

## 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**

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:**

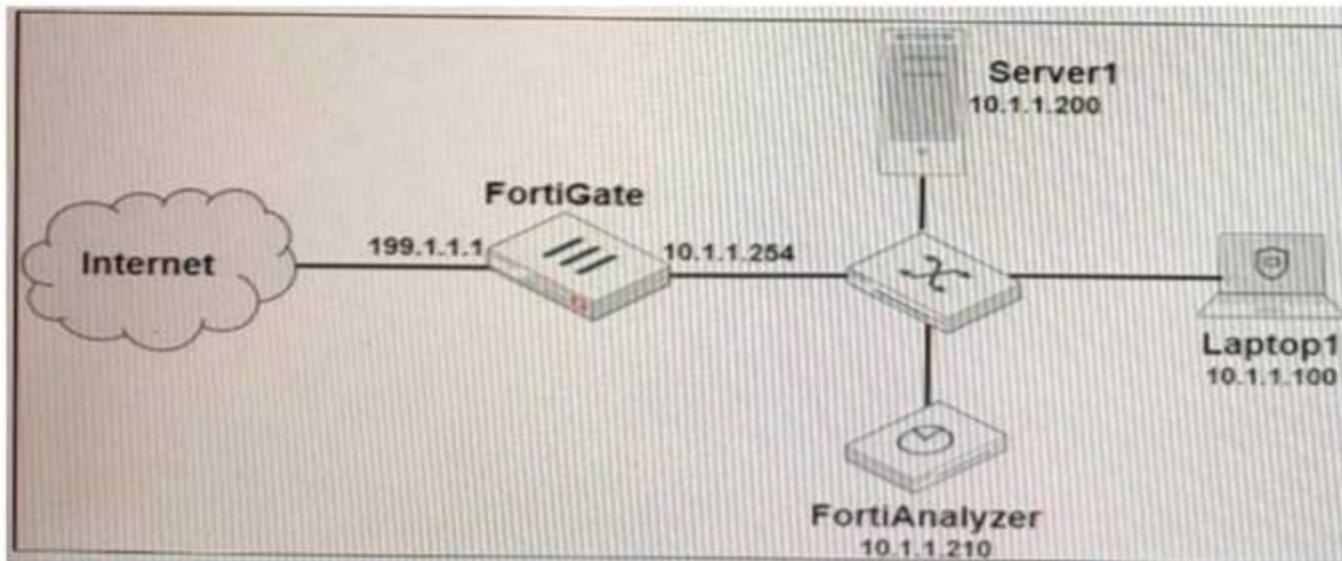
FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 259: The main clauses FortiAnalyzer reports use are as follows:

- 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**

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 3**

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 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**

What are two benefits of using fabric connectors? (Choose two.)

- A. They allow FortiAnalyzer to send logs in real-time to public cloud accounts.
- B. You do not need an additional license to send logs to the cloud platform.
- C. Fabric connectors allow you to improve redundancy.
- D. Using fabric connectors is more efficient than using third-party polling with API.

