Question #1 *Topic 1*

What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

A. Hot swap the disk.

B. There is no need to do anything because the disk will self-recover.

C. Shut down FortiAnalyzer and replace the disk.

D. Run execute format disk to format and restart the FortiAnalyzer device.

Suggested Answer: *C*

Community vote distribution

A (100%)

PiotrSwi 9 months, 3 weeks ago

Selected Answer: A

A - Correct.

upvoted 1 times

MaxTalin 10 months, 2 weeks ago

Hardware raid is hot swapping disk

upvoted 1 times

SH_ 1 year, 3 months ago

Selected Answer: A

Hardware-based RAID supports hot swapping

upvoted 2 times

ckl55995 1 year, 9 months ago

Selected Answer: A

A is correct answer

upvoted 2 times

sauls 1 year, 10 months ago

A. corect

upvoted 3 times

ama6 1 year, 10 months ago

new one Which FortiGate process caches logs when FortiAnalyzer is not reachable?

A. logfiled

B. miglogd

C. oftpd

D. sqlplugind

Answer: B

upvoted 3 times

nerostart 1 year, 10 months ago

Selected Answer: A

A is correct

upvoted 1 times

nerostart 1 year, 10 months ago

A is correct

upvoted 1 times

ahougham 1 year, 11 months ago

A is ok

upvoted 1 times

lucient 1 year, 11 months ago

Selected Answer: A

A) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 83: If a hard disk on a FortiAnalyzer fails, you must replace it. On FortiAnalyzer models that support hardware RAID, you can replace the disk while FortiAnalyzer is still running. This is known as hot swapping. Fortinet supports hot swapping on hardware RAID only.

upvoted 3 times

ZakySama 1 year, 11 months ago

Selected Answer: A

A is correct

upvoted 2 times

dvalsa 2 years ago

Selected Answer: A

A is correct.

upvoted 3 times

Khs01 2 years ago

Selected Answer: A

Hardware RAID not software, correct is A

upvoted 2 times

Khs01 2 years ago

Hardware RAID not software, correct is A

upvoted 2 times

morzart2025 2 years ago

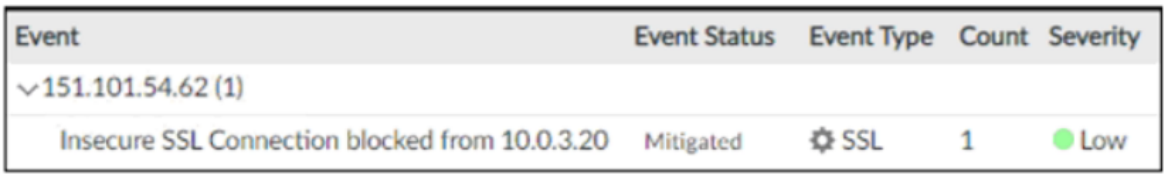
If a hard disk on a FortiAnalyzer fails, you must replace it. On FortiAnalyzer models that support hardware RAID, you can replace the disk while FortiAnalyzer is still running. This is known as hot swapping. Fortinet support hot seapping on hardware RAID only. On FortiAnalyzer devices with software RAID you must shut down FortiAnalyzer prior to exchanging the hard disk.

FortiAnalyzer_7.0_Study_Guide-Online pag. 83

upvoted 4 times

Question #2 *Topic 1*

Refer to the exhibit.



Event	Event Status	Event Type	Count	Severity
151.101.54.62 (1)				
Insecure SSL Connection blocked from 10.0.3.20	Mitigated	SSL	1	Low

Which statement is correct regarding the event displayed?

A. An incident was created from this event.

B. The security risk was blocked or dropped.

C. The security event risk is considered open.

D. The risk source is isolated.

Suggested Answer: *C*

Community vote distribution

B (100%)

PiotrSwi 9 months, 3 weeks ago

Selected Answer: B

B - Correct.

upvoted 1 times

MaxTalin 10 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

omega_raid 1 year, 1 month ago

B is correct. Took exam on 23rd Oct and this question did arise on the exam.

upvoted 2 times

chyeahhh 1 year, 5 months ago

I had a similar question to this today (6/15), but instead of "mitigated" the event said "unhandled".

upvoted 2 times

Reque1 1 year, 3 months ago

me too, Did you pass the exam?

upvoted 2 times

myrmidon3 10 months, 2 weeks ago

Unhandled: If the event is risk is not mitigated or contained, so it is considered open. In this case, the action = pass will have the event status Unhandled.

