Question #1 *Topic 1*

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.

Suggested Answer: *AD*

Community vote distribution

AD (100%)

DaniSerb 9 months, 1 week ago

Selected Answer: AD

A: If the imported playbook has the same name as an existing playbook, to avoid conflicts, FortiAnalyzer will create a new name that includes a timestamp

D: Playbooks are imported with the same status they had (enabled or disabled) when they were exported.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 3 times

[Removed] 1 year, 2 months ago

Selected Answer: AD

A and D are correct.

FortiAnalyzer Analyst 7.2 Study Guide, p. 205, both answers.

upvoted 1 times

ebenav11 1 year, 3 months ago

Selected Answer: AD

A & D are Correct

upvoted 1 times

5fd6f75 1 year, 5 months ago

A and D

upvoted 1 times

x58 1 year, 8 months ago

Selected Answer: AD

A D Correct

upvoted 2 times

Question #2 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

alekgil 10 months ago

Selected Answer: B

B is correct

FortiAnalyzer Analyst 7.2 Study Guide, p. 203

upvoted 3 times

GopiChandMurari 10 months, 3 weeks ago

B is correct

playbook job that include 1 or more failed task is labeled as failed in playbook monitor.

upvoted 3 times

nesquick0 10 months, 2 weeks ago

brother, have you done your exam? is this valid ?

upvoted 1 times

[Removed] 1 year, 2 months ago

Selected Answer: B

B is correct

FortiAnalyzer Analyst 7.2 Study Guide, p. 203

upvoted 1 times

DaniSerb 1 year, 7 months ago

Selected Answer: B

Playbook jobs that include one or more failed tasks are labeled as Failed in Playbook Monitor. A failed status, however, does not mean that all tasks failed. Some individual actions may have completed successfully.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 3 times

x58 1 year, 8 months ago

Selected Answer: B

B correct

upvoted 1 times

Question #3 *Topic 1*

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.

Suggested Answer: *C*

Community vote distribution

C (100%)

⊟ **DaniSerb** 9 months, 1 week ago

Selected Answer: C

C seems to be correct according to - FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

FortiSIEM: SIEM collector functionality only. Must be registered on a licensed FortiSIEM Supervisor

upvoted 2 times

⊟ **77DVD** 1 year ago

Selected Answer: C

MEA - Administration Guide, FortiSIEM 6.7.5
To run the FortiSIEM Collector management extension application, the following requirements must be met:
FortiAnalyzer 7.0.1 or above
FortiSIEM Supervisor, Worker, Collectors 6.3.0 or above.
FortiSIEM Linux Agent 6.3.0 or above.
FortiSIEM Windows Agent 4.1.2 or above.

upvoted 2 times

⊟ **[Removed]** 1 year, 2 months ago

Selected Answer: C

C is correct
FortiAnalyzer Analyst 7.2 Study Guide, p. 96

upvoted 1 times

⊟ **Khalil85** 1 year, 7 months ago

C correct / Fortisiem must be registred on a licensed Fortisiem Supervisor

upvoted 1 times

⊟ **x58** 1 year, 8 months ago

Selected Answer: C

C correct

upvoted 1 times

Question #4 *Topic 1*

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.

Suggested Answer: *CD*

Community vote distribution

CD (100%)

Alexh07 8 months, 2 weeks ago

Selected Answer: CD

The answer is C and D

C - The FortiAnalyzer Outbreak Detection Service is a licensed feature (FortiAnalyzer_Analyst_7.2_Study_Guide-Online p130)

D- Automatically download related event handlers and reports (FortiAnalyzer_Analyst_7.2_Study_Guide-Online p130)

upvoted 2 times

LAFNELL 12 months ago

Selected Answer: CD

C & D are correct

Study Guide p130

upvoted 3 times

DaniSerb 1 year, 1 month ago

Selected Answer: CD

The FortiAnalyzer Outbreak Detection Service is a licensed feature that allows FortiAnalyzer administrators to receive and view outbreak alerts, and automatically download related event handlers and reports from FortiGuard.

Reference - FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 3 times

Question #5 *Topic 1*

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.

Suggested Answer: *AB*

Community vote distribution

BD (47%) AB (29%) BC (24%)

⊟ **LAFNELL** 10 months, 1 week ago

Selected Answer: AB

Study Guide page 77 & 78

A & B are correct

C is false as you can perform log fetching with standard user

D is false as it s not specify anywhere that archieved logs in the server will be archived logs in the client. Logs are retrieve to run queries and reports on forensic analysis.

upvoted 2 times

⊟ **d3vm3t** 10 months, 3 weeks ago

The answer es AB, FortiAnalyzer 7.2 Analyst Self-Paced says: "You can do the log fetching before adding the devices to Device Manager, but you won't be able to see the logs"

upvoted 3 times

⊟ **pmpmailbox** 1 year ago

Selected Answer: AB

You can fetch logs without the device in device manager. However, to view the logs you need to add it.

