG\\_FAZ/1100\\_Storage/0017\\_Deleted%20device%20logs.htm](https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG_FAZ/1100_Storage/0017_Deleted%20device%20logs.htm)

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

**NEW QUESTION 48**

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 51**

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 54

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 57

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 58

What happens when the IOC breach detection engine on FortiAnalyzer finds web logs that match a blocklisted IP address?

- A. The endpoint is marked as Compromised and
- B. optionally, can be put in quarantine.
- C. FortiAnalyzer flags the associated host for further analysis.
- D. A new Infected entry is added for the corresponding endpoint.
- E. The detection engine classifies those logs as Suspicious

Answer: A

#### NEW QUESTION 61

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

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

Answer: CD

#### NEW QUESTION 63

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

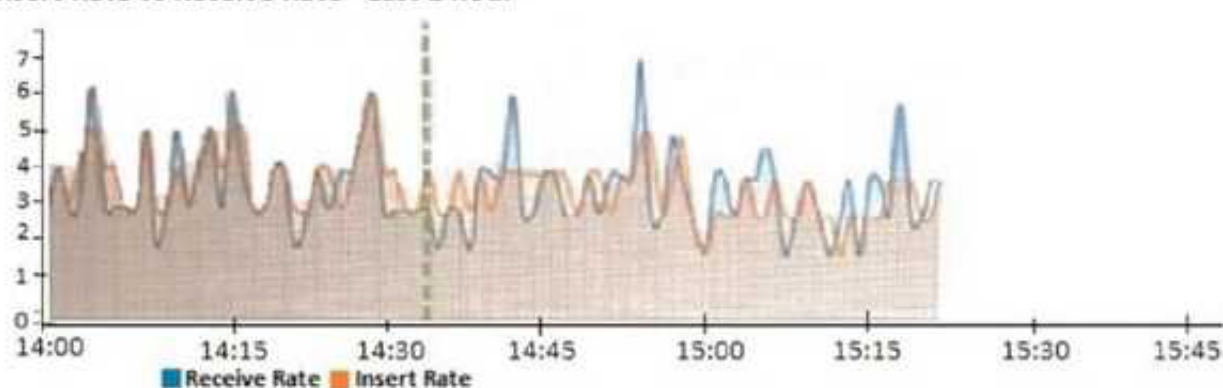
- A. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.
- B. Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.
- C. Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.
- D. Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.

Answer: BD

#### NEW QUESTION 65

View the exhibit.

Insert Rate vs Receive Rate - Last 1 hour



What does the data point at 14:35 tell you?

- A. FortiAnalyzer is dropping logs.
- B. FortiAnalyzer is indexing logs faster than logs are being received.
- C. FortiAnalyzer has temporarily stopped receiving logs so older logs' can be indexed.
- D. The sqlplugind daemon is ahead in indexing by one log.

**Answer:** B

**Explanation:**

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-wi>

#### NEW QUESTION 68

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 70

A play book contains five tasks in total. An administrator executed the playbook and four out of five tasks finished successfully, but one task failed. What will be the status of the playbook after its execution?

- A. Success
- B. Failed
- C. Running
- D. Upstream\_failed

**Answer:** B

**Explanation:**

Playbook jobs that include one or more failed tasks are labeled as Failed in Playbook Monitor. FortiAnalyzer\_7.0\_Study Guide page No: 247

Playbook jobs that include one or more failed tasks are labeled as Failed in Playbook Monitor. A failed status, however, does not mean that all tasks failed. Some individual actions may have been completed successfully.

#### NEW QUESTION 74

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 79

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 83

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 92**

Refer to the exhibit.

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 96**

Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

- A. System information
- B. Logs from registered devices
- C. Report information
- D. Database snapshot

**Answer:** AC

**Explanation:**

What does the System Configuration backup include?



System information, such as the device IP address and administrative user information. Device list, such as any devices you configured to allow log access. Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

FortiAnalyzer\_7.0\_Study\_Guide-Online pag. 29

FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 29: What does the System Configuration backup include?

- System information, such as the device IP address and administrative user information
- Device list, such as any devices you configured to allow log access
- Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

#### NEW QUESTION 101

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 106

Refer to the exhibit.

