Vendor: Fortinet

Exam Code: NSE5_FAZ-7.2

Exam Name: Fortinet NSE 5 - FortiAnalyzer 7.2 Analyst

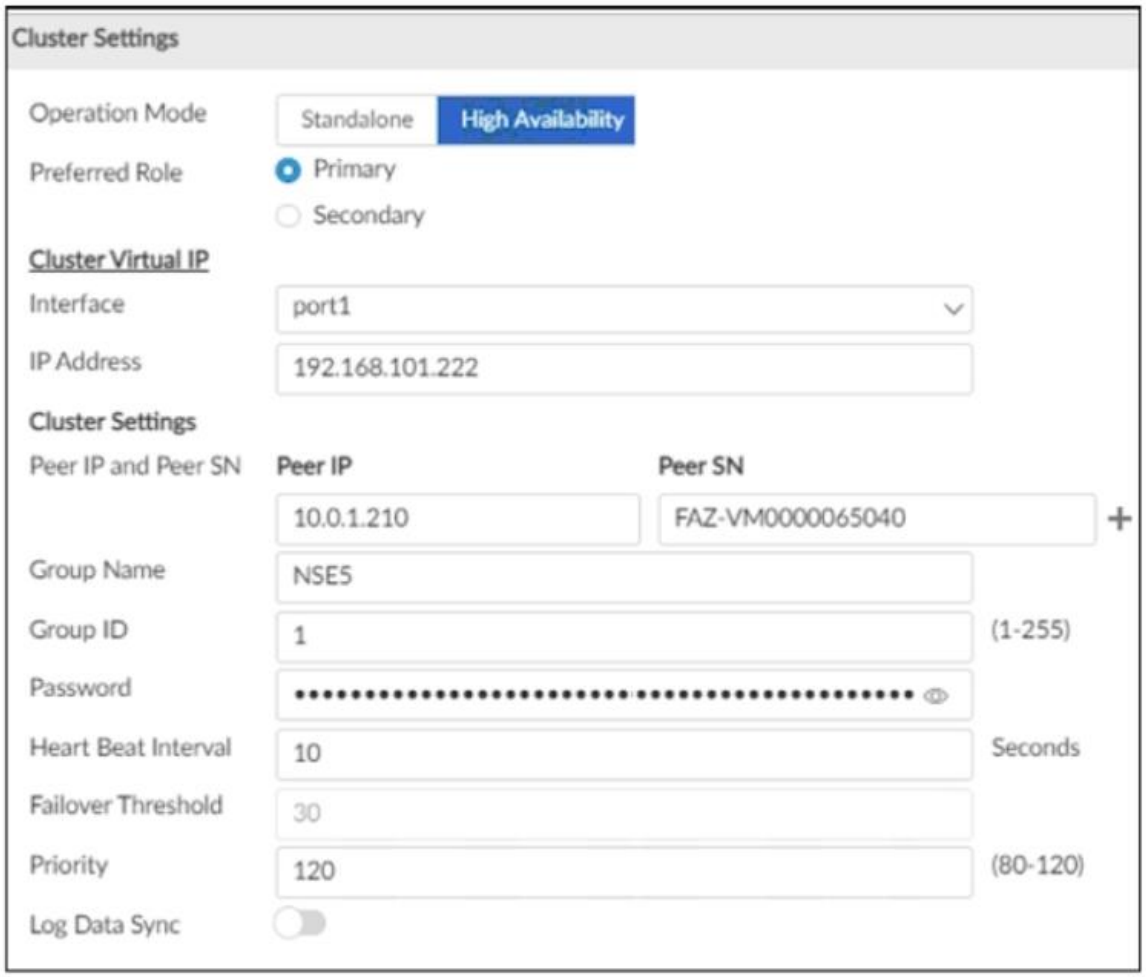
Version: DEMO

QUESTION 1
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
Explanation:
Another common way to load data into a DataSet is to use the DataAdapter class to retrieve data from the database.

QUESTION 2
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:
In the Cluster Virtual IP section, you need to select the interface and type the IP address for which the FAZ device is to provide redundancy. This is the IP that other devices need to point to send their logs once the cluster is up.

QUESTION 3
You crested a playbook on FortiAnalyzer that uses a FortiOS connector.
When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?

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

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

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: AB
Explanation:
A. This is because the fetch client uses the FortiAnalyzer API to retrieve logs, and the API does not require the devices to be added to the local Device Manager.
B. This can be useful if you only want to fetch logs from a specific device, or if you want to exclude logs from certain devices.

QUESTION 5
Which two statements are true regarding the outbreak detection service? (Choose two.)

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

Answer: CD
Explanation:
C. An additional license is required. The Outbreak Detection Service is a licensed feature that must be purchased separately.
D. It automatically downloads new event handlers and reports. When a new outbreak is detected,

the Outbreak Detection Service will automatically download the associated event handlers and reports to the FortiAnalyzer.

QUESTION 6
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
Explanation:
Auto-cache is a feature that allows you to store the results of a report in a hard-cache database. This can significantly reduce the time it takes to generate the report, as the FortiAnalyzer does not need to re-run the query each time the report is requested.
The hard-cache database is updated automatically when new logs are received. This ensures that the report always reflects the latest data.

