



Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 1

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

Which two statements are correct regarding the export and import of playbooks? (Choose two.)

- A. You can import a playbook even if there is another one with the same name in the destination.
- B. Playbooks can be exported and imported only within the same FortiAnalyzer device.
- C. You can export only one playbook at a time.
- D. A playbook that was disabled when it was exported will be disabled when it is imported.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 2

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 3

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

Which statement about the FortiSIEM management extension is correct?

- A. Allows you to manage the entire life cycle of a threat or breach.
- B. Its use of the available disk space is capped at 50%.
- C. It requires a licensed FortiSIEM supervisor.
- D. It can be installed as a dedicated VM.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 4

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 5

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 6

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

Which statement describes a dataset in FortiAnalyzer?

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

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 7

Topic #: 1

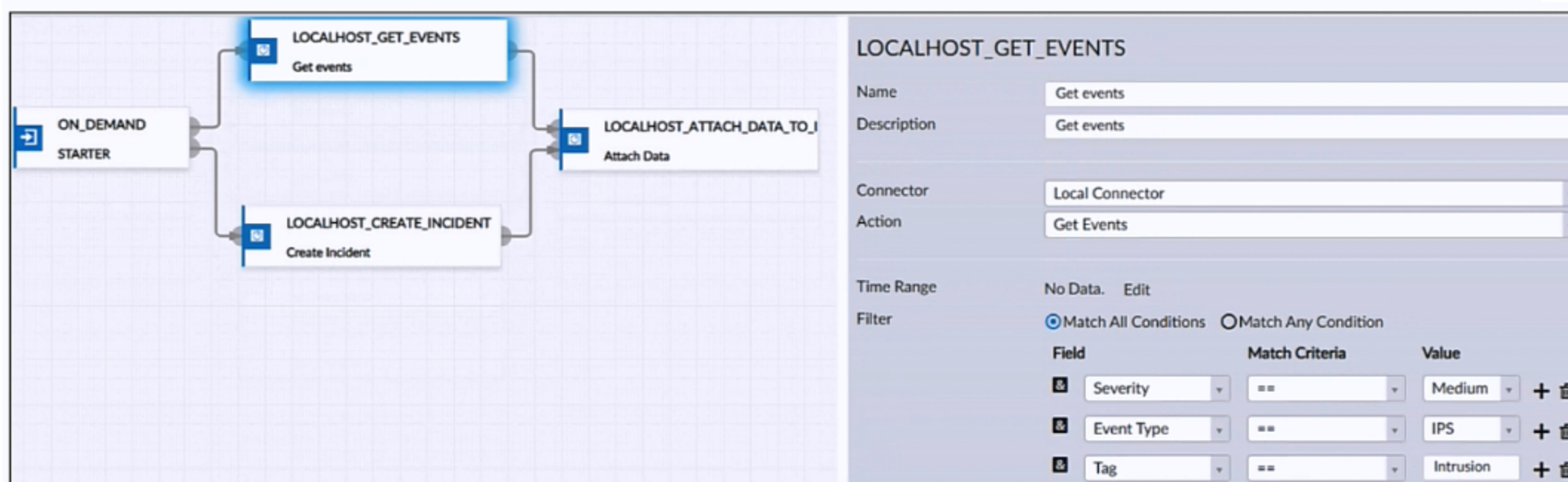
[\[All NSE5\\_FAZ-7.2 Questions\]](#)

Refer to the exhibits.