FAZ Analyst 7.2 Study Guide page 111

upvoted 1 times

ckl55995 1 year, 9 months ago

Selected Answer: B

B is correct

upvoted 1 times

nerostart 1 year, 10 months ago

Selected Answer: B

B is correct

upvoted 2 times

nerostart 1 year, 10 months ago

B is correct

upvoted 1 times

lucient 1 year, 11 months ago

Selected Answer: B

B) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 206: Mitigated: The security risk is mitigated by being blocked or dropped. For example, an IPS/AV log with action=block/drop will have the event status Mitigated.

upvoted 1 times

ZakySama 1 year, 11 months ago

Selected Answer: B

B is correct

upvoted 1 times

dvalsa 2 years ago

Selected Answer: B

Answer B.

upvoted 1 times

Khs01 2 years ago

Selected Answer: B

B is correct

upvoted 1 times

morzart2025 2 years ago

Answer is B.

Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not.

The possible statuses are:

Unhandled: The security event risk is not mitigated or contained, so it is considered open.
Contained: The risk source is isolated.
Mitigated: The security risk is mitigated by being blocked or dropped.
(Blank): Other scenarios.

FortiAnalyzer_7.0_Study_Guide-Online pag. 206

upvoted 4 times

Question #3 *Topic 1*

Which statement correctly describes the management extensions available on FortiAnalyzer?

A. Management extensions do not require additional licenses.

B. Management extensions may require a minimum number of CPU cores to run.

C. Management extensions allow FortiAnalyzer to act as a FortiSIEM supervisor.

D. Management extensions require a dedicated VM for best performance.

Suggested Answer: *C*

Community vote distribution

B (90%) 10%

PiotrSwi 9 months, 3 weeks ago

Selected Answer: B

B - Correct.

upvoted 1 times

Thomas_2020 11 months, 1 week ago

Selected Answer: C

C in correct

upvoted 1 times

omega_raid 1 year, 1 month ago

Answer is B, this appeared on my exam 23rd Oct 2023

upvoted 3 times

LiliRose 1 year, 3 months ago

Selected Answer: B

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 189

upvoted 2 times

jaibarrar 1 year, 8 months ago

B is Correct, page 188 / FortiSIEM MEA: SIEM Collector ONLY.

upvoted 1 times

ckl55995 1 year, 9 months ago

Selected Answer: B

B is correct

upvoted 2 times

Shuri7777 1 year, 9 months ago

B is correct

upvoted 2 times

Christiandus 1 year, 9 months ago

Selected Answer: B

B) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 189: Review the hardware requirements before you enable a management extension application. Some of them require a minimum amount of memory or a minimum number of CPU cores.

upvoted 1 times

nerostart 1 year, 10 months ago

Selected Answer: B

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 189

upvoted 1 times

lucient 1 year, 11 months ago

Selected Answer: B

B) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 189: Review the hardware requirements before you enable a management extension application. Some of them require a minimum amount of memory or a minimum number of CPU cores.

upvoted 1 times

Khs01 2 years ago

Selected Answer: B

The correct answer is B

upvoted 1 times

morzart2025 2 years ago

Answer is B.

FortiAnalyzer_7.0_Study_Guide-Online pag. 189

upvoted 1 times

morzart2025 2 years ago

Answer is B.

Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not.

The possible statuses are:

Unhandled: The security event risk is not mitigated or contained, so it is considered open.
Contained: The risk source is isolated.
Mitigated: The security risk is mitigated by being blocked or dropped.
(Blank): Other scenarios.

FortiAnalyzer_7.0_Study_Guide-Online pag. 189.

upvoted 1 times

Question #4 *Topic 1*

In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results.
Similarly, which feature can you use for FortiView?

A. Export to Custom Chart

B. Export to PDF

C. Export to Chart Builder

D. Export to Report Chart

Suggested Answer: *C*

Community vote distribution

D (100%)

morzart2025 Highly Voted 2 years ago

Answer is D.

Similar to the Chart Builder feature in Log View, you can export a chart from a FortiView. The chart export includes any filters you set on the FortiView.