Answer is A, B.

upvoted 1 times

⊟ **Didesouzads** 1 year, 1 month ago

Selected Answer: BD

For me its a trick question, because the answer C "The fetching profile must include a user with the Super_User profile." give us a sensation that only Super User profile must be include, but in fact we can include Standard User as well, because of that I believe answer D is more accurable

upvoted 2 times

⊟ **fc58c80** 1 year, 2 months ago

Possible answer as to why D is not correct: When you fetch archived logs from the server, its done for the purpose of analyzing and/or running reports on them. I believe the client stores these archived logs separately from its own normal archived logs, and manages them independently.

upvoted 1 times

⊟ **alejandro1985** 1 year, 2 months ago

Selected Answer: BD

B and D are correct.

Ref: FortiAnalyzer_7.4_Analyst_Study_Guide-Online.pdf pag 84

upvoted 2 times

⊟ **Alexh07** 1 year, 2 months ago

Please, could you indicate the precise justification for option D in FortiAnalyzer_7.4_Analyst_Study_Guide-Online.pdf page 84?

upvoted 1 times

⊟ **Alexh07** 1 year, 2 months ago

Selected Answer: BC

A. (F) In FortiAnalyzer Analyst 7.2 Study Guide, p. 78 indicates that it must be the Device Manager but not necessarily a Local Device Manager.

B. (V) In FortiAnalyzer Analyst 7.2 Study Guide, p. 78 indicates that you can choose filters that include logs from specific devices (it can be a single device)

C. (V) In FortiAnalyzer Analyst 7.2 Study Guide, p. 77 indicates in the image of point number one that "must have Super_User or Standard_User profile"

D. (F) In FortiAnalyzer Analyst 7.2 Study Guide, p. 77 indicates the following statement "The FortiAnalyzer device that fetches logs operates as the fetch client, and the other Fortinalyzer device that send logs operates as the fetch server". They focus on the devices, they never mention such terms for archive logs.

upvoted 1 times

⊟ **fc58c80** 1 year, 1 month ago

for option D, page 77 states: "This allows FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer...". It does mention fetching archived logs, but not necessarily that they are archived when they get to the client. I assume
I can make a case for A and B as well:
A: page 78 on the slide says "You must add the devices to Device Manager before you can see the logs in the client. You can do the log fetching BEFORE adding the devices, but y ou won't be able to see the logs". For A to be wrong because it says local DM and not DM seems like they are trying to trick you, and I havent really noticed that on other questions.
C. Page 78 on the slide: During the request, you can choose filters to include:..."

upvoted 1 times

⊟ **fc58c80** 1 year, 1 month ago

I meant to put B and not C. We need an edit button

upvoted 1 times

⊟ **alejandro1985** 1 year, 2 months ago

Hi!,
Answer D states that the user has to be included in the Super_User profile, it does not present it as an option. In the study guide it is presented as an option since it can also be Standard_User.

Reference:
The fetch server administrator user name and password must be for an administrator with either a Standard_User or Super_User profile
https://docs.fortinet.com/document/fortianalyzer/7.4.2/administration-guide/785943/fetching-profiles

upvoted 1 times

⊟ **alejandro1985** 1 year, 2 months ago

Sorry, I was referring to answer C, it is not correct.

upvoted 1 times

⊟ **[Removed]** 1 year, 2 months ago

Selected Answer: AB

After revisiting this question, I suppose that it is broken.
A copule of days I've explained about answers B and D such as correct, but answer A is also true: The fetch client can retrieve logs from devices that are not added to its local Device Manager, I did it on lab.

If we Pass through the understanding about *maybe* answer D is incorrect, if we consider "...become archive logs in the client" that original logs will be moved from fetch server to client, and that's don't occurr.

upvoted 1 times

⊟ **fc58c80** 1 year, 2 months ago

In the lab, I assume you fetched the logs from another FortiAnalyzer? I think if A. stated that it can fetch from FA devices that are not on the Device Manger, then that would be correct. The question just says devices, but FA can't fetch from non-FA devices as far as I'm aware. I could be wrong though

upvoted 1 times

⊟ **alejandro1985** 1 year, 2 months ago

B and D

D: The fetch server administrator user name and password must be for an administrator with either a Standard_User or Super_User profile.

https://docs.fortinet.com/document/fortianalyzer/7.4.2/administration-guide/785943/fetching-profiles

upvoted 1 times

[Removed] 1 year, 2 months ago

Selected Answer: BD

B and D are correct

About answer B, check it on FortiAnalyzer Analyst 7.2 Study Guide, p. 77 and https://docs.fortinet.com/document/fortianalyzer/7.4.2/administration-guide/651442/log-fetching

About answer D, I've just tried the functionally on lab and on production, and I had just archived logs on FortiAnalyzer client. To see analytics logs, it's necessary wait the rebuild ADOM.

upvoted 3 times

bestboy120 1 year, 3 months ago

Selected Answer: BC

https://docs.fortinet.com/document/fortianalyzer/7.4.2/administration-guide/651442/log-fetching
The fetching FortiAnalyzer can query the server FortiAnalyzer and retrieve the log data for a specified device and time period, based on specified filters.

