NSE5_FAZ-7.0 Q&As

Fortinet NSE 5 - FortiAnalyzer 7.0

Pass Fortinet NSE5_FAZ-7.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/nse5_faz-7-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)

A. RADIUS

B. Local

C. LDAP

D. PKI

E. TACACS+

Correct Answer: ACE

QUESTION 2

An administrator has moved FortiGate A from the root ADOM to ADOM1. However, the administrator is not able to generate reports for FortiGate A in ADOM1.

What should the administrator do to solve this issue?

A. Use the execute sql-local rebuild-db command to rebuild all ADOM databases.

B. Use the execute sql-local rebuild-adom ADOM1 command to rebuild the ADOM database.

C. Use the execute sql-report run ADOM1 command to run a report.

D. Use the execute sql-local rebuild-adom root command to rebuild the ADOM database.

Correct Answer: B

Reference: https://help.fortinet.com/fmgr/cli/5-6- 1/FortiManager_CLI_Reference/700_execute/sql-local+.htm

QUESTION 3

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. The security risk was blocked or dropped.

B. The security event risk is considered open.

C. An incident was created from this event.

D. The risk source is isolated.

Correct Answer: A

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

QUESTION 4

Which statement is true about sending notifications with incident updates?

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

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

C. Notifications can be sent only by email.

D. You can send notifications to multiple external platforms

Correct Answer: D

FortiAnalyzer_7.0_Study_Guide-Online pag. 34

QUESTION 5

What is the purpose of a dataset query in FortiAnalyzer?

A. It sorts log data into tables

B. It extracts the database schema

C. It retrieves log data from the database

D. It injects log data into the database

Correct Answer: C

Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.4/administration- guide/148744/creating-datasets

QUESTION 6

Which statement is true when you are upgrading the firmware on an HA cluster made up of two FortiAnalyzer devices?

A. First, upgrade the secondary device, and then upgrade the primary device.

B. Both FortiAnalyzer devices will be upgraded at the same time.

C. You can enable uninterruptible-upgrade so that the normal FortiAnalyzer operations are not interrupted while the cluster firmware upgrades.

D. You can perform the firmware upgrade using only a console connection.

Correct Answer: A

https://docs.fortinet.com/document/fortianalyzer/7.2.0/upgrade-guide/262607/upgrading-fortianalyzer-firmware

>To upgrade firmware for a cluster, Fortinet recommends upgrading the HA secondary units first, followed by the HA primary unit last.

