Vendor: Fortinet

Exam Code: NSE5_FAZ-7.0

Exam Name: Fortinet NSE 5 - FortiAnalyzer 7.0

Version: DEMO

QUESTION 1
What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server?
(Choose two.)

A. SFTP, FTP, or SCP server
B. Mail server
C. Output profile
D. Report scheduling

Answer: AC
Explanation:
There is an option for "uploading reports to server" under configuring the output profile. The available options are: SFTP, FTP and SCP. You have to be careful on the question itself. The question tells you to "upload reports to a server (external server). Which means, a server has been configured already in this case prior to enabling the "upload reports to server".

QUESTION 2
Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)

A. 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.
B. Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.
C. Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.
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.

Answer: BD
Explanation:
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.

QUESTION 3
Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two.)

A. In aggregation mode, you can forward logs to syslog and CEF servers as well.
B. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.
C. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
D. Both modes, forwarding and aggregation, support encryption of logs between devices.

Answer: CD
Explanation:
Aggregation mode is only supported between two FortiAnalyer devices, so A is wrong.
Forwarding is always in real time and does not ONLY forward to other FortiAnalyzer devices. It also forwards to Syslog/CEF. B is wrong.

QUESTION 4
An administrator, fortinet, is able to view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mail server that can be used to send alert emails.
What can be the problem?

A. Fortinet is assigned the Standard_ User administrator profile.
B. A trusted host is configured.
C. ADOM mode is configured with Advanced mode.
D. Fortinet is assigned the Restricted_ User administrator profile.

Answer: A
Explanation:
• Super_User, which, like in FortiGate, provides access to all device and system privileges.
• Standard_User, which provides read and write access to device privileges, but not system privileges.
• Restricted_User, which provides read access only to device privileges, but not system privileges. Access to the Management extensions is also removed.
• No_Permissions_User, which provides no system or device privileges. Can be used, for example, to temporarily remove access granted to existing admins.

QUESTION 5
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.

Answer: A
Explanation:
To upgrade firmware for a cluster, Fortinet recommends upgrading the HA secondary units first, followed by the HA primary unit last.
https://docs.fortinet.com/document/fortianalyzer/7.2.0/upgrade-guide/262607/upgrading-fortianalyzer-firmware

QUESTION 6
What is the purpose of output variables?

A. To store playbook execution statistics
B. To use the output of the previous task as the input of the current task
C. To display details of the connectors used by a playbook

D. To save all the task settings when a playbook is exported

Answer: B
Explanation:
Output variables allow you to use the output from a preceding task as an input to the current task

QUESTION 7
Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

A. System information
B. Logs from registered devices
C. Report information
D. Database snapshot

Answer: AC
Explanation:
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.

QUESTION 8
Which two statements are correct regarding the export and import of playbooks? (Choose two.)

A. You can export only one playbook at a time.
B. You can import a playbook even if there is another one with the same name in the destination.
C. Playbooks can be exported and imported only within the same FortiAnaryzer.
D. A playbook that was disabled when it was exported, will be disabled when it is imported.