https://docs.fortinet.com/document/fortianalyzer/7.4.2/administration-guide/559986/fetch-requests
The data policy for the local ADOM on the client must also support fetching logs from the specified time period. It must keep both archive and analytics logs long enough so they will not be deleted in accordance with the policy. For example: Today is July 1, the ADOM's data policy is configured to keep analytics logs for 30 days (June 1 - 30), and you need to fetch logs from the first week of May. The data policy of the ADOM must be adjusted to keep analytics and archive logs for at least 62 days to cover the entire time span. Otherwise, the fetched logs will be automatically deleted after they are fetched.

upvoted 1 times

bestboy120 1 year, 3 months ago

sorry: The fetch server administrator user name and password must be for an administrator with either a Standard_User or Super_User profile.

upvoted 3 times

myrmidon3 1 year, 4 months ago

Selected Answer: BC

FAZ Analyst 7.2 Study Guide Page: 77-78

upvoted 1 times

myrmidon3 1 year, 4 months ago

B & C
FAZ Analyst 7.2 Study Guide Page: 77-78

upvoted 1 times

rac_sp 1 year, 6 months ago

Selected Answer: AB

A & B correct

upvoted 1 times

Thomas_2020 1 year, 6 months ago

Selected Answer: BC

B & C, Page 168 , FAZ_7.0

upvoted 1 times

Thomas_2020 1 year, 6 months ago

B & C, Page 168 , FAZ_7.0

upvoted 1 times

r_jordan 1 year, 6 months ago

Selected Answer: BD

- retrieve archive logs from another FAZ and run queries or reports on those archived logs
- you can do the log fetching but you won't be able to see the logs if you do not add the FAZ to the Device Manager (pages 77-78)

So I think B and D are more accurate answers.

upvoted 4 times

Question #6 *Topic 1*

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.

Suggested Answer: *A*

Community vote distribution

A (86%) 14%

⊟ **Halmonte0780** 7 months, 1 week ago

Selected Answer: A

A are correct

A dataset is an SQL SELECT query. The result from that query—the specific data polled from the database— is what populates a chart.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2 pages 7

upvoted 1 times

⊟ **alejandro1985** 8 months, 1 week ago

Selected Answer: A

A are correct.

upvoted 1 times

⊟ **DaniSerb** 1 year, 1 month ago

Selected Answer: A

A dataset is an SQL SELECT query. The result from that query—the specific data polled from the database— is what populates a chart.

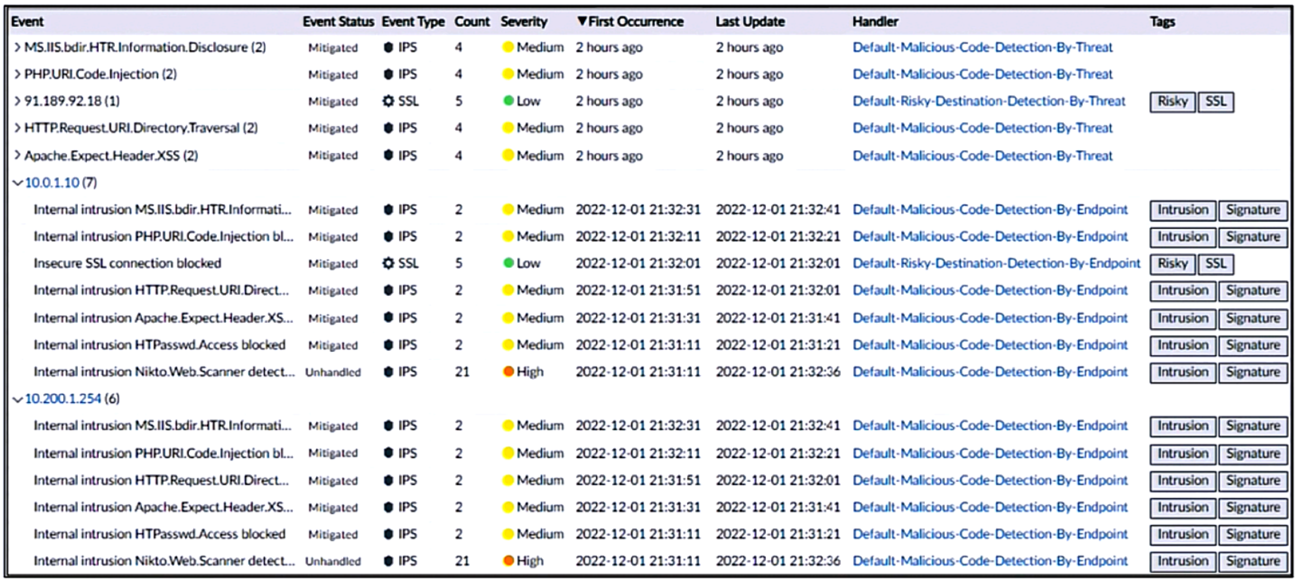
Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 4 times