QUESTION 7

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

A. A FortiGate ADOM

B. The FortiGate serial number

C. A pre-shared key

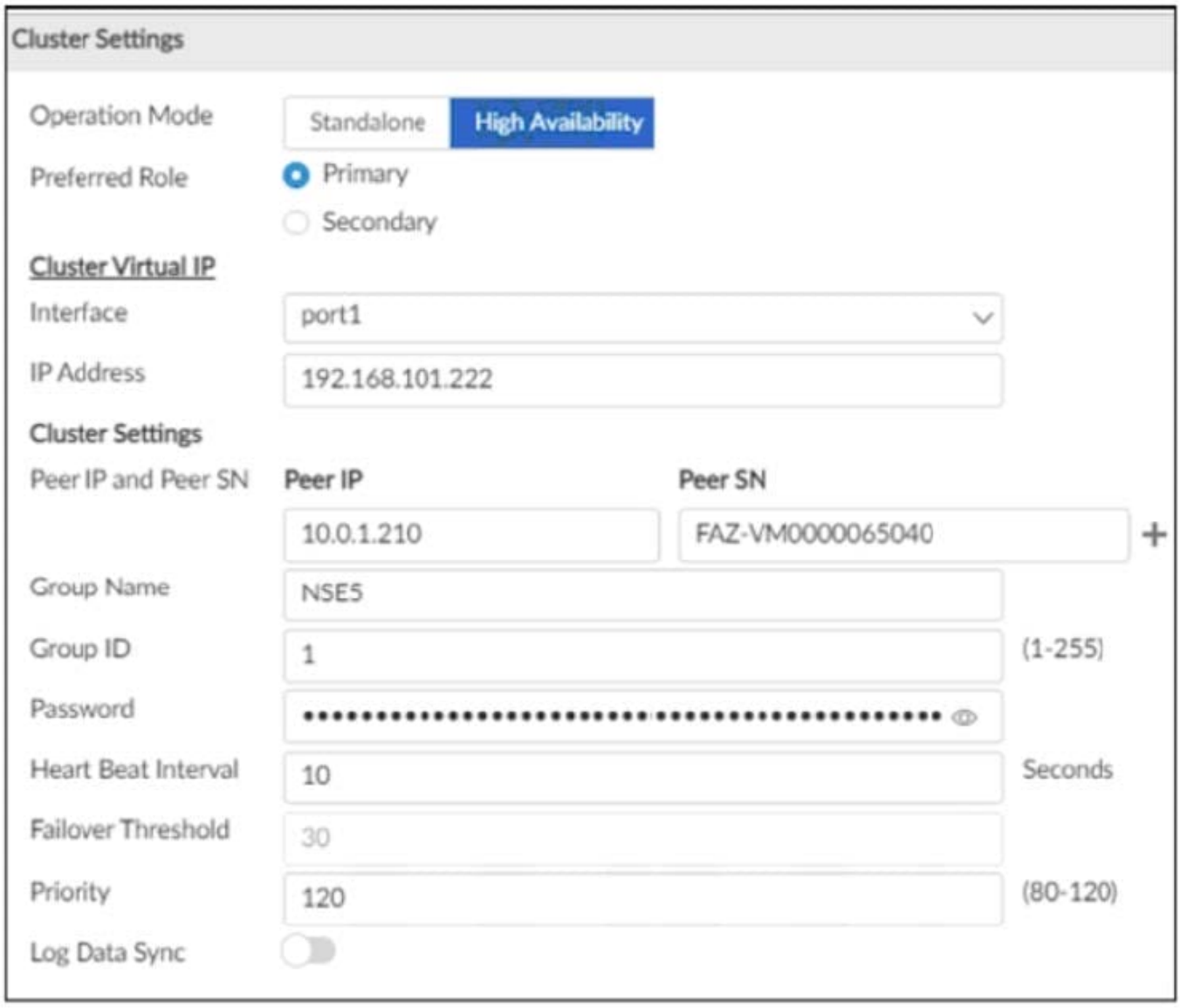
D. Valid FortiAnalyzer credentials

Correct Answer: 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

QUESTION 8

Refer to the exhibit.



The image displays the configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster. What can you conclude from the configuration displayed?

A. This FortiAnalyzer will join to the existing HA cluster as the primary.

B. This FortiAnalyzer is configured to receive logs in its port1.

C. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.