FortiAnalyzer_7.0_Study_Guide-Online pag. 292.

upvoted 5 times

omega_raid Most Recent 1 year, 1 month ago

I can confirm, this appeared on my exam 23rd Oct 2023

upvoted 3 times

ckl55995 1 year, 9 months ago

D is correct

upvoted 1 times

Shuri7777 1 year, 9 months ago

C is correct

upvoted 1 times

Christiandus 1 year, 9 months ago

Selected Answer: D

Answer is D.

Similar to the Chart Builder feature in Log View, you can export a chart from a FortiView. The chart export includes any filters you set on the FortiView.

FortiAnalyzer_7.0_Study_Guide-Online pag. 292.

upvoted 3 times

nerostart 1 year, 10 months ago

Selected Answer: D

Export to Report Chart

upvoted 1 times

lucient 1 year, 11 months ago

Selected Answer: D

D) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 292: Screenshot show the "Export to Report Chart" dialog.

upvoted 2 times

Khs01 2 years ago

Selected Answer: D

Answer is D

upvoted 2 times

Question #5 *Topic 1*

Which daemon is responsible for enforcing the log file size?

A. logfiled

B. oftpd

C. sqlplugind

D. miglogd

Suggested Answer: *D*

Community vote distribution

A (89%) 11%

morzart2025 Highly Voted 2 years ago

Answer is A.

Disk quota enforcement is performed by different processes:

The logfiled process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes.

FortiAnalyzer_7.0_Study_Guide-Online pag. 121

upvoted 5 times

PiotrSwi Most Recent 9 months, 3 weeks ago

Selected Answer: D

D - Correct.

upvoted 1 times

geroboamo 9 months ago

miglogd is the fortigate process shipping logs to faz

upvoted 1 times

MaxTalin 10 months, 2 weeks ago

Correct A

The logfiled process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes

• The sqlplugind process enforces the SQL database size

• The oftpd process enforces the archive file size

upvoted 1 times

ckl55995 1 year, 9 months ago

Selected Answer: A

Answer is A

upvoted 1 times

Christiandus 1 year, 9 months ago

Selected Answer: A

A) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 121: The logfiled process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes.

upvoted 2 times

nerostart 1 year, 10 months ago

Selected Answer: A

Answer is A

upvoted 1 times

lucient 1 year, 11 months ago

Selected Answer: A

A) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 121: The logfiled process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes.

upvoted 2 times

steed47 2 years ago

Selected Answer: A

Answer is A.

upvoted 2 times

wayne0926 2 years ago

Answer is A

FortiAnalyzer_7.0_Study_Guide-Online pag. 121

upvoted 2 times

Question #6 *Topic 1*

For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

A. Principal

B. Identity provider

C. Identity collector

D. Service provider

Suggested Answer: *BD*

Community vote distribution

morzart2025 Highly Voted 2 years ago

B and D.

In FortiAnalyzer, SAML can be enabled across all Security Fabric devices, enabling smooth movement between devices for the administrator by means of single sign-on (SSO).

FortiAnalyzer can play the role of the identity provider (IdP), the service provider (SP), or Fabric SP, when an external identity provider is available.

FortiAnalyzer_7.0_Study_Guide-Online pag. 48

upvoted 6 times

PiotrSwi Most Recent 9 months, 3 weeks ago

Selected Answer: BD

B,D - Correct.

upvoted 1 times

MaxTalin 10 months, 1 week ago

Selected Answer: BD

Correct B and D

FortiAnalyzer can play the role of the identity provider (IdP), the service provider (SP), or Fabric SP, when an external identity provider is available.

upvoted 1 times

Michael348 1 year, 6 months ago

Selected Answer: AC

System configuration backup includes:

System Information -

Device list -

Report Information -

upvoted 1 times

nerostart 1 year, 10 months ago

Selected Answer: BD

B and D

upvoted 2 times

lucient 1 year, 11 months ago

Selected Answer: BD

B and D) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 48: FortiAnalyzer can play the role of the identity provider (IdP), the service provider (SP), or Fabric SP, when an external identity provider is available.

upvoted 3 times

Khs01 2 years ago

Selected Answer: BD

BD is Ok!

upvoted 3 times

Question #7 *Topic 1*

Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

A. Report information

B. Database snapshot

C. System information

D. Logs from registered devices

Suggested Answer: *BD*

Community vote distribution

AC (100%)

lucient Highly Voted 1 year, 11 months ago

Selected Answer: AC

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 29: What does the System Configuration backup include?