### EVENT STATUS

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	
> PHP.URI.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)								
Internal intrusion MS.IIS.bdir.HTR.Informati...	Mitigated	● IPS	2	● Medium	2022-12-01 21:32:31	2022-12-01 21:32:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion PHP.URI.Code.Injection bl...	Mitigated	● IPS	2	● Medium	2022-12-01 21:32:11	2022-12-01 21:32:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Insecure SSL connection blocked	Mitigated	⚙ SSL	5	● Low	2022-12-01 21:32:01	2022-12-01 21:32:01	Default-Risky-Destination-Detection-By-Endpoint	Risky SSL
Internal intrusion HTTP.Request.URI.Direct...	Mitigated	● IPS	2	● Medium	2022-12-01 21:31:51	2022-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Apache.Expect.Header.XS...	Mitigated	● IPS	2	● Medium	2022-12-01 21:31:31	2022-12-01 21:31:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion HTPasswd.Access blocked	Mitigated	● IPS	2	● Medium	2022-12-01 21:31:11	2022-12-01 21:31:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Nikto.Web.Scanner detect...	Unhandled	● IPS	21	● High	2022-12-01 21:31:11	2022-12-01 21:32:36	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
~ 10.200.1.254 (6)								
Internal intrusion MS.IIS.bdir.HTR.Informati...	Mitigated	● IPS	2	● Medium	2022-12-01 21:32:31	2022-12-01 21:32:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion PHP.URI.Code.Injection bl...	Mitigated	● IPS	2	● Medium	2022-12-01 21:32:11	2022-12-01 21:32:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion HTTP.Request.URI.Direct...	Mitigated	● IPS	2	● Medium	2022-12-01 21:31:51	2022-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Apache.Expect.Header.XS...	Mitigated	● IPS	2	● Medium	2022-12-01 21:31:31	2022-12-01 21:31:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion HTPasswd.Access blocked	Mitigated	● IPS	2	● Medium	2022-12-01 21:31:11	2022-12-01 21:31:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature
Internal intrusion Nikto.Web.Scanner detect...	Unhandled	● IPS	21	● High	2022-12-01 21:31:11	2022-12-01 21:32:36	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature

### LOCAL HOST



The diagram shows a playbook starting with an ON\_DEMAND STARTER, which branches into two parallel tasks: LOCALHOST\_GET\_EVENTS (Get events) and LOCALHOST\_CREATE\_INCIDENT (Create Incident). Both tasks then feed into a single task: LOCALHOST\_ATTACH\_DATA\_TO\_I (Attach Data).

**LOCALHOST\_GET\_EVENTS Configuration:**

- Name: Get events
- Description: Get events
- Connector: Local Connector
- Action: Get Events
- Time Range: No Data. Edit
- Filter:
  - Match All Conditions  Match Any Condition
  - Severity == Medium
  - Event Type == IPS
  - Tag == Intrusion

How many events will be added to the incident created after running this playbook?

- A. Thirteen events will be added.
- B. Five events will be added.
- C. No events will be added.
- D. Ten events will be added.