D. After joining to the cluster, this FortiAnalyzer will keep an updated log database.

Correct Answer: B

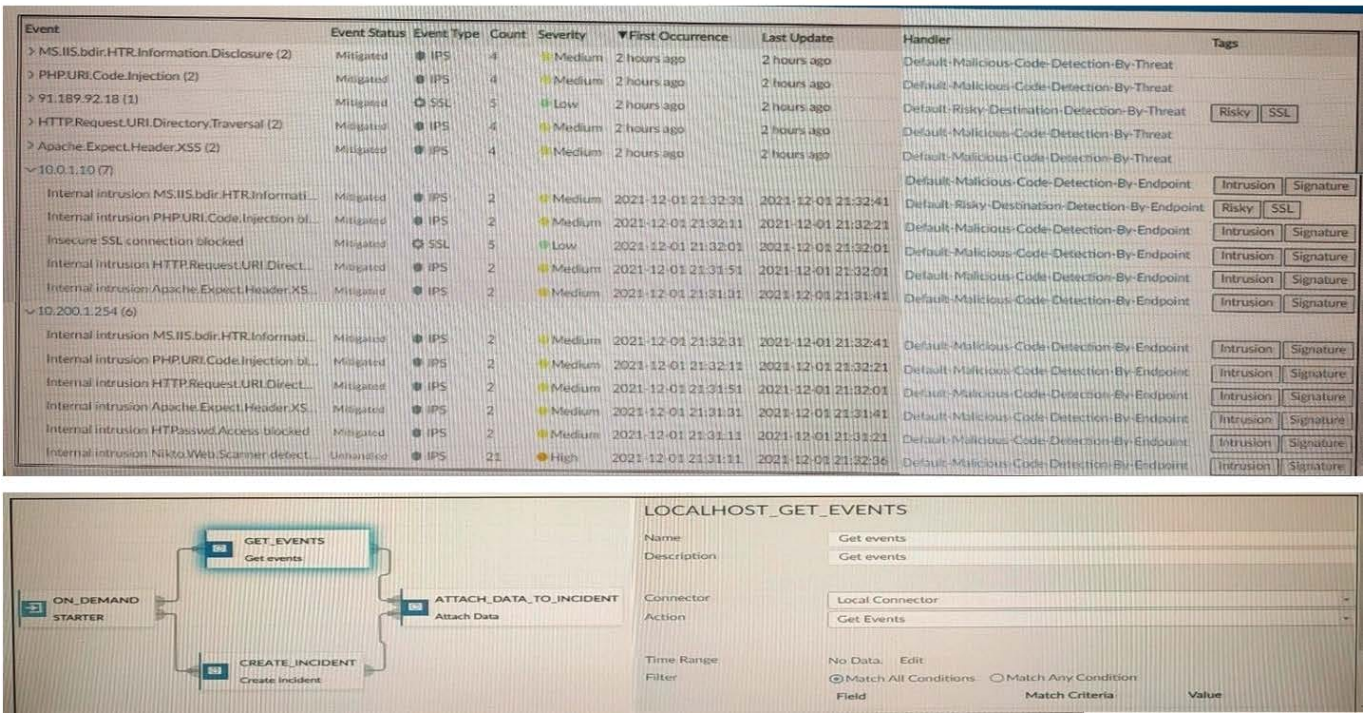
If the preferred role is Primary, then this unit becomes the primary unit if it is configured first in a new HA cluster. If there is an existing primary unit, then this unit becomes a secondary unit.

QUESTION 9

Refer to the exhibits.

Page 306 of 7.0 study guide
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG- FAZ/2300_Reports/0025_Auto-cache.htm

QUESTION 18
Refer to the exhibits.



Page 306 of 7.0 study guide Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/2300_Reports/0025_Auto-cache.htm

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

A. Ten events will be added.

B. No events will be added.

C. Five events will be added.

D. Thirteen events will be added.

Correct Answer: C

QUESTION 10

FortiAnalyzer uses the Optimized Fabric Transfer Protocok (OFTP) over SSL for what purpose?

A. To upload logs to an SFTP server

B. To prevent log modification during backup

C. To send an identical set of logs to a second logging server

D. To encrypt log communication between devices

Correct Answer: D

QUESTION 11

Which daemon is responsible for enforcing the log file size?

A. sqlplugind

B. logfiled

C. miglogd

D. ofrpd

Correct Answer: B

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

QUESTION 12

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 FortiView and generate a report for that administrator.

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

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

D. View the tasks performed by the rogue administrator in Fabric View.

Correct Answer: A

Reference: https://docs.fortinet.com/document/fortimanager/6.4.1/administration- guide/792943/task-monitor

QUESTION 13

What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

A. Chart Builder

B. Export to Report Chart

C. Dataset Library

D. Custom View

Correct Answer: A

Keyword is Fortiview feature. Chart Builder is in Log view and the export to report chart is in the fortiview. they are both similar just generated in different areas.

QUESTION 14

What is the purpose of the following CLI command?

```
# configure system global
    set log-checksum md5
end
```

A. To add a log file checksum

B. To add the MD\\'s hash value and authentication code

C. To add a unique tag to each log to prove that it came from this FortiAnalyzer

D. To encrypt log communications

Correct Answer: A

https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli- reference/849211/global

QUESTION 15

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

A. Forwarded logs cannot be filtered to match specific criteria.

B. Logs are forwarded in real-time only.

C. The client retains a local copy of the logs after forwarding.

D. You can use aggregation mode only with another FortiAnalyzer.

Correct Answer: CD

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/420493/modes
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/621804/log- forwarding