Question #7 Topic 1

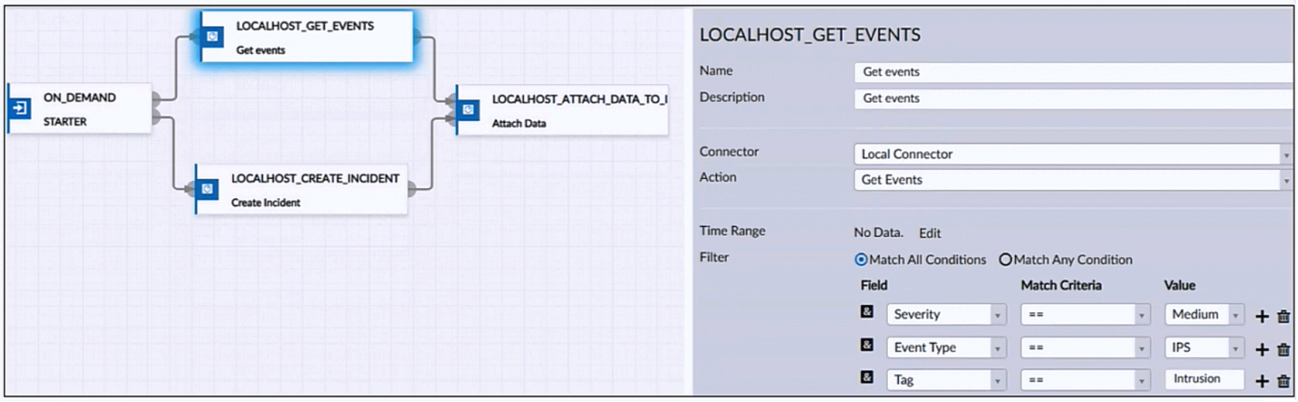
Refer to the exhibits.

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



LOCALHOST_GET_EVENTS

Name	Get events
Description	Get events
Connector	Local Connector
Action	Get Events
Time Range	No Data. Edit
Filter	● Match All Conditions ○ Match Any Condition

Field	Match Criteria	Value
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.

Suggested Answer: *D*

Community vote distribution

D (100%)

Didesouzads 7 months, 1 week ago

Selected Answer: D

The events you need to count are according from the match criteria "Medium, IPS and Intrusion"

upvoted 1 times

Halmonte0780 7 months, 1 week ago

Selected Answer: D

Match all conditions:

Intrusion + IPS + Medium: 10

upvoted 1 times

[Removed] 8 months, 4 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

⊟ **myrmidon3** 10 months, 1 week ago

Selected Answer: D

D is correct.