• System information, such as the device IP address and administrative user information

• Device list, such as any devices you configured to allow log access

• Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

upvoted 5 times

PiotrSwi Most Recent 9 months, 3 weeks ago

Selected Answer: AC

A,C - Correct.

upvoted 1 times

MaxTalin 10 months, 2 weeks ago

AC is correct

System information, such as the device IP address and administrative user information

• Device list, such as any devices you configured to allow log access

• Report information, such as any configured report settings, as well as all your custom

upvoted 1 times

Michael348 1 year, 5 months ago

Selected Answer: AC

System information, such as the device IP address and administrative user information

• Device list, such as any devices you configured to allow log access

• Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports

upvoted 1 times

Khs01 2 years ago

Selected Answer: AC

Correct answer is AC

upvoted 2 times

morzart2025 2 years ago

A and C

What does the System Configuration backup include?

System information, such as the device IP address and administrative user information.

Device list, such as any devices you configured to allow log access.

Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

FortiAnalyzer_7.0_Study_Guide-Online pag. 29

upvoted 3 times

Question #8 *Topic 1*

What is required to authorize a FortiGate on FortiAnalyzer using Fabric authorization?

A. A pre-shared key

B. The FortiGate serial number

C. A FortiGate ADOM

D. Valid FortiAnalyzer credentials

Suggested Answer: *D*

Community vote distribution

D (100%)

PiotrSwi 9 months, 3 weeks ago

Selected Answer: D

D - Correct. FortiAnalyzer Administrator 7.2 Study Guide page 145.

upvoted 1 times

MaxTalin 10 months, 2 weeks ago

correct D

This method requires that both FortiGate and FortiAnalyzer are running version 7.0.1 or higher. It is also required that the FortiGate administrator has valid credentials to log in on FortiAnalyzer and complete the registration.

upvoted 1 times

lucient 1 year, 11 months ago

Selected Answer: D

D) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 93: The fourth method uses the Fortinet Security Fabric authorization process.

This method requires that both FortiGate and FortiAnalyzer are running version 7.0.1 or higher. It is also required that the FortiGate administrator has valid credentials to log in on FortiAnalyzer and complete the registration.

upvoted 2 times

G33 1 year, 11 months ago

D is Correct

https://docs.fortinet.com/document/fortianalyzer/7.2.1/administration-guide/13897/adding-a-fortigate-using-security-fabric-authorization

upvoted 1 times

Franky1286 1 year, 11 months ago

B is OK!!

Administration Guide | FortiAnalyzer 7.2.1 | Fortinet Documentation Library

upvoted 1 times

Khs01 2 years ago

Selected Answer: D

D is Ok!

upvoted 4 times

morzart2025 2 years ago

Answer is D

This method requires that both FortiGate and FortiAnalyzer are running version 7.0.1 or higher. It is also required that the FortiGate administrator has valid credentials to log in on FortiAnalyzer and complete the registration.

FortiAnalyzer_7.0_Study_Guide-Online pag. 93

upvoted 2 times

Question #9 *Topic 1*

Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

A. FortiAnalyzer HA can function without VRRP, and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.

B. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.

C. All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.

D. FortiAnalyzer HA implementation is supported by all cloud providers.

Suggested Answer: *BC*

Community vote distribution

BC (100%)

PiotrSwi 9 months, 3 weeks ago

Selected Answer: BC

B,C - Correct.

upvoted 1 times

Marchrist 1 year, 4 months ago

Selected Answer: BC

B and C

upvoted 2 times

chyeahhh 1 year, 5 months ago

can confirm this was on exam today (6/15)

upvoted 2 times

lucient 1 year, 11 months ago

Selected Answer: BC

B and C: FortiAnalyzer_7.0_Study_Guide-Online.pdf page 60:

Synchronizes logs and data securely among multiple FortiAnalyzer devices. System and configuration settings applicable to HA are also synchronized.

All devices must run in the same operation mode: analyzer or collector.

upvoted 2 times

Khs01 2 years ago

Selected Answer: BC

BC is Ok!

upvoted 2 times

morzart2025 2 years ago

B and C

FortiAnalyzer HA implementation works only in networks where Virtual Router Redundancy Protocol (VRRP) is permitted. Therefore it may not be supported by some public cloud infrastructures.