<p>FortiAnalyzer1# get system status</p> <p>Platform Type : FAZVM64-KVM</p> <p>Platform Full Name : FortiAnalyzer-VM64-KVM</p> <p>Version : v7.2.1-build1215 220809 (GA)</p> <p>Serial Number : FAZ-VM0000065040</p> <p>BIOS version : 04000002</p> <p>Hostname : FortiAnalyzer1</p> <p>Max Number of Admin Domains : 5</p> <p>Admin Domain Configuration : Enabled</p> <p>FIPS Mode : Disabled</p> <p>HA Mode : Stand Alone</p> <p>Branch Point : 1215</p> <p>Release Version Information : GA</p> <p>Time Zone : (GMT-8:00) Pacific Time (US &amp; Canada)</p> <p>Disk Usage : Free 43.60GB, Total 58.80GB</p> <p>File System : Ext4</p> <p>License Status : Valid</p> <p>FortiAnalyzer1# get system global</p> <p>adom-mode : normal</p> <p>adom-select : enable</p> <p>adom-status : enable</p> <p>console-output : standard</p> <p>country-flag : enable</p> <p>enc-algorithm : high</p> <p>ha-member-auto-grouping : enable</p> <p>hostname : FortiAnalyzer2</p> <p>log-checksum : md5</p> <p>log-forward-cache-size : 5</p> <p>log-mode : analyzer</p> <p>longitude : (null)</p> <p>max-aggregation-tasks : 0</p> <p>max-running-reports : 1</p> <p>oftp-ssl-protocol : tlsv1.2</p> <p>ssl-low-encryption : disable</p> <p>ssl-protocol : tlsv1.3 tlsv1.2</p> <p>task-list-size : 2000</p> <p>web-service-protocol : tlsv1.3 tlsv1.2</p>	<p>FortiAnalyzer3# get system status</p> <p>Platform Type : FAZVM64-KVM</p> <p>Platform Full Name : FortiAnalyzer-VM64-KVM</p> <p>Version : v7.2.1-build1215 220809 (GA)</p> <p>Serial Number : FAZ-VM0000065042</p> <p>BIOS version : 04000002</p> <p>Hostname : FortiAnalyzer3</p> <p>Max Number of Admin Domains : 5</p> <p>Admin Domain Configuration : Enabled</p> <p>FIPS Mode : Disabled</p> <p>HA Mode : Stand Alone</p> <p>Branch Point : 1215</p> <p>Release Version Information : GA</p> <p>Time Zone : (GMT-8:00) Pacific Time (US &amp; Canada)</p> <p>Disk Usage : Free 12.98GB, Total 79.80GB</p> <p>File System : Ext4</p> <p>License Status : Valid</p> <p>FortiAnalyzer3# get system global</p> <p>adom-mode : normal</p> <p>adom-select : enable</p> <p>adom-status : enable</p> <p>console-output : standard</p> <p>country-flag : enable</p> <p>enc-algorithm : high</p> <p>ha-member-auto-grouping : enable</p> <p>hostname : FortiAnalyzer3</p> <p>log-checksum : md5</p> <p>log-forward-cache-size : 5</p> <p>log-mode : analyzer</p> <p>longitude : (null)</p> <p>max-aggregation-tasks : 0</p> <p>max-running-reports : 5</p> <p>oftp-ssl-protocol : tlsv1.2</p> <p>ssl-low-encryption : disable</p> <p>ssl-protocol : tlsv1.3 tlsv1.2</p> <p>task-list-size : 2000</p> <p>web-service-protocol : tlsv1.3 tlsv1.2</p>
---	---

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 109

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 114

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 117

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 120

Which daemon is responsible for enforcing the log file size?

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

**Answer:** B

#### Explanation:

FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 121: The logfiled process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes.

#### NEW QUESTION 125

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 128

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 130

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 132

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

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

**Answer:** AB

#### NEW QUESTION 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 140

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 142

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 144

View the exhibit:

**Data Policy**

Keep Logs for Analytics	60	Days
Keep Logs for Archive	365	Days

**Disk Utilization**

Maximum Allowed	1000	MB	Out of Available: 62.8 GB
Analytics: Archive	70%	30%	
Alert and Delete When Usage Reaches	90%		

☐ Modify

What does the 1000MB maximum for disk utilization refer to?