upvoted 1 times

⊟ **r_jordan** 1 year ago

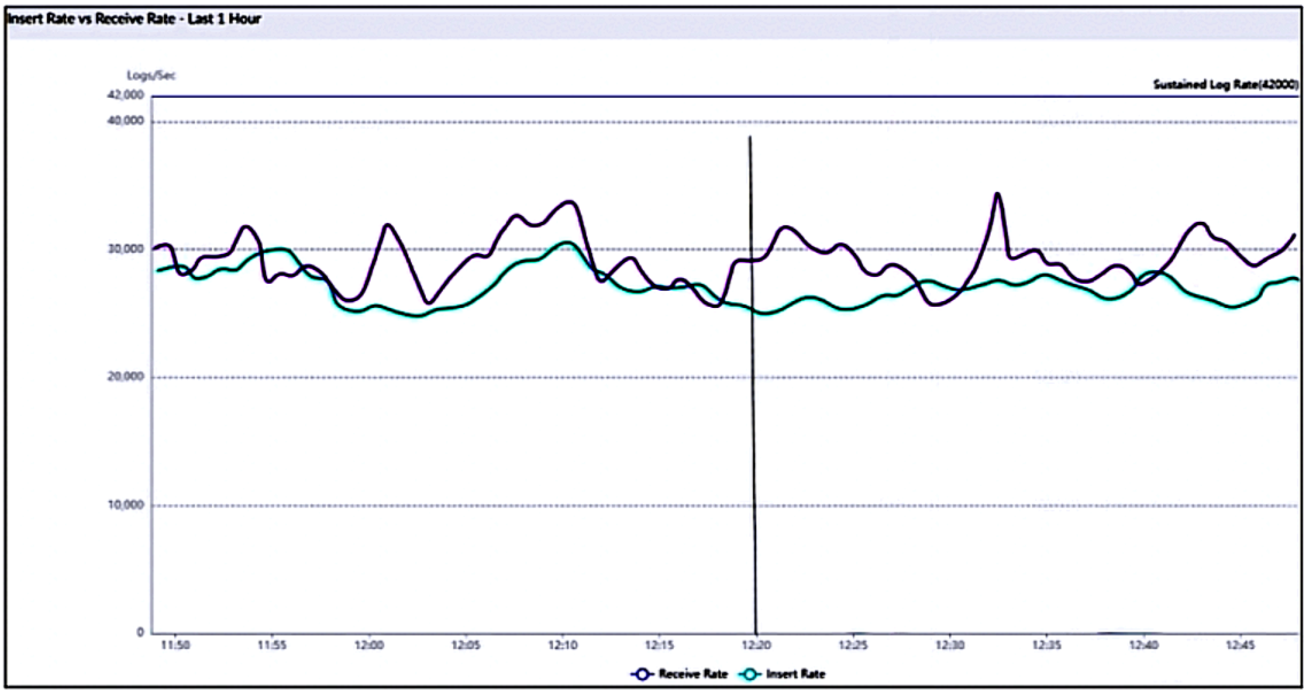
Selected Answer: D

D is correct

upvoted 2 times

Question #8 *Topic 1*

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.

Suggested Answer: *C*

Community vote distribution

C (100%)

DBFront 8 months, 1 week ago

Selected Answer: C

C is the right answer. 7.2 Study Guide

upvoted 1 times

DaniSerb 9 months, 1 week ago

Selected Answer: C

Insert Rate vs. Receive Rate is a graph that shows the rate at which raw logs reach the FortiAnalyzer (receive rate) and the rate at which they are indexed (insert rate) by the SQL database and the sqlplugind daemon. At minimum, the difference between these parameters should be generally consistent.

Log Insert Lag Time shows the amount of time between when a log was received and when it was indexed. Ideally, this parameter should be as small as possible with the occasional spikes according to the network activity being logged. A good baseline should be created to allow for the identification of possible performance issues.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 4 times

[Removed] 1 year, 2 months ago

Selected Answer: C

C is correct

upvoted 1 times

ebenav11 1 year, 3 months ago

Selected Answer: C

Option C

upvoted 1 times

Question #9 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (83%) C (17%)

⊟ **Adoking** 11 months, 2 weeks ago

Selected Answer: B

B is correct answer.
FortiAnalyzer Analyst 7.2 Study Guide 189

upvoted 1 times

⊟ **[Removed]** 1 year, 2 months ago

Selected Answer: B

B is correct answer.
FortiAnalyzer Analyst 7.2 Study Guide 184
I've just validate on GUI of FortiAnalyzer and a FortiGate

upvoted 1 times

⊟ **sandfred** 1 year, 6 months ago

Selected Answer: B

B. Incoming Webhook

FortiAnalyzer Analyst 7.2 Study Guide 184

1. Traffic flows through the FortiGate
2. FortiGate sends logs to FortiAnalyzer
3. FortiAnalyzer detects some suspicious traffic and generates an event
4. The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate so that it runs an automation stitch
5. FortiGate runs the automation stitch with the corrective or preventive actions

upvoted 4 times

⊟ **andreadg88** 1 year, 6 months ago

Selected Answer: B

you must enable an automation rule using the Incoming Webhook Call trigger on the FortiGate side

upvoted 2 times

⊟ **DaniSerb** 1 year, 7 months ago

Selected Answer: B

FortiOS connector will be listed as soon as the first FortiGate is added to FortiAnalyzer.
However, in order to see the actions related to that FortiOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on the FortiGate side.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 2 times

⊟ **DaniSerb** 1 year, 7 months ago

Selected Answer: C

FortiOS connector will be listed as soon as the first FortiGate is added to FortiAnalyzer.
However, in order to see the actions related to that FortiOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on the FortiGate side.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2
upvoted 2 times

Question #10 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

DaniSerb Highly Voted 👍 1 year, 1 month ago

Selected Answer: C

Threat hunting consists of proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach will help the analyst find any threats that might have eluded detection by the current security solutions or configurations.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 6 times

M_70 Most Recent 🕒 8 months ago

Selected Answer: C

The feature in FortiAnalyzer that allows you to use a proactive approach when managing your network security is C. Threat hunting.

Threat hunting in FortiAnalyzer enables you to proactively search through network data to detect and isolate advanced threats before they cause harm or breach data. This capability is crucial for a proactive cybersecurity strategy, allowing security teams to identify and respond to potential threats before they become actual incidents.

upvoted 1 times

[Removed] 8 months, 3 weeks ago

Selected Answer: C

C is correct.

FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2, p. 125

upvoted 1 times

Question #11 *Topic 1*

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.

Suggested Answer: *C*

Community vote distribution

C (100%)

Halmonte0780 7 months ago

Selected Answer: C

FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2, page 111

upvoted 1 times

DaniSerb 1 year, 1 month ago

Selected Answer: C

Contained: The risk source is isolated.
For example, an AV log with action=quarantine will have the event status Contained.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 4 times

Question #12 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

DaniSerb Highly Voted 1 year, 1 month ago

Selected Answer: B

Trigger variables allow you to use information from the trigger of a playbook when it has been configured with an incident or event trigger. For example, a single playbook can be triggered by more than one device. A Run Report action can include a filter for the endpoint IP address from the event that triggered the playbook.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 6 times

[Removed] Most Recent 8 months, 3 weeks ago

Selected Answer: B

B is correct.

FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2, p. 198

upvoted 1 times

myrmidon3 11 months, 2 weeks ago

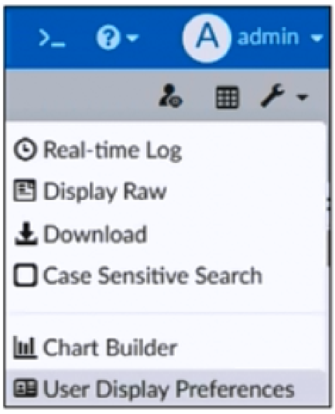
Selected Answer: B

FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2 page 198

upvoted 2 times

Question #13 Topic 1

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

Suggested Answer: *B*

Community vote distribution

B (100%)

Halmonte0780 7 months, 1 week ago

Selected Answer: B

FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2 page 160

upvoted 1 times

Thomas_2020 1 year ago

Selected Answer: B

B is true

upvoted 1 times

r_jordan 1 year ago

Selected Answer: B

it is B

upvoted 1 times

DaniSerb 1 year, 1 month ago

Selected Answer: B

A quick way to build a custom dataset and chart is to use the chart builder tool. This tool is located in LogView, and allows you to build a dataset and chart automatically, based on your filtered search results. In LogView, set filters to return the logs you want.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 3 times

Question #14 *Topic 1*

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.

Suggested Answer: *CD*

Community vote distribution

CD (94%) 6%

⊟ **DaniSerb** Highly Voted 1 year, 1 month ago

Selected Answer: CD

To boost the report performance and reduce report generation time, you can enable auto-cache in the settings of the report. In this case, the hcache is automatically updated when new logs come in and new log tables are generated.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 7 times

⊟ **[Removed]** Most Recent 8 months, 3 weeks ago

Selected Answer: CD

C and D are correct.

FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2, p. 166

upvoted 1 times

⊟ **myrmidon3** 11 months, 2 weeks ago

Selected Answer: CD

To boost the report performance and reduce report generation time, you can enable auto-cache in the settings of the report. In this case, the hcache is automatically updated when new logs come in and new log tables are generated.
FAZ Analyst 7.2 Study Guide page 166

upvoted 3 times

⊟ **rac_sp** 1 year ago

Selected Answer: CD

Data is stored in the cache

upvoted 2 times

⊟ **Thomas_2020** 1 year ago

Selected Answer: CD

CyD is Correct

upvoted 3 times

⊟ **r_jordan** 1 year ago

Reports are not stored in the cache. Data stored in cache. C and D

upvoted 3 times

⊟ **shinichi18** 1 year, 1 month ago

Selected Answer: BD

B y D....

upvoted 1 times

Question #15 *Topic 1*

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.

Suggested Answer: *D*

Community vote distribution

D (100%)

Halmonte0780 7 months, 1 week ago

Selected Answer: D

FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2 page 121

upvoted 1 times

Alexh07 8 months, 2 weeks ago

Selected Answer: D

A. (F) In FortiAnalyzer Analyst 7.2 Study Guide, p. 121 indicates that there are three reporting methods that are "created", "updated" and "deleted"

B. (F) In FortiAnalyzer Analyst 7.2 Study Guide, p. 165 indicates that the output profiles are used to send generated reports, but not for notifications.

C. (F) In FortiAnalyzer Analyst 7.2 Study Guide, p. 121 indicates that the FortiAnalyzer can send a notification to external platforms, in plural and not to a single platform.

D. (V) In FortiAnalyzer Analyst 7.2 Study Guide, p. 121 indicates that you can add more than one fabric connector, each with the same or different notification settings.

upvoted 3 times

[Removed] 8 months, 3 weeks ago

Selected Answer: D

D is correct.

FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2, p. 110

upvoted 1 times

r_jordan 1 year ago

Selected Answer: D

D is correct

upvoted 1 times

DaniSerb 1 year, 1 month ago

Selected Answer: D

Incidents will usually go through several stages during the analysis process. In most cases, it is important to make sure all parties involved are notified when the incident status is updated.

You can add more than one fabric connector, each with the same or different notification settings. The receiving side of the connector must be configured for the notifications to be sent successfully.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 3 times

Question #16 Topic 1

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.

Suggested Answer: *A*

Community vote distribution

A (100%)

DaniSerb Highly Voted 1 year, 1 month ago

Selected Answer: A

Also keep in mind that after a new playbook is created, FortiAnalyzer will need a few minutes to parse it. For example, if you try to run a newly created playbook configured with an ON_DEMAND trigger before that time, you will get an error, like the one shown on the slide, telling you why the playbook failed to run.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 6 times

Halmonte0780 Most Recent 7 months, 1 week ago

Selected Answer: A

FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2 page 197

upvoted 1 times

[Removed] 8 months, 3 weeks ago

Selected Answer: A

A is correct.