FortiAnalyzer_7.0_Study_Guide-Online pag. 60

upvoted 1 times

Question #10 *Topic 1*

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

A. FortiView Monitor

B. Threat hunting

C. Incidents dashboards

D. Outbreak alert services

Suggested Answer: *B*

Community vote distribution

B (100%)

PiotrSwi 9 months, 3 weeks ago

Selected Answer: B

B - Correct. FortiAnalyzer 7.0 Study Guide page 217.

upvoted 1 times

Marchrist 1 year, 4 months ago

Selected Answer: B

threat hunting

upvoted 1 times

lucient 1 year, 11 months ago

Selected Answer: B

B) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 217: Threat hunting consists in proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach will help administrator find any threats that might have eluded detection by the current security solutions or configurations.

upvoted 3 times

D10SJoker 1 year, 11 months ago

Answer is B

FortiAnalyzer_7.0_Study_Guide-Online pag. 217

upvoted 1 times

Khs01 2 years ago

Selected Answer: B

B is Ok!

upvoted 2 times

Question #11 *Topic 1*

When working with FortiAnalyzer reports, what is the purpose of a dataset?

A. To set the data included in templates

B. To retrieve data from the database

C. To provide the layout used for reports

D. To define the chart type to be used

Suggested Answer: *B*

Community vote distribution

B (100%)

PiotrSwi 9 months, 3 weeks ago

Selected Answer: B

B - Correct. FortiAnalyzer Administration 7.2. Study Guide page 190.

upvoted 1 times

jcarlosBO 1 year, 3 months ago

Selected Answer: B

Respuesta B

FortiAnalyzer_7.0_Study_Guide-Online pag. 257

upvoted 1 times

lucient 1 year, 11 months ago

Selected Answer: B

B) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 257:

Datasets: Structured Query Language (SQL) SELECT queries that extract specific data from the database

upvoted 4 times

D10SJoker 1 year, 11 months ago

Answer is B

FortiAnalyzer_7.0_Study_Guide-Online pag. 257

upvoted 1 times

Khs01 2 years ago

Selected Answer: B

B is Ok!

upvoted 1 times

Question #12 *Topic 1*

Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)

A. Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.

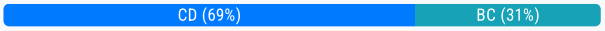
B. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.

C. Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.

D. Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.

Suggested Answer: *BD*

Community vote distribution



morzart2025 Highly Voted 2 years ago

C and D

Using FortiAnalyzer, you can enable log fetching. This allows FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer, which you can then run queries or reports on for forensic analysis.

The FortiAnalyzer device that fetches logs operates as the fetch client, and the other FortiAnalyzer device that sends logs operates as the fetch server. Log fetching can happen only between two FortiAnalyzer devices, and both of them must be running the same firmware version. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end.

FortiAnalyzer_7.0_Study_Guide-Online pag. 168

upvoted 8 times

PiotrSwi Most Recent 9 months, 3 weeks ago

C,D - Correct. FortiAnalyzer 7.0. Study Guide page 168.

upvoted 1 times

MaxTalin 10 months, 2 weeks ago

Coorect C and D

Log fetching is used to retrieve archived logs from one FortiAnalyzer device to another. This allows administrators to run queries and reports against historic data, which can be useful for forensic analysis.

Log fetching can only be done on two FortiAnalyzer devices running the same firmware

upvoted 2 times

SH_ 1 year, 3 months ago

Selected Answer: CD

CD are correct. See https://docs.fortinet.com/document/fortianalyzer/7.4.0/administration-guide/651442/log-fetching

upvoted 2 times

Michael348 1 year, 6 months ago

Selected Answer: CD

B - says the Perform 2 roles with same FortiAnalyzer device.

should perform 2 roles with different FortiAnalyzer device at the other end.

So should be C and D

upvoted 2 times

Robku 1 year, 7 months ago

C and D

FAZ must run the same firmware version

And a FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different

FortiAnalyzer devices at the other end.
Key word is different in this case.
upvoted 2 times

Nappel 1 year, 8 months ago

Selected Answer: BC

FortiAnalyzer_7.0_Study_Guide-Online page: 168 | Log Fetching can happen only between two FortiAnalyzer devices, and both of them must be running the same Firmware.
This makes Answer C correct

FortiAnalyzer_7.0_Study_Guide-Online page: 168 | A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different FortiAnalyzers devices at the other end.
This makes answer B correct.
upvoted 1 times

mohamedismail 8 months, 2 weeks ago

same FortiAnalyzer devices - which is B is wrong
upvoted 1 times

AngelCruz21 1 year, 9 months ago

Selected Answer: CD

C and D
upvoted 1 times

iZippo 1 year, 9 months ago

The correct statements regarding log fetching on FortiAnalyzer are:

B. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.

D. Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.

Explanation:

A is not a true statement because log fetching allows the administrator to fetch logs from other Fortinet devices, not from another FortiAnalyzer.

C is not a true statement because log fetching can be done between FortiAnalyzer devices running different firmware versions.

Therefore, B and D are the two statements that are true regarding log fetching on FortiAnalyzer.
upvoted 1 times

Fikachew 1 year, 9 months ago

Selected Answer: BC

B and C.
The answer D states that the FAZ fetches logs and sends the to a third FAZ to use. In the study guide at page 168 it states that it fetches logs from another FAZ and is being used by the current FAZ. Also documents says that this can only be done between two FAZ devices, NOT forwarded to a third.
upvoted 2 times

Christiandus 1 year, 9 months ago

Selected Answer: CD

C and D

Using FortiAnalyzer, you can enable log fetching. This allows FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer, which you can then run queries or reports on for forensic analysis.

The FortiAnalyzer device that fetches logs operates as the fetch client, and the other FortiAnalyzer device that sends logs operates as the fetch server. Log fetching can happen only between two FortiAnalyzer devices, and both of them must be running the same firmware version. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end.

FortiAnalyzer_7.0_Study_Guide-Online pag. 168
upvoted 3 times

certmeupnow 1 year, 10 months ago
C and D.

Classic devil in the details gotcha. B says *same* FortiAnalyzer devices, which is wrong... has to be *different* FAZ devices.
upvoted 1 times

KP001 1 year, 10 months ago
C and D

FortiAnalyzer_7.0_Study_Guide-Online page 168;

Log fetching can happen only between two FortiAnalyzer devices, and both of them must be running the same firmware version.

A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end.
(Key words different devices, makes answer B incorrect)
upvoted 1 times

nerostart 1 year, 10 months ago
Selected Answer: BC
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 168:

Log fetching can happen only between two FortiAnalyzer devices,
and both of them must be running the same firmware version.

A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end.
upvoted 2 times

Christiandus 1 year, 9 months ago
B. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.

Keyword is same. Your source clearly states the opposite.
upvoted 1 times

lucient 1 year, 11 months ago
Selected Answer: CD
C and D) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 168:

Using FortiAnalyzer, you can enable log fetching. This allows FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer, which you can then run queries or reports on for forensic analysis.

Log fetching can happen only between two FortiAnalyzer devices,
and both of them must be running the same firmware version.
upvoted 1 times

Khs01 2 years ago
Selected Answer: CD
C and D are the correct answers
upvoted 2 times

Question #13 *Topic 1*

Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)

A. By deploying different FortiAnalyzer devices in both modes, you can improve their overall performance.

B. When in collector mode. FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.

C. When in collector mode. FortiAnalyzer supports event management and reporting features.

D. Collector mode is the default operating mode.

Suggested Answer: *BD*

Community vote distribution

AB (100%)

066c9f3 1 month, 2 weeks ago

A, B

FortiAnalyzer Administrator 7.2 Study Guide p. 44

upvoted 1 times

PiotrSwi 9 months, 3 weeks ago

Selected Answer: AB

A,B - Correct.

upvoted 1 times

MaxTalin 10 months, 2 weeks ago

Correct A and B

A When operating in collector mode, the device collects logs from multiple devices and then forwards those logs, in their original binary format, to another device

B collector does not have the same feature-rich options as an analyzer, because its only purpose is to collect and forward logs. It does not allow event management or A collector does not have the same feature-rich options as an analyzer, because its only purpose is to collect and forward logs. It does not allow event management or reporting

upvoted 1 times

JIM231jim 1 year, 3 months ago

A and B

upvoted 1 times

chyeahhh 1 year, 5 months ago

can confirm this was on exam today (6/15)

upvoted 1 times

Robku 1 year, 7 months ago

A and B

C and D are definately wrong, which makes A and B correct.

upvoted 1 times

Westh 1 year, 9 months ago

Selected Answer: AB

See page 10 & 11

upvoted 2 times

iZippo 1 year, 9 months ago

The correct statements regarding FortiAnalyzer operating modes are:

B. When in collector mode, FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.

C. When in collector mode, FortiAnalyzer supports event management and reporting features.

Explanation:

A is not a true statement because there are no different operating modes to deploy multiple FortiAnalyzer devices. FortiAnalyzer can be deployed in either collector mode or analyzer mode.

