

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' =\* USERI'
- B. SELECT devid WHERE 'u3er'='USERI' FROM \$ log GROUP BY devid
- C. SELECT devid FROM Slog- WHERE \*user' =' USERI' GROUP BY devid
- D. FROM Slog WHERE 'user\* =' USERI' 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?

Internal intrusion PHPURICodeInjection bL.       Miligated       IPS       2       Medium       2021-12-01 21:32:11       2021-12-01 21:32:12       Default-Malicious-Code-Detection-By-Endpoint       Intrusion Signatu         Insecure SSL connection blocked       Miligated       OS SL       5       Low       2021-12-01 21:32:01       Default-Malicious-Code-Detection-By-Endpoint       Risky SSL         Internal intrusion HTTP.Request.URLDirect       Miligated       IPS       2       Medium       2021-12-01 21:32:01       Default-Malicious-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion Apache.Expect.Header.XS       Miligated       IPS       2       Medium       2021-12-01 21:31:31       2021-12-01 21:31:21       Default-Malicious-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion NITPAsswd.Access blocked       Miligated       IPS       2       Medium       2021-12-01 21:31:11       2021-12-01 21:32:31       Default-Malicious-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion NILSDdir.HTR.Informati       Miligated       IPS       2       Medium       2021-12-01 21:32:31       2021-12-01 21:32:41       Default-Malicious-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion NILSDdir.HTR.Informati       Miligated       IPS       2       Medium       2021	Event	Event Status	Event Type	Count	Severity	▼First Occurrence	Last Update	Handler	Tags		
>9.1189.92.18 (1)       Migazet       Q SSL       5       Uz       Phorn ago       Default-Makicon-Detection-By-Threat       Reky SSL         >AMTRERequest.UB.Directory,Tavenal (2)       Migazet       IPS       4       Median       2 hours ago       Default-Makicon-Code-Detection-By-Threat         >Aquebe.Expect.Header.XSL (2)       Migazet       IPS       4       Median       2 hours ago       Default-Makicon-Code-Detection-By-Threat         >V001.107       Internal intrusion MSIIS.bdr.MTR.Informat       Migazet       IPS       2       Median       2021-12:01 21:32:11       2021-12:01 21:32:12       Default-Makicon-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion MPH/DRICode.lipection B       Migazet       IPS       2       Median       2021-12:01 21:32:01       Default-Makicon-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion MPH/DRICode.lipection B       Migazet       IPS       2       Median       2021-12:01 21:32:01       Default-Makicon-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion MSIIS.bdr.MTRIMental       Migazet       IPS       2       Median       2021-12:01 21:31:11       2021-12:01 21:31:11       2021-12:01 21:32:11       Default-Makicon-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion MSIIS.bdr.MTRImental <td>&gt; MS.IIS.bdir.HTR.Information.Disclosure (2)</td> <td>Mitigated</td> <td>IPS IPS</td> <td>4</td> <td>Medium</td> <td>2 hours ago</td> <td>2 hours ago</td> <td>Default-Malicious-Code-Detection-By-Threat</td> <td></td>	> MS.IIS.bdir.HTR.Information.Disclosure (2)	Mitigated	IPS IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat			
1) HTPRequestURIDirectory.Traversal (2)       Misjated       9 IPS       4       Meduar       2 hours ago       Default-Malicious-Code-Detection-By-Threat         2) Agache Expect.Header.XSS (2)       Misjated       9 IPS       4       Meduar       2 hours ago       Default-Malicious-Code-Detection-By-Threat         +100.1107       Internal Intrusion SIISbidt/TRI-Informat.       Misjated       9 IPS       2       Meduar       2021-12-01 21:32:41       Default-Malicious-Code-Detection-By-Endpoint       Intrusion Signature         Internal Intrusion PMPURI Code.Injection bl.       