Answer: AC

**NEW QUESTION 6**

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 7**

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

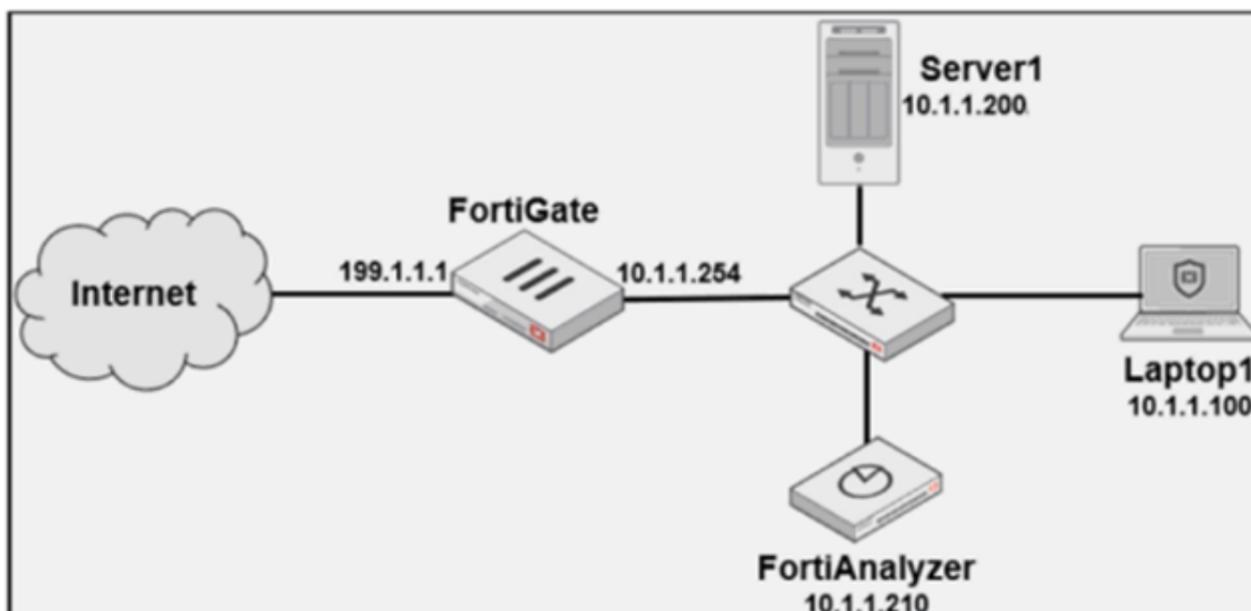
Answer: AC

**Explanation:**

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

**NEW QUESTION 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**

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 10

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 10

By default, what happens when a log file reaches its maximum file size?

- A. FortiAnalyzer overwrites the log files.
- B. FortiAnalyzer stops logging.
- C. FortiAnalyzer rolls the active log by renaming the file.
- D. FortiAnalyzer forwards logs to syslog.

**Answer: C**

#### NEW QUESTION 14

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 18

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 23

In the FortiAnalyzer FortiView, source and destination IP addresses from FortiGate devices are not resolving to a hostname.

How can you resolve the source and destination IP addresses, without introducing any additional performance impact to FortiAnalyzer?

- A. Resolve IP addresses on a per-ADOM basis to reduce delay on FortiView while IPs resolve
- B. Configure # set resolve-ip enable in the system FortiView settings
- C. Configure local DNS servers on FortiAnalyzer
- D. Resolve IP addresses on FortiGate

**Answer: D**

#### Explanation:

<https://packetplant.com/fortigate-and-fortianalyzer-resolve-source-and-destination-ip/>

“As a best practice, it is recommended to resolve IPs on the FortiGate end. This is because you get both source and destination, and it offloads the work from FortiAnalyzer. On FortiAnalyzer, this IP resolution does destination IPs only”

#### NEW QUESTION 28

Which statement describes a dataset in FortiAnalyzer?

- A. They determine what data is retrieved from the databases
- B. They provide the layout used for reports.
- C. They are used to set the data included in template
- D. They define the chart types to be used in report