Show Suggested Answer

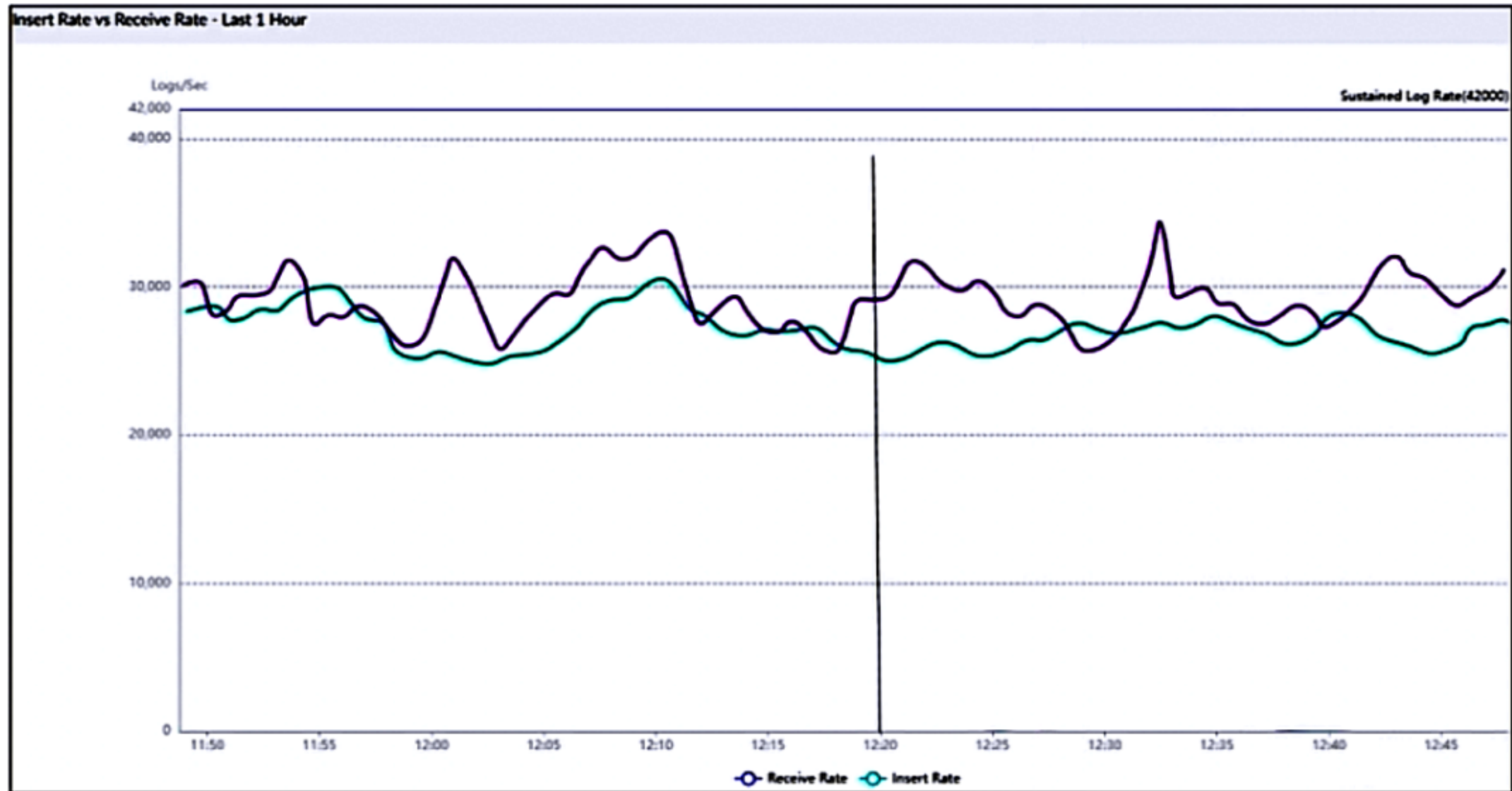
Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 8

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

Refer to the exhibit.



What does the data point at 12:20 indicate?

- A. The performance of FortiAnalyzer is below the baseline.
- B. FortiAnalyzer is using its cache to avoid dropping logs.
- C. The log insert lag time is increasing.
- D. The sqlplugind service is caught up with new logs.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 9

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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. Fabric Connector event
- D. FortiOS Event Log

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 10

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

- A. Outbreak alert services
- B. FortiView Monitor
- C. Threat hunting
- D. Incidents dashboard

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 11

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

Which log will generate an event with the status Contained?

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

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 12

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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

Show Suggested Answer



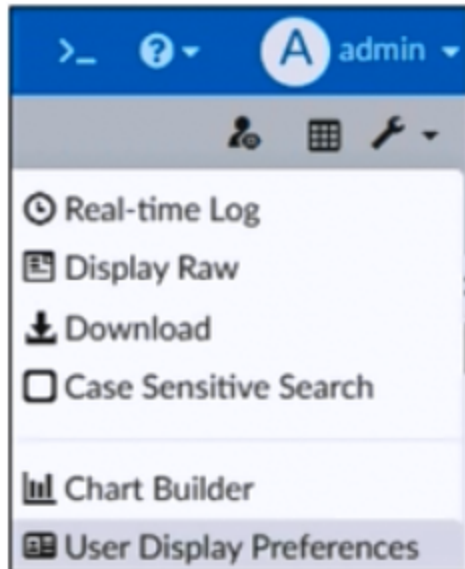
Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 13

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 14

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 15

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 16

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

Why must you wait for several minutes before you run a playbook that you just created?