QUESTION 7
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.

Answer: A
Explanation:
When you create a new playbook, FortiAnalyzer needs to parse the playbook file to understand the commands and tasks that it contains. This can take a few minutes, depending on the size and complexity of the playbook.

QUESTION 8
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
Explanation:
Online logs are the logs that are currently being processed by FortiAnalyzer. They are not yet rolled over or archived. They can be viewed using the Log Browse feature in FortiAnalyzer.

QUESTION 9
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
Explanation:
To do this, follow these steps:
1. Go to Incidents & Events > Incidents.
2. Select the incident that you want to attach the report to.
3. Click the Properties tab.
4. In the Reports section, click Add.
5. Select the report that you want to attach.
6. Click OK.
The report will be attached to the incident.

QUESTION 10
Which item must you configure on FortiAnalyzer to email generated reports automatically?

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

Answer: A
Explanation:
The Output profile specifies the email server that will be used to send the reports, as well as the email address that will receive the reports.

QUESTION 11
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: A
Explanation:
The FortiSOAR management extension is a software application that runs on FortiManager. It allows you to manage FortiSOAR instances, including creating and managing playbooks, tasks, and automations.

QUESTION 12
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

Answer: C
Explanation:
The diagnose sql command is a set of commands that can be used to diagnose the SQL database on a FortiAnalyzer. The status subcommand displays the current status of the SQL database, including the number of active query connections and the hcache status.
The sqlplugind parameter specifies that the status of the SQL plugin should be displayed. The SQL plugin is responsible for handling SQL queries on the FortiAnalyzer.

QUESTION 13
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.

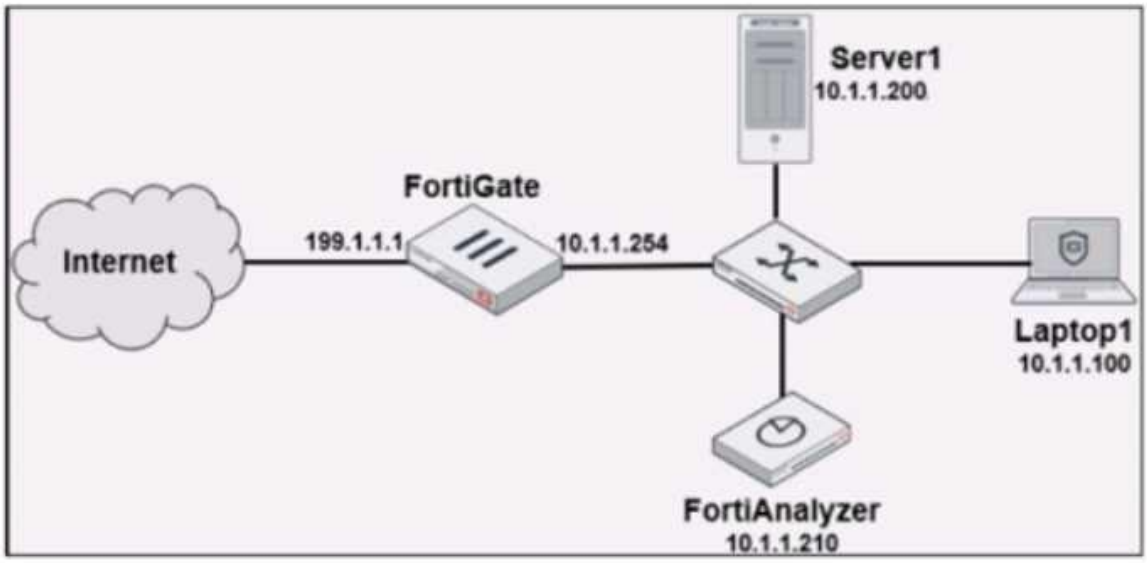
Answer: AD
Explanation:
A. They allow FortiAnalyzer to send logs in real-time to public cloud accounts. Fabric connectors are a way to send logs from FortiAnalyzer to cloud-based services, such as Splunk and Microsoft Azure Sentinel. This allows you to centralize your logs and get insights from them in real time.
D. Using fabric connectors is more efficient than using third-party polling with API. Fabric connectors use a direct connection between FortiAnalyzer and the cloud service, which is more efficient than polling the cloud service with an API.

QUESTION 14
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
Explanation:
The contained status is used to indicate that an event has been detected and mitigated. In the case of an AV log with action=quarantine, the malware has been detected and isolated from the system.

QUESTION 15
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

QUESTION 16
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
Explanation:
B. The logfiled service has not indexed all the expected logs. The logfiled service is responsible for indexing the logs that are received by FortiAnalyzer. If the logfiled service has not indexed all the expected logs, then the information from those logs will not be included in the report.
C. The logs were overwritten by the data retention policy. FortiAnalyzer has a data retention policy that specifies how long logs are kept. If the logs that you are interested in were overwritten by the data retention policy, then they will not be included in the report.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**