**Answer: A**

**NEW QUESTION 33**

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 35**

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 37**

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 41**

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 45**

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 48**

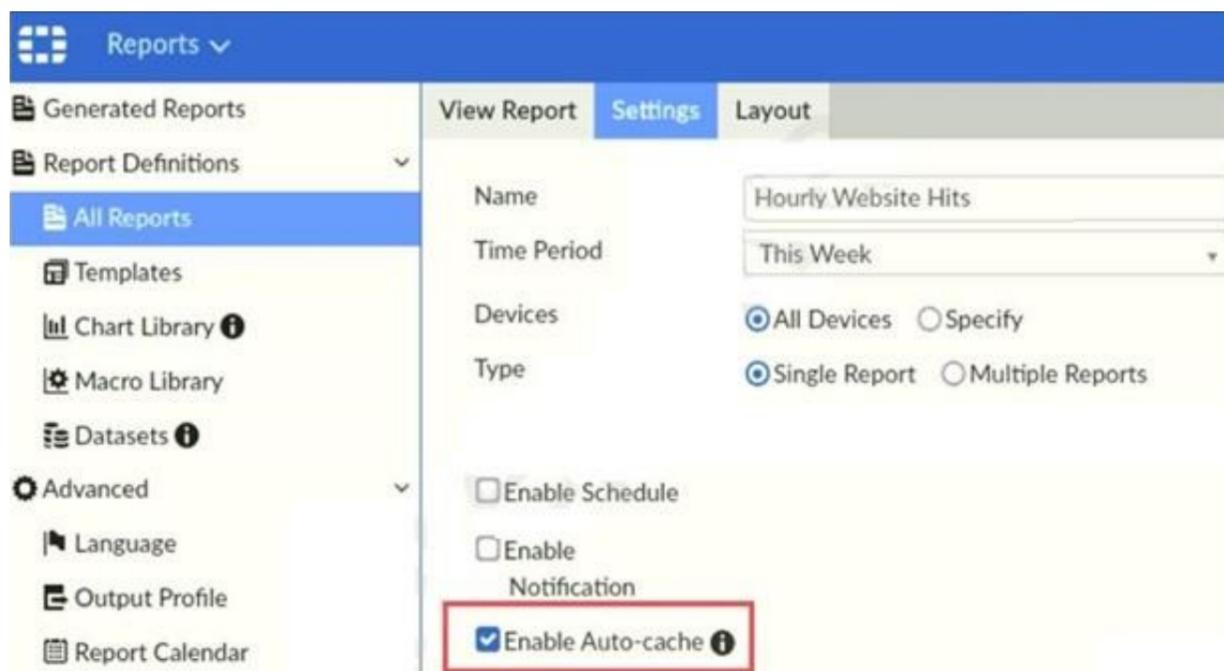
What are the operating modes of FortiAnalyzer? (Choose two)

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

**Answer:** CD

**NEW QUESTION 50**

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 51**

Which daemon is responsible for enforcing raw log file size?

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

**Answer:** A

**NEW QUESTION 54**

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 59**

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 63**

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 65**

What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

- A. Log correlation
- B. Host name resolution
- C. Log collection
- D. Real-time forwarding

**Answer: A**

**NEW QUESTION 67**

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 69**

Refer to the exhibit.

<pre>FortiAnalyzer1# get system status Platform Type           : FAZVM64-KVM Platform Full Name      : FortiAnalyzer-VM64-KVM Version                 : v7.2.1-build1215 220809 (GA) Serial Number           : FAZ-VM0000065040 BIOS version            : 04000002 Hostname                : FortiAnalyzer1 Max Number of Admin Domains : 5 Admin Domain Configuration : Enabled FIPS Mode                : Disabled HA Mode                 : Stand Alone Branch Point            : 1215 Release Version Information : GA Time Zone                : (GMT-8:00) Pacific Time (US &amp; 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                         : 2000                         : tlsv1.3 tlsv1.2</pre>	<pre>FortiAnalyzer3# get system status Platform Type           : FAZVM64-KVM Platform Full Name      : FortiAnalyzer-VM64-KVM Version                 : v7.2.1-build1215 220809 (GA) Serial Number           : FAZ-VM0000065042 BIOS version            : 04000002 Hostname                : FortiAnalyzer3 Max Number of Admin Domains : 5 Admin Domain Configuration : Enabled FIPS Mode                : Disabled HA Mode                 : Stand Alone Branch Point            : 1215 Release Version Information : GA Time Zone                : (GMT-8:00) Pacific Time (US &amp; 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                         : 2000 webbservice-proto       : tlsv1.3 tlsv1.2</pre>
--	--

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 72**

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 75**

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 79**

What is the recommended method of expanding disk space on a FortiAnalyzer VM?

- A. From the VM host manager, add an additional virtual disk and use the #execute lvm extend <disk number> command to expand the storage
- B. From the VM host manager, expand the size of the existing virtual disk
- C. From the VM host manager, expand the size of the existing virtual disk and use the # execute format disk command to reformat the disk
- D. From the VM host manager, add an additional virtual disk and rebuild your RAID array

**Answer:** A

**Explanation:**

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD40848>

**NEW QUESTION 82**

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 83**

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 87**

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 91**

What does the disk status Degraded mean for RAID management?

- A. One or more drives are missing from the FortiAnalyzer unit.
- B. The drive is no longer available to the operating system.
- C. The FortiAnalyzer device is writing to all the hard drives on the device in order to make the array fault tolerant.
- D. The FortiAnalyzer device is writing data to a newly added hard drive in order to restore the hard drive to an optimal state.
- E. The hard drives are no longer being used by the RAID controller.