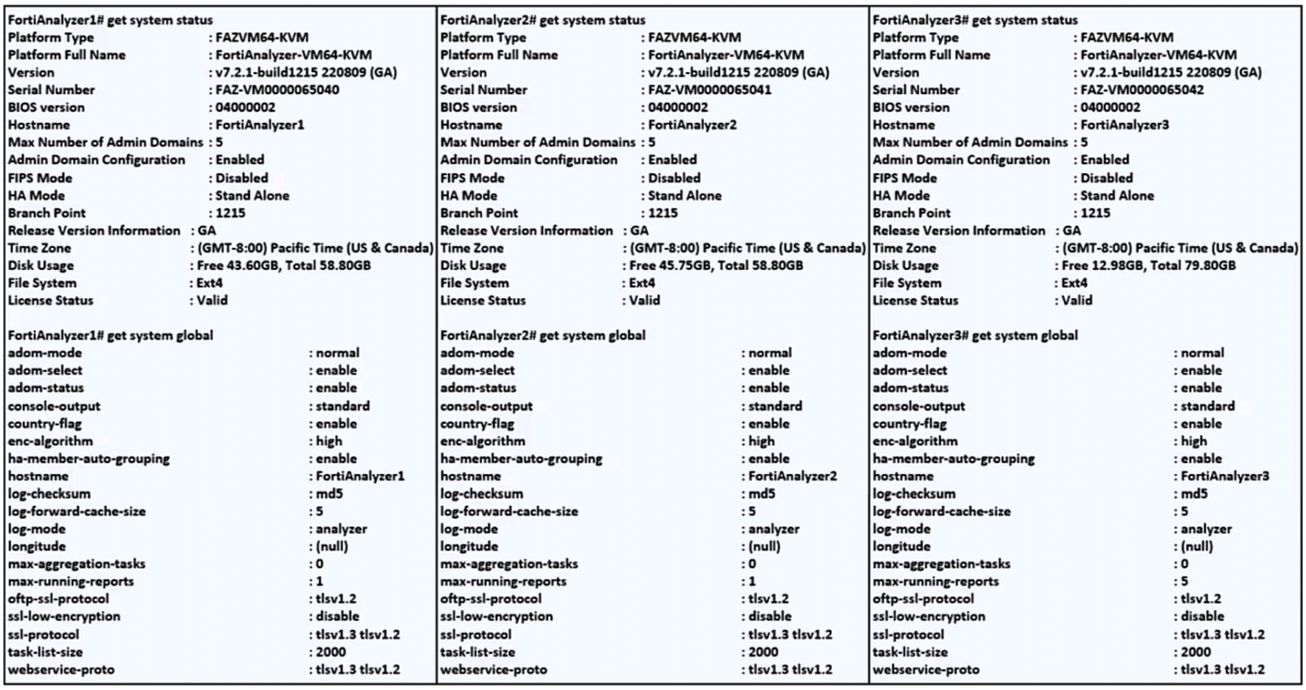
FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 1 times

Question #17

Topic 1

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                                : 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
```

```
FortiAnalyzer2# get system status
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

FortiAnalyzer2# 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
task-list-size                          : 2000
webservice-proto                        : tlsv1.3 tlsv1.2
```

```
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
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

Suggested Answer: *B*

Community vote distribution

C (95%) 5%

DaniSerb Highly Voted 1 year, 7 months ago

Selected Answer: C

Members are devices in the FortiAnalyzer Fabric that send information to the supervisor for centralized viewing. When configured as a member, FortiAnalyzer devices continue to have access to the FortiAnalyzer features identified in the FortiAnalyzer Administration Guide. Incidents and events are created or raised from each member.

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 7 times

emershow Highly Voted 1 year, 5 months ago

The display of this question is incorrect, exam topics please check.

upvoted 5 times

LAFNELL Most Recent 10 months, 1 week ago

Selected Answer: C

Answer C

Study guide Page 47: in FAZ Fabric, members must be in Analyzer mode

upvoted 1 times

Alexh07 1 year, 2 months ago

Selected Answer: C

C is Correct

In FortiAnalyzer Analyst 7.2 Study Guide, p. 47 indicates all FortiAnalyzer Fabric members must be configured with the same time zone settings as the supervisor.

upvoted 3 times

[Removed] 1 year, 2 months ago

Selected Answer: C

C is correct.

upvoted 1 times

m_beluy 1 year, 3 months ago

Selected Answer: C

See log-mode: Analyzer.