- A. The disk quota for the FortiAnalyzer model
- B. The disk quota for all devices in the ADOM
- C. The disk quota for each device in the ADOM
- D. The disk quota for the ADOM type

**Answer:** B

#### Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-pol>

#### NEW QUESTION 148

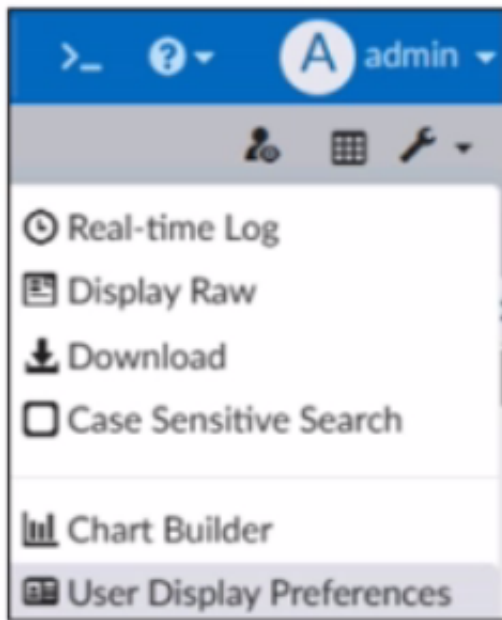
If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

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

**Answer:** D

#### NEW QUESTION 151

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 154

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 157

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.

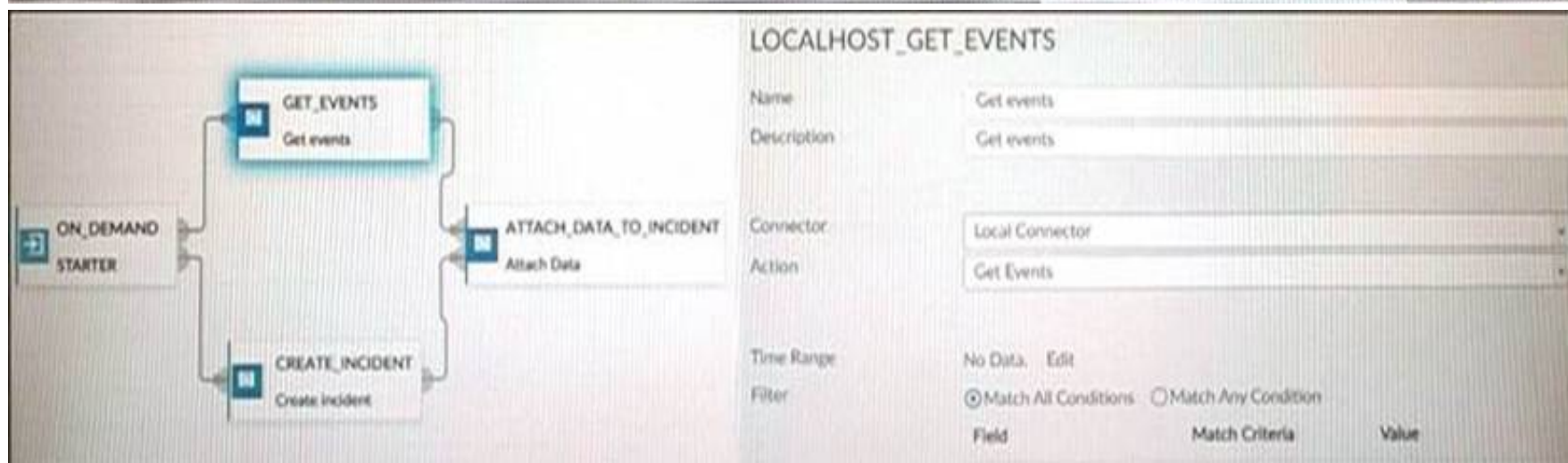
<https://docs.fortinet.com/document/fortianalyzer/7.2.1/administration-guide/13897/adding-a-fortigate-using-secu>

#### NEW QUESTION 161

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 21:32:33	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 21:32:33	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 165

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 168

.....

## 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/](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