D is not a true statement because analyzer mode is the default operating mode.

Therefore, B and C are the two statements that are true regarding FortiAnalyzer operating modes.
ChatGPT
upvoted 1 times

jl88 1 year, 9 months ago
iZippo, thank you for your help but using ChatGPT is very confusing. These generated answers and the community answers are different. So, in my opinion, this is not helpfull at all.
upvoted 1 times

CertificateStudyingGuy 1 year, 9 months ago
I wouldn't recommend using ChatGPT for something where reference material is frequently wrong, such as the main page here without scraping the comments
upvoted 2 times

Christiandus 1 year, 9 months ago
Selected Answer: AB
A and B are correct.
upvoted 1 times

KP001 1 year, 10 months ago
A and B are correct.

Default mode is analyzer mode.
Collector mode does not support events or reporting.
upvoted 1 times

nerostart 1 year, 10 months ago
Selected Answer: AB
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 10, 11
upvoted 1 times

lucient 1 year, 11 months ago
Selected Answer: AB
A) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 11: By using both analyzer and collector modes, you increase FortiAnalyzer performance: Collectors offload the task of receiving logs from multiple devices from the analyzer. This allows the analyzer to focus on data analysis and reporting tasks

B) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 10: When operating in collector mode, the device collects logs from multiple devices and then forwards those logs, in their original binary format, to another device, such as a FortiAnalyzer operating in analyzer mode.
upvoted 3 times

whatz 1 year, 11 months ago
D: is wrong since the default mode is Analyzer mode (https://docs2.fortinet.com/document/fortianalyzer/7.0.5/administration-guide/15523/analyzer-mode)
C: is wrong since in collector mode reporting and events are not supported.
(https://docs2.fortinet.com/document/fortianalyzer/7.0.5/administration-guide/412125/analyzer-and-collector-feature-comparison)
upvoted 1 times

stephanas 1 year, 11 months ago
Selected Answer: AB
A and B are correct
upvoted 1 times

D10SJoker 1 year, 11 months ago
A and B are correct.
FortiAnalyzer_7.0_Study_Guide-Online pag. 10
upvoted 2 times

Khs01 2 years ago

Selected Answer: AB

A and B are the correct answers

upvoted 3 times

Question #14 *Topic 1*

Which statement is true about sending notifications with incident updates?

A. You can send notifications to multiple external platforms.

B. If you use multiple fabric connectors, all connectors must have the same notification settings.

C. Notifications can be sent only by email.

D. Notifications can be sent only when an incident is updated or deleted.

Suggested Answer: *A*

Community vote distribution

A (100%)

PiotrSwi 9 months, 3 weeks ago

Selected Answer: A

A - Correct.

upvoted 1 times

KP001 1 year, 10 months ago

A is correct.

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 213.

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.

upvoted 4 times

nerostart 1 year, 10 months ago

Selected Answer: A

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 201

upvoted 1 times

lucient 1 year, 11 months ago

Selected Answer: A

A) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 34: Fabric connectors also enable FortiAnalyzer to send notifications to ITSM platforms when a new incident is created or for any subsequent updates.

upvoted 1 times

D10SJoker 1 year, 11 months ago

Correct answer is A.

FortiAnalyzer_7.0_Study_Guide-Online pag. 34

upvoted 1 times

Khs01 2 years ago

Selected Answer: A

A is Ok!

upvoted 1 times

Question #15 *Topic 1*

Which SQL query is in the correct order to query the database in the FortiAnalyzer?

A. SELECT devid WHERE 'user'='USER1' FROM $log GROUP BY devid

B. FROM $log WHERE 'user'='USER1' SELECT devid GROUP BY devid

C. SELECT devid FROM $log WHERE 'user'='USER1' GROUP BY devid

D. SELECT devid FROM $log GROUP BY devid WHERE 'user'='USER1'

Suggested Answer: *C*

Community vote distribution

C (100%)

[Removed] 1 year, 3 months ago

C is correct

upvoted 1 times

chyeahhh 1 year, 5 months ago

can confirm this was on exam today (6/15)

upvoted 1 times

KP001 1 year, 10 months ago

C is correct.