- A. FortiAnalyzer needs that time to parse the new playbook.
- B. FortiAnalyzer needs that time to back up the current playbooks.
- C. FortiAnalyzer needs that time to ensure there are no other playbooks running.
- D. FortiAnalyzer needs that time to debug the new playbook.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 17

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

Refer to the exhibit.

<b>FortiAnalyzer1# get system status</b> 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	<b>FortiAnalyzer2# get system status</b> Platform Type : FAZVM64-KVM Platform Full Name : FortiAnalyzer-VM64-KVM Version : v7.2.1-build1215 220809 (GA) Serial Number : FAZ-VM0000065041 BIOS version : 04000002 Hostname : FortiAnalyzer2 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 45.75GB, Total 58.80GB File System : Ext4 License Status : Valid	<b>FortiAnalyzer3# get system status</b> 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
<b>FortiAnalyzer1# get system global</b> adom-mode : normal adom-select : enable adom-status : enable console-output : standard country-flag : enable enc-algorithm : high ha-member-auto-grouping : enable hostname : FortiAnalyzer1 log-checksum : md5 log-forward-cache-size : 5 log-mode : analyzer longitude : (null) max-aggregation-tasks : 0 max-running-reports : 1 oftp-ssl-protocol : tlsv1.2 ssl-low-encryption : disable ssl-protocol : tlsv1.3 tlsv1.2 task-list-size : 2000 webservice-proto : tlsv1.3 tlsv1.2	<b>FortiAnalyzer2# get system global</b> adom-mode : normal adom-select : enable adom-status : enable console-output : standard country-flag : enable enc-algorithm : high ha-member-auto-grouping : enable hostname : FortiAnalyzer2 log-checksum : md5 log-forward-cache-size : 5 log-mode : analyzer longitude : (null) max-aggregation-tasks : 0 max-running-reports : 1 oftp-ssl-protocol : tlsv1.2 ssl-low-encryption : disable ssl-protocol : tlsv1.3 tlsv1.2 task-list-size : 2000 webservice-proto : tlsv1.3 tlsv1.2	<b>FortiAnalyzer3# get system global</b> adom-mode : normal adom-select : enable adom-status : enable console-output : standard country-flag : enable enc-algorithm : high ha-member-auto-grouping : enable hostname : FortiAnalyzer3 log-checksum : md5 log-forward-cache-size : 5 log-mode : analyzer longitude : (null) max-aggregation-tasks : 0 max-running-reports : 5 oftp-ssl-protocol : tlsv1.2 ssl-low-encryption : disable ssl-protocol : tlsv1.3 tlsv1.2 task-list-size : 2000 webservice-proto : tlsv1.3 tlsv1.2

Based on the partial outputs displayed, which devices can be members of a FortiAnalyzer Fabric?

- A. FortiAnalyzer1 and FortiAnalyzer3
- B. FortiAnalyzer1 and FortiAnalyzer2
- C. All devices listed can be members
- D. FortiAnalyzer2 and FortiAnalyzer3

Show Suggested Answer

Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 18

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

An administrator has configured the following settings:

```
config system fortiview setting
```

```
set resolve-ip enable
```

```
end
```

What is the significance of running 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. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.
- D. You must configure local DNS servers on FortiGate for this command to resolve IP addresses on FortiAnalyzer.