Misjated       9 IPS       2       Meduar       2021-12-01 21:32:01       Default-Malicious-Code-Detection-By-Endpoint       Intrusion Signature         Internal Intrusion Apple Decol.Apple: Code.Injection Apple Endpoint       Internal Intrusion Apple Decol.Apple: Code.Injection Apple: Endpoint       Internal Intrusion Signature       PIPS       2       Meduar       2021-12-01 21:32:01       Default-Malicious-Code-Detection-By-Endpoint       Internal Intrusion Signature         Internal Intrusion MITPRequestURB.Direct.       Misjated       PIPS       2       Meduar       2021-12-01 21:32:11       2021-12-01 21:32:12       Default-Malicious-Code-Detection-By-Endpoint       Internal Intrusion Signature         Internal Intrusion Misibadir.HTRI-Informat.       Misjated       PIPS       2       Meduar       2021-12-01 21:32:11	> PHP.URI.Code.Injection (2)	Mitigated	IPS IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat			
A Aache Expect. Header.XSS [2]       Migued       IPS       4       Indexing and the approximation of the approximatin approximate of the size of the approximate of the size	> 91.189.92.18 (1)	Mitigated	¢ SSL	5	Low	2 hours ago	2 hours ago	Default-Risky-Destination-Detection-By-Threat	Risky SSL		
ADD.1.10[7] Internal Intrusion MSIIS.bdf:HTR.Informati Misjaeta     IPS         1PS         2 Media         2021-12-01 21:32:31         2021-12-01 21:32:41         Default-Malicious-Code-Detection-By-Endpoint         Intrusion         Signatu         Internal Intrusion PHPURILCode.Injection bi.         Misjaeta         1PS         2 Media         2021-12-01 21:32:31         2021-12-01 21:32:41         Default-Malicious-Code-Detection-By-Endpoint         Intrusion         Signatu         Internal Intrusion PHPURILCode.Injection         Misjaeta         1PS         2 Media         2021-12-01 21:32:0         Default-Malicious-Code-Detection-By-Endpoint         Intrusion         Signatu         Internal Intrusion PHPURILCode.Injection         Misjaeta         1PS         2 Media         2021-12-01 21:32:0         Default-Malicious-Code-Detection-By-Endpoint         Intrusion         Signatu         Internal Intrusion MITPRequestURI.Direct         Misjaeta         1PS         2 Media         2021-12-01 21:32:1         2021-12-01 21:32:0         Default-Malicious-Code-Detection-By-Endpoint         Intrusion         Signatu         Internal Intrusion MISto Web.Scamer detect         Unsuaded         IPS         2 Media         2021-12-01 21:32:1         2021-12-01 21:32:3         Default-Malicious-Code-Detection-By-Endpoint         Intrusion         Signatu         Internal Intrusion MISto Web.Scamer detect         Unsuaded         IPS         2 Media         2021-12-01 21:32:3         2021-12-01 21:32:4         Default-Malicious-Code-Detection-By-Endpoint         Intrusion         Signatu         Internal Intrusion MISto Web.Scamer detect         Unsuaded         IPS         2 Media         2021-12-01 21:32:3         2021-12-01 21:32:4         Default-Malicious-Code-Detection-By-Endpoint         Intrusion         Signatu         Internal Intrusion MITPRequestInt         IPS         2 Media         2021-12-01 21:32:3         2021-12-01 21:32:4         Default-Malicious-Code-Detection-By-Endpoint	> HTTP.Request.URI.Directory.Traversal (2)	Mitigated	IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat			
Internal Intrusion MSIISbdfr.HTR.Informati       Mitigatel       IPS       2       Median       2021-12-01       2132241       Default-Malicious-Code-Detection-By-Endpoint       Intrusion       Signatu         Internal Intrusion PHURIC Code.Injection bL       Mitigatel       IPS       2       Median       2021-12-01       2132211       Default-Malicious-Code-Detection-By-Endpoint       Intrusion       Signatu         Internal Intrusion PHURIC Code.Injection bL       Mitigatel       IPS       2       Median       2021-12-01       2132210       Default-Malicious-Code-Detection-By-Endpoint       Intrusion       Signatu         Internal Intrusion MIRID Mache.Espect Header-XL       Mitigatel       IPS       2       Median       2021-12-01       213312       Default-Malicious-Code-Detection-By-Endpoint       Intrusion       Signatu         Internal Intrusion MIRID Meb.Scamer