FortiAnalyzer in Collector mode cannot be a FortiAnalyzer Fabric.

upvoted 1 times

hugoescorcia82 1 year, 5 months ago

Selected Answer: C

In the guide only talks about the same time

upvoted 1 times

mordechayd 1 year, 6 months ago

Selected Answer: C

C. all Forti analyzers with the same timezone and in the analyzer operation mode (not collector) can be part of fortianalyzer fabric

upvoted 5 times

shinichi18 1 year, 7 months ago

Selected Answer: B

estaria correcta la B si es debido a la linea max-running-reports

upvoted 1 times

Question #18 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

B (60%) C (40%)

Aminshon Highly Voted 1 year, 1 month ago

Selected Answer: B

https://community.fortinet.com/t5/FortiAnalyzer/Technical-Tip-Configuring-FortiGate-and-FortiAnalyzer-to-resolve/ta-p/223347

Note that SOC/FortiView has its own settings which control if the destination IP addresses should be resolved or not, as this would use the FortiAnalyzer side system DNS servers to resolve both source and destination. Enable hostname resolution in the CLI:

```
config system fortiview setting
set resolve-ip enable
end
```

upvoted 5 times

rafaeldiino Most Recent 10 months ago

B, resolve Source and Destination.

upvoted 1 times

elcho0o 1 year, 1 month ago

Selected Answer: C

https://community.fortinet.com/t5/Support-Forum/Hostnames-in-FortiAnalyzer/td-p/95351

upvoted 1 times

Didesouzads 1 year, 1 month ago

Selected Answer: C

I agree with the previous answers

upvoted 1 times

zeebo340 1 year, 1 month ago

Selected Answer: C

Answer is C

upvoted 1 times

ebenav11 1 year, 3 months ago

Only destination will be resolved, option C

upvoted 2 times

r_jordan 1 year, 6 months ago

Selected Answer: C

only Destination will be resolved

upvoted 2 times

Thomas_2020 1 year, 6 months ago

Selected Answer: C

C, pag 167 Faz 7.0

upvoted 1 times

⊟ **DaniSerb** 1 year, 7 months ago

Selected Answer: B

https://community.fortinet.com/t5/FortiAnalyzer/Technical-Tip-How-to-configure-FortiGate-and-FortiAnalyzer-to/ta-p/223347

upvoted 4 times

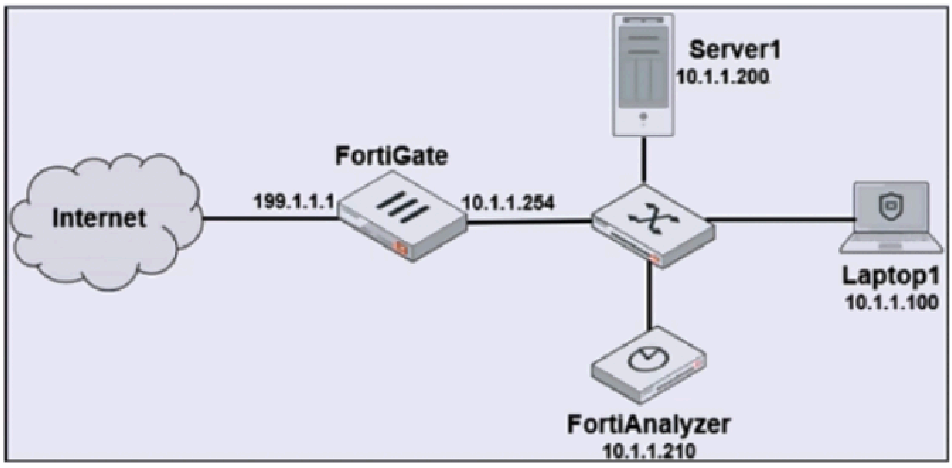
⊟ **rac_sp** 1 year, 6 months ago

Note that SOC/FortiView has its own settings which control if the destination IP addresses should be resolved or not, as this would use the FortiAnalyzer side system DNS servers to resolve both source and destination.

upvoted 2 times

Question #19 Topic 1

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

Suggested Answer: *D*

Community vote distribution

D (100%)

sandfred 1 year ago

Selected Answer: D

Similar example from FortiAnalyzer 7.0 Lab Guide, page 85:

Edit the generic text filter with user==admin to match any login attempts with that user.

4. Add the text operation=="login failed" to match only failed login attempts.

If you don't include this condition, you will get more matches than what is required.

5. 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.

You need this syntax because the requirements do not specify the method the
attacker uses to try to access FortiAnalyzer.

If you were looking only for attempts using a browser, you could use performed_
on!="GUI(10.0.1.10)" instead.

If you were looking only for attempts using SSH, you could use performed_
on!="ssh(10.0.1.10)" instead.

6. Combine the three conditions with a logical and.

operation=="login failed" & user==admin & performed_on!~10.0.1.10

upvoted 4 times

Question #20 *Topic 1*

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.

Suggested Answer: *AB*

Community vote distribution

AB (100%)

[Removed] 8 months, 3 weeks ago

Selected Answer: AB

A and B are correct.

FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2, p. 73

upvoted 1 times

[Removed] 8 months, 3 weeks ago

A and B are correct.

FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2, p. 73

upvoted 1 times

r_jordan 1 year ago

Selected Answer: AB

A and B

upvoted 1 times

DaniSerb 1 year, 1 month ago

Selected Answer: AB

A: FortiAnalyzer downloads threat intelligence FortiGuard package (TDS) every day

B: FortiAnalyzer runs real-time threat detection when it receives logs from the FortiGate web filter

Reference: FortiAnalyzer Analyst Study Guide for FortiAnalyzer 7.2

upvoted 4 times