PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 5FortiAnalyzer 7.6 Analyst

Fortinet FCP_FAZ_AN-7.6

Version Demo

Total Demo Questions: 10

Total Premium Questions: 107

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction and Initial Configuration	2
Topic 2, Administration and Device Management	8
Topic 3, Logging	24
Topic 4, Reports	26
Topic 5, Events	17
Topic 6, Incidents and Playbooks	23
Topic 7, Threat Hunting	7
Total	107

QUESTION NO: 1

When managing incidents on FortiAnalyzer, what must an analyst be aware of?

A. You can manually attach generated reports to incidents.

B. The status of the incident is always linked to the status of the attached event.

C. Severity incidents rated with the level High have an initial service-level agreement (SLA) response time of 1 hour.

D. Incidents must be acknowledged before they can be analyzed.

ANSWER: A

Explanation:

You can manually attach generated reports to incidents. FortiAnalyzer incident management provides a case-oriented workspace in which analysts can retain investigation context and supporting evidence with the incident record. A generated report can be associated with an incident manually, allowing the analyst to preserve relevant reporting output—such as log summaries, traffic analysis, or a report prepared for escalation—alongside the incident's investigation workflow. This is valuable when an incident must be handed off to another analyst, reviewed by management, or retained for audit and post-incident analysis, because the supporting report remains accessible from the same case record rather than needing to be located separately. The attachment capability therefore helps maintain a complete, traceable incident record and supports consistent SOC investigation procedures. Fortinet documents the incident-management workflow and the available incident actions in the FortiAnalyzer Administration Guide. See the FortiAnalyzer 7.6.0 Administration Guide and the FortiAnalyzer 7.6 documentation library for the applicable product documentation.

QUESTION NO: 2

Which two statements about variables in FortiAnalyzer playbooks are true? (Choose two.)

A. Trigger variables can provide context from the event or incident that started the playbook.

B. A task can use output from an earlier task as input for a later task.

C. Variables are available only when a playbook is run manually.

D. Variables can be configured only in connector settings.

ANSWER: A B

Explanation:

Trigger variables provide information from the condition that started the playbook. A task can use trigger-derived values, such as an event identifier, device name, source address, or incident details, to operate on the same security context that caused the workflow to run.

Task output can also be used by later tasks in the workflow. This allows one task to collect, transform, or retrieve information and then make the result available to a downstream task. These variable capabilities make playbooks reusable and allow actions to use runtime information instead of static configuration values. Fortinet documents playbook variables and task configuration in the FortiAnalyzer 7.6 Administration Guide.

QUESTION NO: 3

After generating a report, you notice the information you were expecting to see is not included in it. However, you confirm that the logs are there:

Which two actions should you perform? (Choose two.)

A. Check the time frame covered by the report.

B. Disable auto-cache.

C. Increase the report utilization quota.

D. Test the dataset.

ANSWER: A D

Explanation:

Check the time frame covered by the report and test the dataset. FortiAnalyzer generates reports using a configured reporting period, so report output includes only data whose timestamps fall within that selected range. Logs can be present and searchable in Log View while still being excluded from a report if the report's start time, end time, or relative time setting does not encompass those events. Confirming the reporting period is therefore essential before investigating the report content further.

Report charts and tables are populated through datasets, which use SQL queries to select, filter, and aggregate the relevant log records. Testing the dataset lets the administrator run its query interactively and inspect whether it returns the expected information with the applicable ADOM, devices, log types, filters, and time selection. This directly validates the data source used by the report component and helps identify whether the expected records are being retrieved before the full report is generated. Fortinet's reporting documentation describes report datasets and the dataset test capability in the FortiAnalyzer Administration Guide: Datasets. General report configuration, including report time periods, is documented in the FortiAnalyzer Administration Guide: Reports.

QUESTION NO: 4

Which log will generate an event with the status Unhandled?

A. An AV log with action=quarantine.

B. An IPS log with action=pass.

C. A WebFilter log will action=dropped.

D. An AppControl log with action=blocked.

ANSWER: B

Explanation:

An IPS log with action=pass generates an event with the status Unhandled because the IPS engine detected traffic matching an IPS signature, but the configured response allowed that traffic to continue. FortiAnalyzer correlates security logs into events and uses the enforcement outcome recorded by the originating FortiGate to help establish the event status. A detected intrusion that is passed has not been blocked, reset, quarantined, or otherwise remediated at the time of detection. Therefore, the event remains an outstanding security condition requiring attention, which is represented by the Unhandled status.

This distinction is important operationally: detection alone does not mean the threat has been contained. IPS signatures can be configured with different actions, and a pass action records the detection while permitting the session or traffic. Analysts should treat such events as evidence of potentially malicious activity that was observed but not automatically stopped, then investigate the affected host, traffic, signature context, and relevant policy configuration. FortiAnalyzer event-management concepts and event status workflows are documented in the FortiAnalyzer 7.6 Administration Guide. The IPS log fields and action values generated by FortiGate are described in the FortiOS Log Message Reference.