detect       Unhanded       IPS       2       Median       2021-12-01       213221       Default-Malicious-Code-Detection-By-Endpoint       Intrusion       Signatu         Internal Intrusion MIRID Meb.Scamer detect       Unhanded       IPS       2       Median       2021-12-01       213221       Default-Malicious-Code-Detection-By-Endpoint       Intrusion       Signatu         Internal Intrusion MIRID Meb.Scamer detect       Unhanded       IPS <t< td=""><td>&gt; Apache.Expect.Header.XSS (2)</td><td>Mitigated</td><td>IPS IPS</td><td>4</td><td>Medium</td><td>2 hours ago</td><td>2 hours ago</td><td>Default-Malicious-Code-Detection-By-Threat</td><td></td></t<>	> Apache.Expect.Header.XSS (2)	Mitigated	IPS IPS	4	Medium	2 hours ago	2 hours ago	Default-Malicious-Code-Detection-By-Threat			
Internal intrusion PHPURI.Code.Injection bL.       Milgated       IPS       2       Medium       2021-12-01 21:32:11       2021-12-01 21:32:21       Default-Mulicious-Code-Detection-By-Endpoint       Intrusion       Signatu         Internal intrusion HTPRequest.URI.Direct       Milgated       IPS       2       Medium       2021-12-01 21:32:10       2021-12-01 21:32:00       Default-Mulicious-Code-Detection-By-Endpoint       Intrusion       Signatu         Internal intrusion HTPRequest.URI.Direct       Milgated       IPS       2       Medium       2021-12-01 21:31:11       2021-12-01 21:32:01       Default-Mulicious-Code-Detection-By-Endpoint       Intrusion       Signatu         Internal intrusion HTPRequest.URI.Direct       Milgated       IPS       2       Medium       2021-12-01 21:31:11       2021-12-01 21:32:01       Default-Mulicious-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion NISLOWeb.Scanner detect       Unhanded       IPS       2       Medium       2021-12-01 21:32:11       2021-12-01 21:32:01       Default-Mulicious-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion NSIIS.bidr.HTR.Informati       Milgated       IPS       2       Medium       2021-12-01 21:32:11       2021-12-01 21:32:10       Default-Mulicious-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion PAURI.C	~10.0.1.10 (7)										
Insecure SSL connection blocked       Mitigate       Q SSL       5       Low       2021-12-01 21:32:0       Default-Risky-Destination-Detection-By-Endpoint       Risky SSL         Internal intrusion HTTPRequestURI.Direct.       Mitigated       IPS       2       Medium       2021-12-01 21:31:0       2021-12-01 21:32:0       Default-Malicious-Code-Detection-By-Endpoint       Ristrusion Signatu         Internal intrusion HTTPRequestURI.Direct.       Mitigated       IPS       2       Medium       2021-12-01 21:31:1       2021-12-01 21:32:0       Default-Malicious-Code-Detection-By-Endpoint       Ristrusion Signatu         Internal intrusion HTTPRequestURI.Direct.       Mitigated       IPS       2       Medium       2021-12-01 21:32:1       2021-12-01 21:32:0       Default-Malicious-Code-Detection-By-Endpoint       Ristrusion Signatu         v102001254 (d)       Internal intrusion NSIUSbdir/HTRInformati.       Mitigated       IPS       2       Medium       2021-12-01 21:32:1       2021-12-01 21:32:0       Default-Malicious-Code-Detection-By-Endpoint       Ristrusion Signatu         Internal intrusion PRRquestURI.Direct.       Mitigated       IPS       2       Medium       2021-12-01 21:32:1       2021-12-01 21:32:0       Default-Malicious-Code-Detection-By-Endpoint       Ristrusion Signatu         Internal intrusion PRRquestURI.Direct.       Mitigated       IPS       2 <t< td=""><td>Internal intrusion MS.IIS.bdir.HTR.Informati</td><td>Mitigated</td><td>IPS</td><td>2</td><td>Medium</td><td>2021-12-01 21:32:31</td><td>2021-12-01 21:32:41</td><td>Default-Malicious-Code-Detection-By-Endpoint</td><td>Intrusion Signature</td></t<>	Internal intrusion MS.IIS.bdir.HTR.Informati	Mitigated	IPS	2	Medium	2021-12-01 21:32:31	2021-12-01 21:32:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature		
