Free Questions for NSE5_FAZ-7.2 by dumpshq

Shared by Cooke on 23-08-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which statement about the FortiSIEM management extension is correct?

Options:

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.

Answer:

A

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

What does the data point at 12:20 indicate?

Options:

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.

Answer:

C

Question 3

Question Type: **MultipleChoice**

Refer to the exhibit.

```
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 & 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
```

```
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 & 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
```

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

Options:

A- FortiAnalyzerl and FortiAnalyzer3

B- FortiAnalyzer1 and FortiAnalyzer2

C- All devices listed can be members

D- FortiAnalyzer2 and FortiAnalyzer3

Answer:

C

Question 4

Question Type: **MultipleChoice**

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

Options:

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

Answer:

A

Question 5

Question Type: **MultipleChoice**

Which statement about sending notifications with incident updates is true?

Options:

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

Question 6

Question Type: MultipleChoice

What is the purpose of trigger variables?

Options:

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

Question 7

Question Type: MultipleChoice

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?

Options:

A- Running

B- Failed

C- Upstream_failed

D- Success

Answer:

B

Question 8

Question Type: MultipleChoice

Which statement describes a dataset in FortiAnalyzer?

Options:

A- They determine what data is retrieved from the database.

B- hey 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.

Answer:

A

Question 9

Question Type: MultipleChoice

What is the purpose of using prefilters when configuring event handlers?

Options:

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.

Answer:

A

Question 10

Question Type: MultipleChoice

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.)

Options:

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.

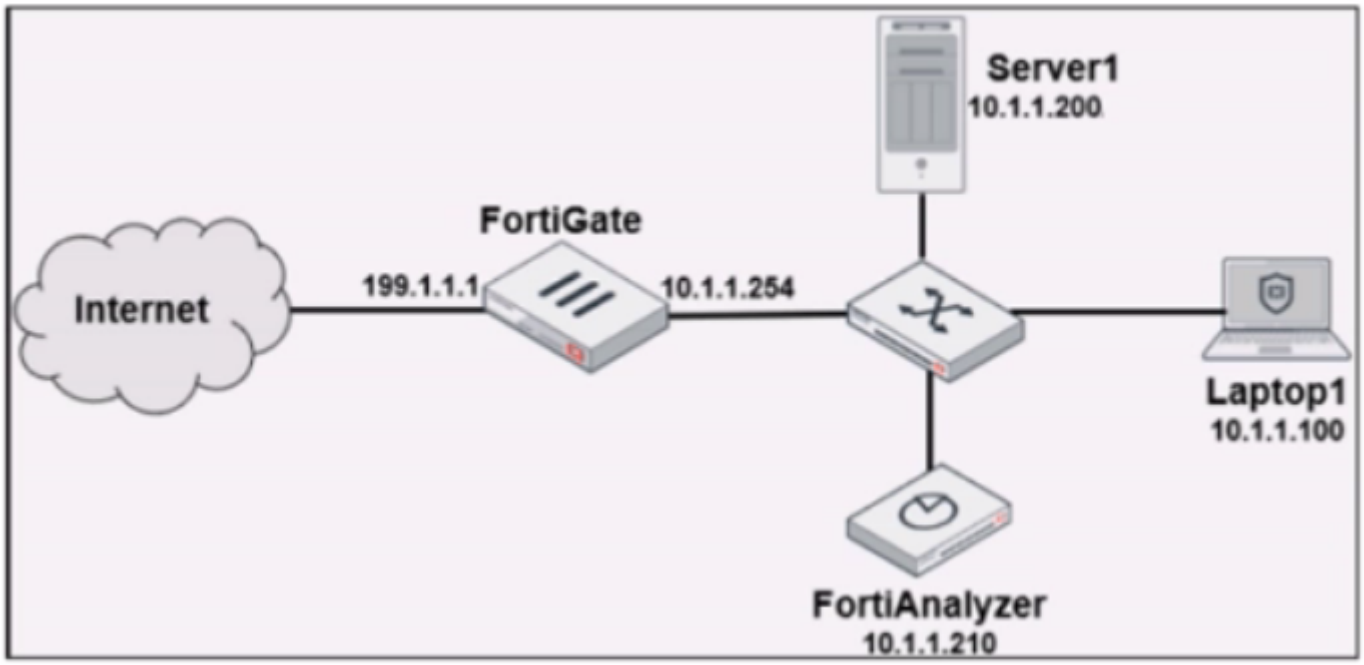
Answer:

B, C

Question 11

Question Type: **MultipleChoice**

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?

Options:

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