SELECT - FROM - GROUP

upvoted 1 times

nerostart 1 year, 10 months ago

Selected Answer: C

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 317 - SQL and Dataset

upvoted 1 times

lucient 1 year, 11 months ago

Selected Answer: C

C) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 259: The main clauses FortiAnalyzer reports use are as follows:

•FROM

•WHERE

•GROUP BY

•ORDER BY

• LIMIT

• OFFSET

Accordingly, following the SELECT keyword, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide.

upvoted 3 times

Khs01 2 years ago

C is OK!

upvoted 1 times

Question #16 *Topic 1*

A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed by that rogue administrator on FortiAnalyzer.
What can you do on FortiAnalyzer to accomplish this?

A. Click Task Monitor and view the tasks performed by that administrator.

B. Click Fabric View and view the tasks performed by the rogue administrator.

C. Click Log View and generate a report for that administrator.

D. Click FortiView and generate a report for that administrator.

Suggested Answer: *C*

Community vote distribution

A (100%)

PiotrSwi 9 months, 3 weeks ago

Selected Answer: A

A - Correct.

upvoted 1 times

Thomas_2020 1 year, 2 months ago

The answer is A since the administrator access was presented in the FAZ, not in the FGT

upvoted 1 times

[Removed] 1 year, 3 months ago

A is correct

upvoted 1 times

Marchrist 1 year, 4 months ago

Selected Answer: A

A is correct

upvoted 1 times

jafaxe791 1 year, 8 months ago

A is the correct answer as mentioned below by other users

upvoted 1 times

iZippo 1 year, 9 months ago

C. Click Log View and generate a report for that administrator.

Explanation:

The Log View feature on FortiAnalyzer provides a way to view and analyze log data. To generate a report for the rogue administrator, you can apply filters to the log data to show only the activity performed by that administrator.

upvoted 2 times

lsl 1 year, 6 months ago

Please stop posting ChatGPT responses.

upvoted 3 times

lucient 1 year, 11 months ago

Selected Answer: A

A) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 54: View the tasks FortiAnalyzer administrators have performed, including progress and status.

upvoted 3 times

G33 1 year, 11 months ago

A is the correct answer

upvoted 1 times

Khs01 2 years ago

Selected Answer: A

Correct answer is A

upvoted 2 times

Question #17 *Topic 1*

Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two.)

A. Both modes, forwarding and aggregation, support encryption of logs between devices.

B. In aggregation mode, you can forward logs to syslog and CEF servers as well.

C. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.

D. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.

Suggested Answer: *BD*

Community vote distribution

AC (100%)

MaxTalin 10 months, 2 weeks ago

Correct A and C

Aggregation mode stores logs and content files and uploads them to the FortiAnalyzer server at a scheduled time.

upvoted 1 times

chyeahhh 1 year, 5 months ago

can confirm this was on exam today (6/15)

upvoted 1 times

kavela1 1 year, 10 months ago

C&D

https://docs2.fortinet.com/document/fortianalyzer/7.0.5/administration-guide/420493/modes

upvoted 1 times

nerostart 1 year, 10 months ago

Selected Answer: AC

Aggregation mode is only supported between two FortiAnalyer devices.

upvoted 1 times

lucient 1 year, 11 months ago

Selected Answer: AC

Right answers

A) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 148: The log communication between devices can be protected by encryption, with the desired encryption level, using the commands shown on the slide. (You need to interpret this. "Real time" and "aggregation" is about the "moment" when Fortigate sends the logs. However, no matter the moment, Fortigate will upload logs encrypted or unencrypted based on previous / differente config).

C) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 147: Aggregation: Logs and content files stored and uploaded at scheduled time.

Wrong answers

B) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 146: Aggregation mode is only supported between two FortiAnalyzer devices.

D) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 147: FortiAnalyzer can also forward logs in real-time mode to a syslog server, a Common Event Format (CEF) server, or another FortiAnalyzer.

upvoted 3 times

ilbartonicola 1 year, 11 months ago

Selected Answer: AC

Aggregation mode is only supported between two FortiAnalyer devices, so B is wrong

forwarding mode can forward logs in real-time mode to a syslog server, cef or another fortianalyzer

upvoted 1 times