Internal intrusion HTTPRequest.URI.Direct Miligated 0 IPS 2 0 Medium 2021-12-01 21:31:51 2021-12-01 21:32:10 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion NTPAsswelAccess blocked Miligated 0 IPS 2 0 Medium 2021-12-01 21:31:11 2021-12-01 21:31:21 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MS.IIS.bdir.HTR.Informat Miligated 0 IPS 2 0 Medium 2021-12-01 21:32:11 2021-12-01 21:32:32 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MS.IIS.bdir.HTR.Informat Miligated 0 IPS 2 0 Medium 2021-12-01 21:32:11 2021-12-01 21:32:12 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MS.IIS.bdir.HTR.Informat Miligated 0 IPS 2 0 Medium 2021-12-01 21:32:11 2021-12-01 21:32:12 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MS.IIS.bdir.HTR.Informat Miligated 0 IPS 2 0 Medium 2021-12-01 21:32:11 2021-12-01 21:32:10 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MS.IIS.bdir.HTR.Informat Miligated 0 IPS 2 0 Medium 2021-12-01 21:32:11 2021-12-01 21:32:10 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MS.IIS.bdir.HTR.Informat Miligated 0 IPS 2 0 Medium 2021-12-01 21:32:11 2021-12-01 21:32:10 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Apache.Expect.Header.XS Miligated 0 IPS 2 0 Medium 2021-12-01 21:31:11 2021-12-01 21:32:10 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MIRD.Web.Scanner detect Unhandled 0 IPS 2 0 Medium 2021-12-01 21:31:11 2021-12-01 21:31:11 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Niko.Web.Scanner detect Unhandled 0 IPS 2 0 Medium 2021-12-01 21:31:11 2021-12-01 21:31:20 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Milito.Web.Scanner detect Unhandled 0 IPS 21 0 High 2021-12-01 21:31:11 2021-12-01 21:	Internal intrusion PHP.URI.Code.Injection bl	Mitigated	IPS	2	Medium	2021-12-01 21:32:11	2021-12-01 21:32:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature		
Internal intrusion Apache Expect HeaderXS Mitigated 0 IPS 2 0 Medium 2021-12-01 21:31:31 2021-12-01 21:31:41 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MIRDWeb Scanner detect Unhanded 0 IPS 2 0 Medium 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MSIIS bdir,HTR.Informati Mitigated 0 IPS 2 0 Medium 2021-12-01 21:32:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MSIIS bdir,HTR.Informati Mitigated 0 IPS 2 0 Medium 2021-12-01 21:32:11 2021-12-01 21:32:21 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MFIPD RFD.RCD.elinetton Mitigated 0 IPS 2 0 Medium 2021-12-01 21:32:11 2021-12-01 21:32:21 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion PHPD.RCD.elinetton Mitigated 0 IPS 2 0 Medium 2021-12-01 21:32:11 2021-12-01 21:32:21 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion ACcess blocked Mitigated 0 IPS 2 0 Medium 2021-12-01 21:31:11 2021-12-01 21:32:10 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion NHTP.Request.URI.Direct Mitigated 0 IPS 2 0 Medium 2021-12-01 21:31:11 2021-12-01 21:31:10 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nito.Web Scanner detect Unhandled 0 IPS 2 0 Medium 2021-12-01 21:31:11 2021-12-01 21:31:10 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nito.Web Scanner detect Unhandled 0 IPS 21 0 High 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nito.Web Scanner detect Unhandled 0 IPS 21 0 High 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nito.Web Scanner detect Unhandled 0 IPS 21 0 High 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-D	Insecure SSL connection blocked	Mitigated	¢ SSL	5	Low	2021-12-01 21:32:01	2021-12-01 21:32:01	Default-Risky-Destination-Detection-By-Endpoint	Risky SSL		