Show Suggested Answer



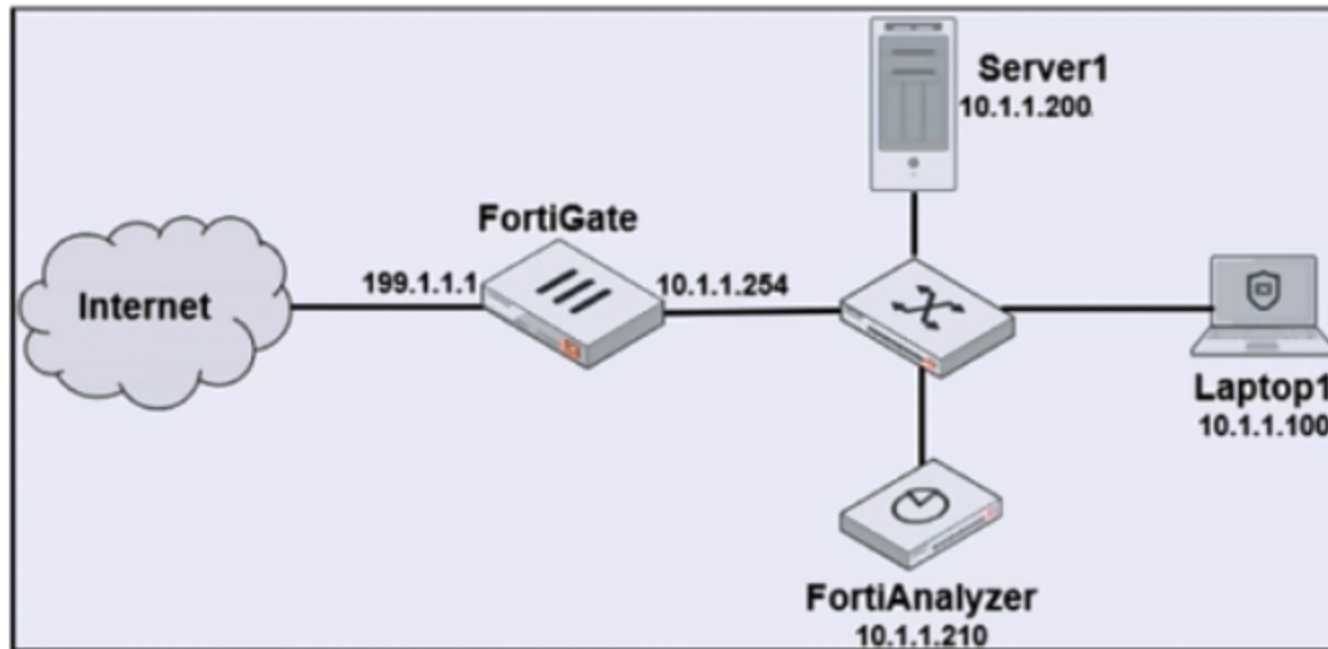
Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 19

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

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`

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 20

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

Which two actions should an administrator take to view Compromised Hosts on FortiAnalyzer? (Choose two.)

- A. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
- B. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up to date.
- C. Make sure all endpoints are reachable by FortiAnalyzer.
- D. Enable device detection on the FortiGate devices that are sending logs to FortiAnalyzer.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 21

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 22

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 23

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

Why run the command `diagnose sql status sqlplugind`?

- A. To list the current SQL processes running
- B. To check what is the database log insertion status
- C. To display the SQL query connections and hcache status
- D. To view the current hcache size

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 24

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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.

Show Suggested Answer







Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 25

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 26

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 27

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 28

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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

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

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 29

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

---

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.

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FAZ-7.2

Question #: 30

Topic #: 1

[\[All NSE5\\_FAZ-7.2 Questions\]](#)

Refer to the exhibit.

Event	Event Status	Event Type	Count	Severity
√ ffb07fb6990e3b5da86d66d43b488a967c.ws (2)				
Web traffic to C&C from 10.0.3.20 detected	Unhandled	Web Filter	1	Critical

Which statement is correct regarding the event displayed?

- A. The security event risk is considered open.
- B. The security risk was blocked or dropped.
- C. The risk source is isolated.
- D. An incident was created from this event.

Show Suggested Answer