QUESTION NO: 5

You discover that a few reports are taking a long time to generate. Which two steps can you take to troubleshoot? (Choose two.)

A. Remove old reports from the hcache

B. Enable auto-cache and run the reports again

C. Increase the ADOM reports quota

D. Review report diagnostics

ANSWER: B D

Explanation:

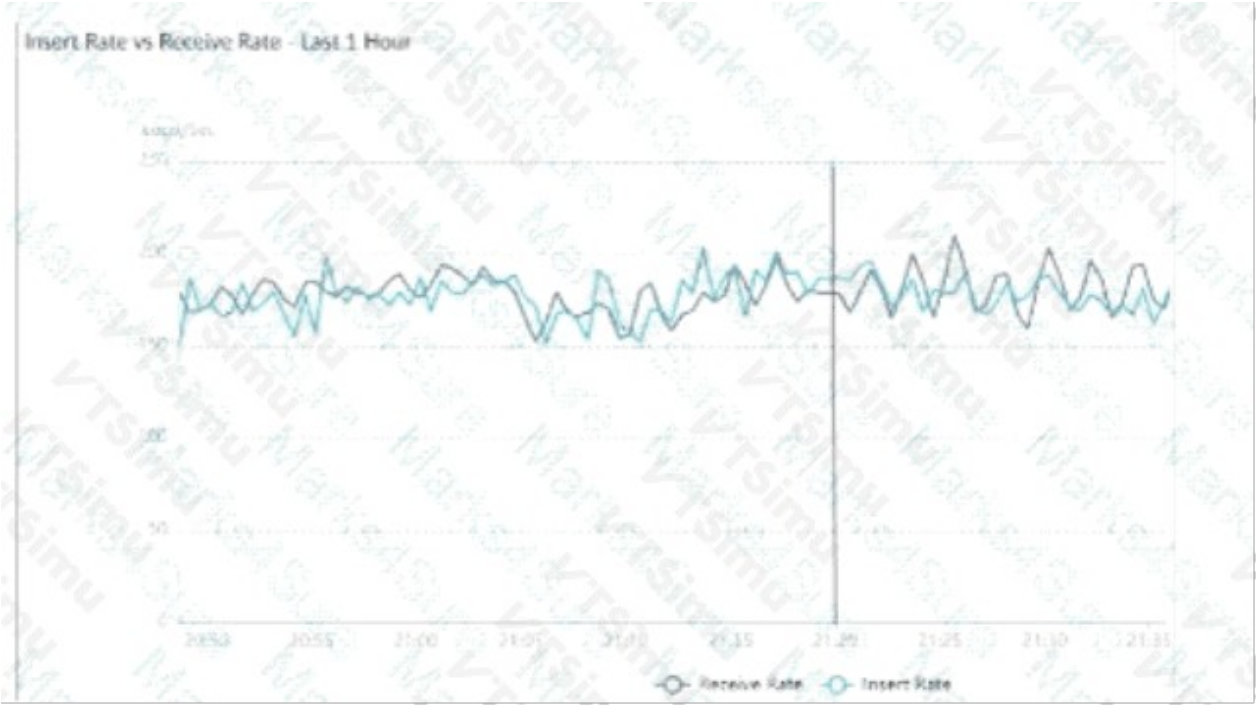
Review report diagnostics is appropriate because FortiAnalyzer includes report diagnostic information that exposes the stages involved in generating a report. Reviewing this output helps an administrator identify whether execution time is being consumed by dataset queries, SQL processing, cache operations, log retrieval, or report rendering. This evidence is essential when only a small number of reports are affected, since it enables the administrator to focus remediation on the specific report components and data-processing activity responsible for the delay.

Enable auto-cache and run the reports again is also appropriate because report caching can reduce the work required during subsequent report generation. Auto-cache allows FortiAnalyzer to prepare and retain data used by report datasets, including historical cache data where applicable. Re-running the affected reports after enabling this capability verifies whether reused or preprocessed data improves completion time, particularly for reports that query large log volumes or use computationally intensive datasets. These actions combine performance evidence with a supported optimization mechanism, allowing the administrator to diagnose and improve the slow reports without broadly changing unrelated ADOM settings. Fortinet's reporting guidance is available in the FortiAnalyzer 7.6 Administration Guide and the FortiAnalyzer 7.6 documentation portal.

QUESTION NO: 6 - (SIMULATION)

SIMULATION

Refer to Exhibit:



What does the data point at 21:20 indicate?

ANSWER: See the explanation for the answer

Explanation:

Answer: At **21:20**, the **Insert Rate is higher than the Receive Rate**.