Internal intrusion HTPasswitAccess blocked Mitigated PIPS 2 • Medium 2021-12-01 21:31:1 2021-12-01 21:32:30 Default Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion NSUIS.bdir.HTRLnformati. Mitigated PIPS 2 • Medium 2021-12-01 21:32:1 2021-12-01 21:32:41 Default Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MSUIS.bdir.HTRLnformati. Mitigated PIPS 2 • Medium 2021-12-01 21:32:1 2021-12-01 21:32:41 Default Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MSUIS.bdir.HTRLnformati. Mitigated PIPS 2 • Medium 2021-12-01 21:32:1 2021-12-01 21:32:41 Default Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Apache.Expect Header.XS. Mitigated PIPS 2 • Medium 2021-12-01 21:31:1 2021-12-01 21:32:1 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MTADSWALAccess blocked Mitigated PIPS 2 • Medium 2021-12-01 21:31:1 2021-12-01 21:31:2 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion HTPasswALAccess blocked Mitigated PIPS 2 • Medium 2021-12-01 21:31:1 2021-12-01 21:31:2 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto.Web.Scanner detect. Unhandle PIPS 21 • High 2021-12-01 21:31:1 2021-12-01 21:31:2 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto.Web.Scanner detect. Unhandle PIPS 21 • High 2021-12-01 21:31:1 2021-12-01 21:32:3 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto.Web.Scanner detect. Unhandle PIPS 21 • High 2021-12-01 21:31:1 2021-12-01 21:32:3 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto.Web.Scanner detect. Unhandle PIPS 21 • High 2021-12-01 21:31:1 2021-12-01 21:32:3 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto.Web.Scanner detect. Unhandle PIPS 21 • High 2021-12-01 21:32:1 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion	Internal intrusion HTTP.Request.URI.Direct	Mitigated	IPS	2	Medium	2021-12-01 21:31:51	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature		
Internal intrusion Nikto Web.Scanner detect Unhandled       IPS       21       High       2021-12-01 21:32:11       2021-12-01 21:32:36       Default-Malicious-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion MS.IIS.bdir.HTR.Informati       Miligated       IPS       2       Medium       2021-12-01 21:32:31       2021-12-01 21:32:41       Default-Malicious-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion MS.IIS.bdir.HTR.Informati       Miligated       IPS       2       Medium       2021-12-01 21:32:41       2021-12-01 21:32:41       Default-Malicious-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion MFIP.Request.UR.IDrect       Miligated       IPS       2       Medium       2021-12-01 21:31:11       2021-12-01 21:32:21       Default-Malicious-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion MTPaswed.Access blocked       Miligated       IPS       2       Medium       2021-12-01 21:31:11       2021-12-01 21:32:12       Default-Malicious-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion Nikto.Web.Scanner detect       Unhandled       IPS       21       Medium       2021-12-01 21:31:11       2021-12-01 21:32:12       Default-Malicious-Code-Detection-By-Endpoint       Intrusion Signatu         Internal intrusion Nikto.Web.Scanner detect       Unhandled<	Internal intrusion Apache.Expect.Header.XS	Mitigated	IPS IPS	2	Medium	2021-12-01 21:31:31	2021-12-01 21:31:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature		
V1.2020.1254 (6) Internal intrusion MSJISJdir,HTR,Informati Mitigated IIPS 2 Medium 2021-12-01 21:32:31 2021-12-01 21:32:31 2021-12-01 21:32:31 2021-12-01 21:32:31 2021-12-01 21:32:31 2021-12-01 21:32:31 2021-12-01 21:32:31 2021-12-01 21:32:31 2021-12-01 21:32:31 2021-12-01 21:32:31 2021-12-01 21:32:31 2021-12-01 21:32:31 2021-12-01 21:32:31 2021-12-01 21:32:31 2021-12-01 21:31:31 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto.Web Scanner detec Unhandled IIPS 21 High 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto.Web Scanner detec Unhandled IIPS 21 High 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto.Web Scanner detec Unhandled IIPS 21 High 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion IIII Auto-IIII Auto-IIIII Auto-IIII Auto-IIII Auto-IIIII Auto-IIIII Auto-IIIIII Auto-IIIIIII Auto-IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Internal intrusion HTPasswd.Access blocked	Mitigated	IPS IPS	2	Medium	2021-12-01 21:31:11	2021-12-01 21:31:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature		