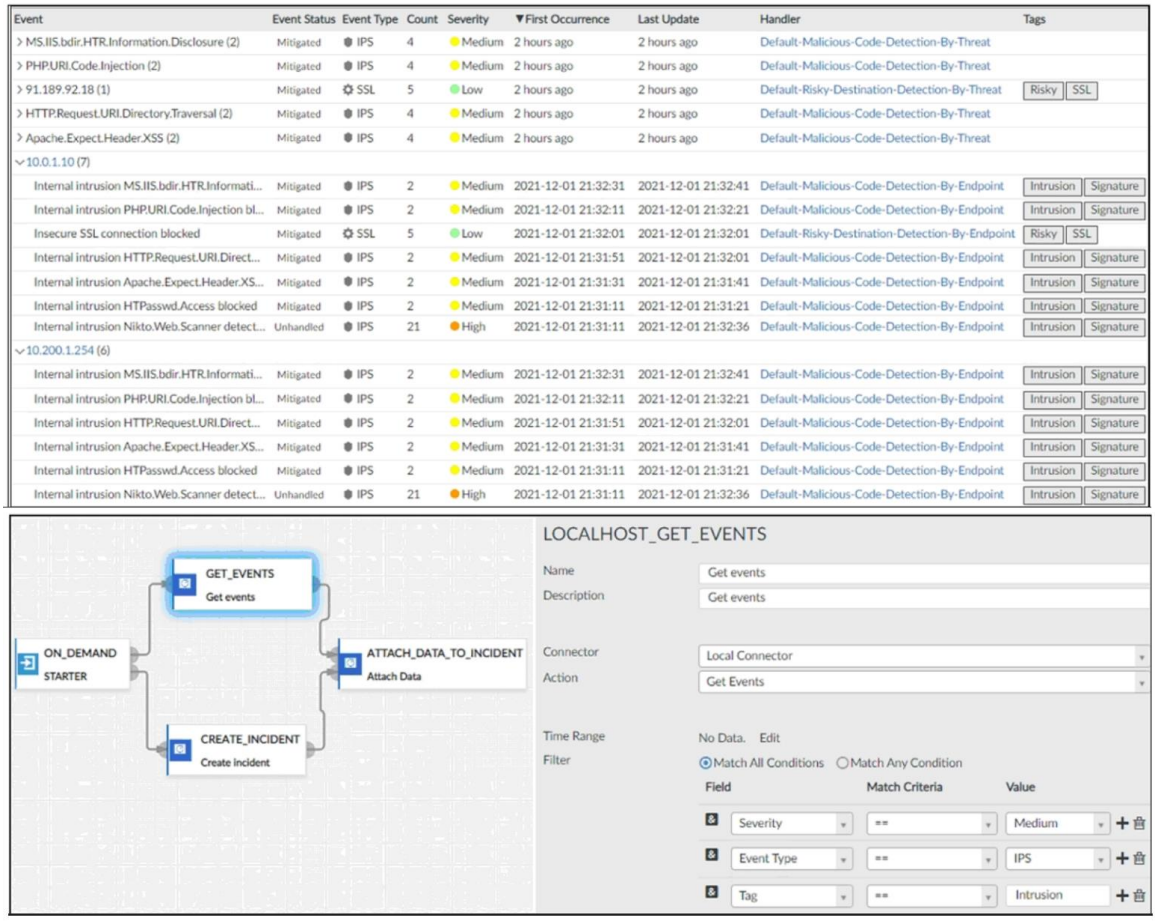
Answer: BD
Explanation:
B: If the imported playbook has the same name as an existing one, FortiAnalyzer will create a new name that includes a timestamp to avoid conflicts.
D: Playbooks are imported with the same status they had (enabled or disabled) when they were exported. Playbooks set to run automatically should be exported while they are disabled to avoid unintended runs on the destination.

QUESTION 9
Which SQL query is in the correct order to query the database in the FortiAnslyzer?

A. SELECT devid FROM Slog GROOP BY devid WHERE * user' =* USERl'
B. SELECT devid WHERE 'u3er'='USERl' FROM $ log GROUP BY devid
C. SELECT devid FROM Slog- WHERE *user' =' USERl' GROUP BY devid
D. FROM Slog WHERE 'user* =' USERl' SELECT devid GROUP BY devid

Answer: C

QUESTION 110
Refer to the exhibits. 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.

Answer: A
Explanation:
Intrusion + IPS + Medium = 10

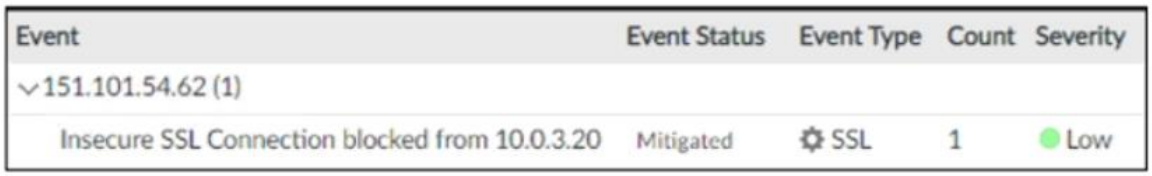
QUESTION 11
Which daemon is responsible for enforcing the log file size?

A. sqlplugind
B. logfiled
C. miglogd
D. ofrpd

Answer: B

Explanation:
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.

QUESTION 12
Refer to the exhibit. 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.

Answer: A
Explanation:
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.

QUESTION 13
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

Answer: D
Explanation:
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.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

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

★ Average **99.9%** Success Rate.

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

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

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

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

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

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html