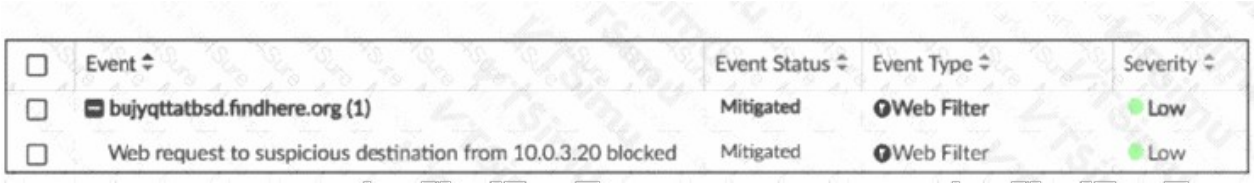
This means FortiAnalyzer is inserting/indexing logs into its database faster than it is receiving new logs at that time. Therefore, it is processing any accumulated log queue (catching up), rather than creating an indexing backlog.

Receive Rate: rate of incoming raw logs.
Insert Rate: rate at which FortiAnalyzer processes and inserts/indexes logs.

QUESTION NO: 7 - (SIMULATION)

SIMULATION

(Refer to the exhibit.



Which statement about the displayed event is correct? (Choose one answer)

ANSWER: See the explanation for the answer

Explanation:

Correct statement: The suspicious web request from `10.0.3.20` was blocked, and the event was successfully mitigated.

QUESTION NO: 8

Which three tasks can be performed on FortiAnalyzer using FortiAI? (Choose three.)

A. Configure site-to-site VPN using FortiAI.

B. Perform Incident investigation and response.

C. Identify potential impacts and recommend remediation.

D. Configure SD-WAN overlay using FortiAI.

E. Perform threat hunting.

ANSWER: B C E

Explanation:

FortiAI in FortiAnalyzer is designed to accelerate security-operations analysis by applying generative-AI assistance to the telemetry, incidents, and analytics available in FortiAnalyzer. **Perform Incident investigation and response.** is correct because FortiAI can help an analyst investigate a detected incident by interpreting the available security context, summarizing relevant findings, and assisting with response-oriented analysis. This reduces the time required to move from an alert to an informed investigation.

Identify potential impacts and recommend remediation. is also a FortiAI capability. During analysis, FortiAI can assist in assessing the possible effect of suspicious activity and produce relevant remediation guidance. This supports informed analyst decisions and helps teams prioritize containment and recovery actions using the incident evidence available in FortiAnalyzer.

Perform threat hunting. is correct because FortiAI supports natural-language, analyst-led exploration of log data and security findings. Analysts can use this assistance to investigate suspicious behaviors, identify related activity, and search for indicators or patterns across the centralized data retained by FortiAnalyzer. Fortinet documents FortiAnalyzer AI-assisted operations in the FortiAnalyzer 7.6 Administration Guide and provides product context at FortiAnalyzer.

QUESTION NO: 9

Which statement about the FortiSOAR management extension is correct?

A. It requires a FortiManager configured to manage FortiGate.

B. It runs as a docker container on FortiAnalyzer.

C. It requires a dedicated FortiSOAR device or VM.

D. It does not include a limited trial by default.

ANSWER: B

Explanation:

It runs as a docker container on FortiAnalyzer. FortiSOAR Management Extension is a containerized FortiSOAR deployment that FortiAnalyzer hosts locally through its Management Extensions framework. This architecture integrates SOAR functions with FortiAnalyzer operations while retaining the extension as an application running on the FortiAnalyzer appliance or VM, rather than treating it as a separately deployed full FortiSOAR instance. Administrators install, configure, and access the extension from the FortiAnalyzer management-extension environment, allowing FortiAnalyzer data and workflows to be used for orchestration and response activities.

Fortinet describes Management Extensions as applications that run in Docker containers on FortiAnalyzer. The FortiSOAR Management Extension is specifically designed for this supported container-based hosting model and is managed as part of the FortiAnalyzer platform. This distinction is important when planning resources and deployment: the relevant FortiAnalyzer system must have sufficient capacity for the extension and its associated workloads. For Fortinet's product documentation and Management Extensions context, see the FortiAnalyzer 7.6 documentation portal and the FortiAnalyzer 7.6 Administration Guide.

QUESTION NO: 10

What is the relationship between a FortiAnalyzer dataset and a chart?

A. A chart uses a dataset as its data source.

B. A dataset uses a chart to define its SQL query.

C. A chart is required to archive logs.

D. A dataset can be used only by one report template.

ANSWER: A

Explanation:

A dataset supplies the SQL query and resulting data that a chart uses for presentation. The dataset determines which log records are selected, filtered, grouped, or aggregated. The chart then defines how those results are displayed, such as in a table, bar chart, pie chart, or line chart.

This separation allows administrators to reuse the same dataset in more than one chart while applying different visualizations to the returned data. Fortinet documents datasets and charts as reporting-library components in the FortiAnalyzer 7.6 Administration Guide.