Internal intrusion MSIISbdir/HTRInformati Mitigated IIPS 2 Medium 2021-12-01 21:32:31 2021-12-01 21:32:11 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion MHTP/Request.URLDirect Mitigated IIPS 2 Medium 2021-12-01 21:31:51 2021-12-01 21:32:01 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Apache.Expect.Header.XS Mitigated IIPS 2 Medium 2021-12-01 21:31:51 2021-12-01 21:31:21 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion NIMto Web Scanner detect Unhandled IIPS 2 Medium 2021-12-01 21:31:11 2021-12-01 21:31:21 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Web Scanner detect Unhandled IIPS 21 Medium 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Web Scanner detect Unhandled IIPS 21 Medium 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Web Scanner detect Unhandled IIPS 21 Medium 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Web Scanner detect Unhandled IIPS 21 Medium 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Web Scanner detect Unhandled IIPS 21 Medium 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Web Scanner detect Unhandled IIPS 21 Medium 2021-12-01 21:31:11 2021-12-01 21:32:10 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Web Scanner detect Unhandled IIPS 21 Medium 2021-12-01 21:31:10 Coll-1-01 21:32:10 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Web Scanner detect Unhandled IIPS 21 Medium 2021-12-01 21:31:10 Coll-1-01 Coll-1-01 21:32:10 Medium 202	Internal intrusion Nikto.Web.Scanner detect	Unhandled	IPS	21	High	2021-12-01 21:31:11	2021-12-01 21:32:36	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature		
Internal intrusion PHPURICOde Injection bl., Mitjaated IPS 2 Medium 2021-12-01 21:32:11 2021-12-01 21:32:21 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Apache.Expect Header XS., Mitjaated IPS 2 Medium 2021-12-01 21:31:31 2021-12-01 21:31:41 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nitko Web Scanner detect., Unhandled IPS 2 Medium 2021-12-01 21:31:11 2021-12-01 21:31:21 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nitko Web Scanner detect., Unhandled IPS 2 Medium 2021-12-01 21:31:11 2021-12-01 21:31:20 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nitko Web Scanner detect., Unhandled IPS 21 High 2021-12-01 21:31:11 2021-12-01 21:32:36 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nitko Web Scanner detect., Unhandled IPS 21 High 2021-12-01 21:31:11 2021-12-01 21:32:36 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nitko Web Scanner detect., Unhandled IPS 21 High 2021-12-01 21:31:11 2021-12-01 21:32:36 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Intrusion Signatu Intrusion Signatu Advance Scanner detect., Unhandled IPS 21 High 2021-12-01 21:31:11 2021-12-01 21:32:36 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Intrusion Signatu Advance Scanner detect., Unhandled IPS 21 High 2021-12-01 21:31:11 2021-12-01 21:32:36 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Intrusion Signatu Advance Scanner detect. Unhandled IPS 21 High 2021-12-01 21:31:11 2021-12-01 21:32:10 Local Connector Intrusion Signatu Advance Scanner detect. Unhandled IPS 20 High 2021-12-01 21:31:11 2021-12-01 21:32:10 Local Connector Intrusion Int	×10.200.1.254 (6)										
Internal intrusion HTTP:Request_URLDirect Mitigated IPS 2 Medium 2021-12-01 21:31:51 2021-12-01 21:32:01 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Apache.Expect Header.XS Mitigated IPS 2 Medium 2021-12-01 21:31:31 2021-12-01 21:31:21 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Web Scanner detect Unhandled IPS 21 Medium 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Web Scanner detect Unhandled IPS 21 Medium 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Web Scanner detect Unhandled IPS 21 Medium 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Web Scanner detect Unhandled IPS 21 Medium 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Web Scanner detect Unhandled IPS 21 Medium 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Meb Scanner detect Unhandled IPS 21 Medium 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto Meb Scanner detect Unhandled IPS 21 Medium 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Intrus	Internal intrusion MS.IIS.bdir.HTR.Informati	Mitigated	IPS	2	Medium	2021-12-01 21:32:31	2021-12-01 21:32:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signatur		