**Answer:** D

**NEW QUESTION 96**

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 100**

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 103**

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 108**

Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally? (Choose two.)

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

**Answer: AB**

**NEW QUESTION 109**

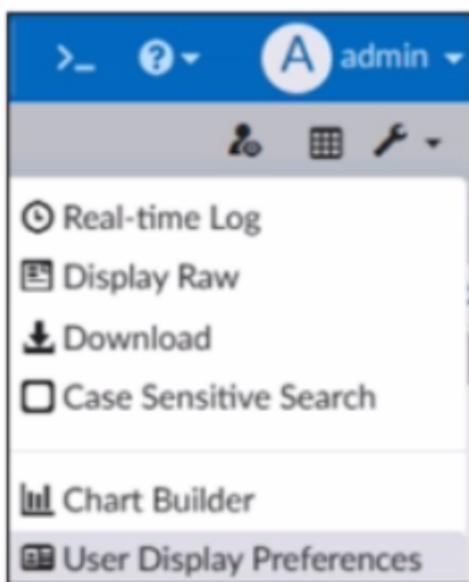
If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

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

**Answer: D**

**NEW QUESTION 110**

Refer to the exhibit.



What is the purpose of using the Chart Builder feature on FortiAnalyzer?

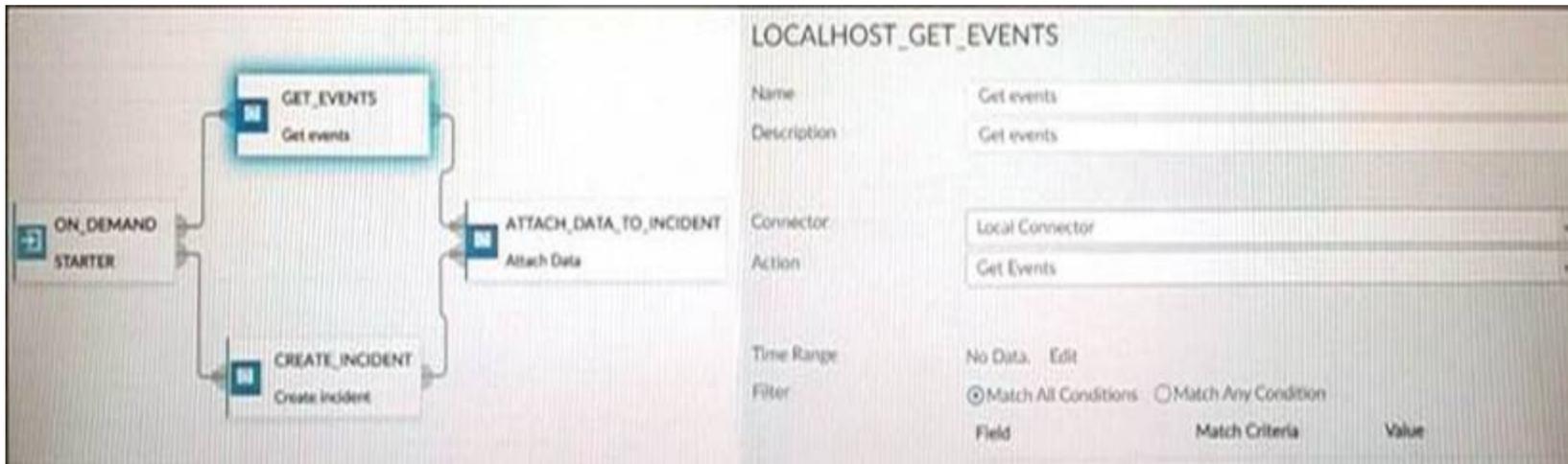
- A. To add a new chart under FortiView to be used in new reports
- B. To build a dataset and chart automatically, based on the filtered search results
- C. To add charts directly to generate reports in the current ADOM
- D. To build a chart automatically based on the top 100 log entries

**Answer: B**

**NEW QUESTION 111**

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.Request.URI.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.Request.URI 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.Request.URI 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 HTPassword.Access blocked	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 114

.....

## 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