Internal intrusion Apache.Expect.Header.XS Mitigated IPS 2 Medium 2021-12-01 21:31:31 2021-12-01 21:31:31 2021-12-01 21:31:31 2021-12-01 21:31:31 2021-12-01 21:31:31 2021-12-01 21:31:31 2021-12-01 21:31:31 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signature Internal intrusion Nikto.Web.Scanner detect Unhandled IPS 21 High 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signature Intrusion Intrusion Intrusion Signature Intrusion Intrusio	Internal intrusion PHP.URI.Code.Injection bl	Mitigated	IPS	2	Medium	2021-12-01 21:32:11	2021-12-01 21:32:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signatur		
Internal intrusion HTPasswd.Access blocked Mitigated IPS 2 Medium 2021-12-01 21:31:11 2021-12-01 21:31:21 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Internal intrusion Nikto.Web.Scanner detect Unhandled IPS 21 High 2021-12-01 21:31:11 2021-12-01 21:32:30 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signatu Intrusion Signatu Intrusion Signatu Intrusion Cet events Description Cet events Connector Action Cet Events Time Range No Data. Edit Filter @Match All Conditions OMatch Any Condition	Internal intrusion HTTP.Request.URI.Direct	Mitigated	IPS	2	Medium	2021-12-01 21:31:51	2021-12-01 21:32:01	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature		
Internal intrusion Nikto Web Scanner detect Unhandled IPS 21 High 2021-12-01 21:31:11 2021-12-01 21:32:36 Default-Malicious-Code-Detection-By-Endpoint Intrusion Signature DN_DEMAND GET_EVENTS Get vents Connector Attach Data CREATE_INCIDENT Create incident	Internal intrusion Apache.Expect.Header.XS	Mitigated	IPS	2	Medium	2021-12-01 21:31:31	2021-12-01 21:31:41	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature		
ON_DEMAND     GET_EVENTS     Get events     Description     Get events     Description     Get events     Connector     Attach Data     Connector     Connector     Connector     Connector     Connector     Connector     Connector     Time Range     No Data. Edit     Filter     OMatch All Conditions     OMatch Any Condition	Internal intrusion HTPasswd.Access blocked	Mitigated	IPS IPS	2	Medium	2021-12-01 21:31:11	2021-12-01 21:31:21	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature		
ON_DEMAND       GET_EVENTS       Description       Get events         STARTER       ATTACH_DATA_TO_INCIDENT       Connector       Connector         Attach Data       Connector       Connector         Time Range       No Data. Edit       Filter       OMatch All Conditions OMatch Any Condition	Internal intrusion Nikto.Web.Scanner detect	Unhandled	IPS	21	<ul> <li>High</li> </ul>	2021-12-01 21:31:11	2021-12-01 21:32:36	Default-Malicious-Code-Detection-By-Endpoint	Intrusion Signature		
STARTER     Attach Data     Action     Get Events       CREATE_INCIDENT Create incident     Time Range     No Data.     Edit       Filter     Match All Conditions     Match Any Condition		s				Name	Get eve	nts			
CREATE_INCIDENT Create incident Filter Match All Conditions OMatch Any Condition											
Filter   Match All Conditions  Match Any Condition			Accaen	Cata		Action	Get Eve	nts			
	CREATE_INC	IDENT				Time Range	No Data.	Edit			
, Field Match Criteria Value	Create inciden	t -				Filter	<ul> <li>Match</li> </ul>	All Conditions O Match Any Condition			
							Field	Match Criteria Va	lue		
							Se Se	everity + == + N	Medium *		
Severity • == • Medium • 4											

Event Type \*

v =

Tag Tag

\* IPS

\* Intrusion

· 十台

+ 台

- 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?

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

#### 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.

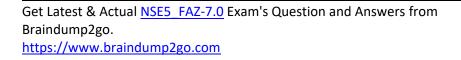
# Thank You for Trying Our Product

## 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: <a href="http://www.braindump2go.com/all-products.html">http://www.braindump2go.com/all-products.html</a>







**★** Instant Download **★** PDF And VCE **★** 100% Passing Guarantee **★** 100% Money Back Guarantee



10% Discount Coupon Code: ASTR14