



Fortinet

Exam Questions NSE6_FAZ-7.2

Fortinet NSE 6 - FortiAnalyzer 7.2 Administrator

NEW QUESTION 1

What is true about FortiAnalyzer reports?

- A. When you enable auto-cache, reports are scheduled by default.
- B. Reports can be saved in a CSV format.
- C. You require an output profile before reports are generated.
- D. The reports from one ADOM are available for all ADOMs.

Answer: C

Explanation:

For FortiAnalyzer reports, an output profile must be configured before reports can be generated and sent to an external server or system. This output profile determines how the reports are distributed, whether by email, uploaded to a server, or any other supported method. The options such as auto-cache, saving reports in CSV format, or reports availability across different ADOMs are separate features/settings and not directly related to the requirement of having an output profile for report generation.

NEW QUESTION 2

Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate on FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

- A. LDAP servers IP addresses added as trusted hosts
- B. One or more remote LDAP servers
- C. A local wildcard administrator account
- D. An administrator group

Answer: BD

Explanation:

To allow non-local administrators to authenticate on FortiAnalyzer with any user account in a single LDAP group, you must configure one or more remote LDAP servers and an administrator group. First, you configure the LDAP server(s) by specifying the server name, IP, and other details such as the Common Name Identifier and Distinguished Name. Then, you add the LDAP server to a user group. Finally, you create an administrator account that uses this user group for authentication, allowing any user from the specified LDAP group to authenticate. References: FortiAnalyzer 7.2 Administrator Guide, "Configuring remote authentication for administrators using LDAP" section.

NEW QUESTION 3

What is true about a FortiAnalyzer Fabric?

- A. Supervisors support HA.
- B. Members events can be raised from the supervisor.
- C. The supervisor and members cannot be in different time zones
- D. The members send their logs to the supervisor.

Answer: D

Explanation:

In a FortiAnalyzer Fabric, the FortiAnalyzer can recognize a Security Fabric group of devices, and it supports the Security Fabric by storing and analyzing logs from these units as if they were from a single device. The members of the Security Fabric group send their logs to the FortiAnalyzer, which acts as a supervisor for log storage and analysis, providing a centralized point of visibility and control over the logs. References: FortiAnalyzer 7.4.1 Administration Guide, "Security Fabric" section.

NEW QUESTION 4

Which two parameters impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

- A. Disk size
- B. Total quota
- C. RAID level
- D. License type

Answer: AC

Explanation:

The amount of reserved disk space required by FortiAnalyzer is influenced by the disk size and the RAID level. The system reserves a portion of the disk space for system use and unexpected quota overflow, with the rest available for device allocation. The RAID level determines the disk size and the reserved disk quota level, with different RAID configurations leading to variations in the reserved space. References: FortiAnalyzer 7.2 Administrator Guide, "Disk Space Allocation" and "RAID Level Impact" sections.

NEW QUESTION 5

In a Fortinet Security Fabric, what can make an upstream FortiGate create traffic logs associated with sessions initiated on downstream FortiGate devices?

- A. The traffic destination is another FortiGate in the fabric.
- B. Log redundancy is configured in the fabric.
- C. The upstream FortiGate is configured to do NAT.
- D. The downstream device cannot connect to FortiAnalyzer.

Answer: D

Explanation:

In a Fortinet Security Fabric, an upstream FortiGate may create traffic logs for sessions initiated on downstream FortiGate devices if the downstream device is unable to connect to FortiAnalyzer. This allows for continuity of logging and ensures that session logs are captured and stored even if the downstream device loses its connection to the log management system. References: FortiAnalyzer 7.4.1 Administration Guide, "Fortinet Security Fabric" section.

NEW QUESTION 6

Which feature can you configure to add redundancy to FortiAnalyzer?

- A. Primary and secondary DNS
- B. VLAN interfaces
- C. IPv6 administrative access
- D. Link aggregation

Answer: D

Explanation:

Link aggregation is a method used to combine multiple network connections in parallel to increase throughput and provide redundancy in case one of the links fail. This feature is used in network appliances, including FortiAnalyzer, to add redundancy to the network connections, ensuring that there is a backup path for traffic if the primary path becomes unavailable. References: The FortiAnalyzer 7.4.1 Administration Guide explains the concept of link aggregation and its relevance to

NEW QUESTION 7

Refer to the exhibit.

Wireshark · Packet 5 · sniffer_port3.1 (1).pcap

```

> Frame 5: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits)
> Ethernet II, Src: MS-NLB-PhysServer-09_of:00:01:06 (02:09:0f:00:01:06),
> Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210
> User Datagram Protocol, Src Port: 8678, Dst Port: 514
  [truncated] Syslog message: (unknown):  \001\020\020\004\000\001\0
  > Message:  \001\020\020\004
  
```

0000	02 09 0f 00 02 06 02 09 0f 00 01 06 08 00 45 00 E-
0010	01 4b bb b3 00 00 3f 11 a4 8c 0a c8 03 01 0a c8	-K....?.....
0020	01 d2 21 e6 02 02 01 37 81 ea ec cf 20 60 01 10	..!....7....
0030	10 04 00 01 00 f7 00 fe 63 a1 53 9a 46 47 56 4d c·S·FGVM
0040	30 31 30 30 30 30 36 35 30 33 36 52 65 6d 6f	01000006 5036Remo
0050	74 65 2d 46 6f 72 74 69 47 61 74 65 72 6f 6f 74	te-Forti Gateroot
0060	00 fe f1 14 64 61 74 65 3d 32 30 32 32 2d 31 32date =2022-12
0070	2d 31 39 20 74 69 6d 65 3d 32 32 3a 31 38 3a 30	-19 time =22:18:0
0080	32 20 65 76 65 6e 74 13 00 f1 29 31 36 37 31 35	2 event- ..)16715
0090	31 37 30 38 32 34 34 35 33 36 31 38 38 31 20 74	17082445 361881 t
00a0	7a 3d 22 2d 30 38 30 30 22 20 6c 6f 67 69 64 3d	r="-0800 " logid=
00b0	22 30 31 30 30 30 32 30 30 31 34 22 20 74 79 70	"0100020 014" typ
00c0	65 3d 22 42 00 52 22 20 73 75 62 10 00 f1 11 73	e="B·R" sub...s
00d0	79 73 74 65 6d 22 20 6c 65 76 65 6c 3d 22 77 61	ystem" l evel="wa
00e0	72 6e 69 6e 67 22 20 76 64 3d 22 72 6f 6f 74 4b	rning" v d="rootK
00f0	00 f0 12 64 65 73 63 3d 22 54 65 73 74 22 20 75	...desc= "Test" u
0100	73 65 72 3d 22 61 64 6d 69 6e 22 20 61 63 74 69	ser="adm in" acti
0110	6f 6e 3d 22 6f 00 f0 0a 6e 22 20 73 74 61 74 75	on="o... n" statu
0120	73 3d 22 73 75 63 63 65 73 73 22 20 6d 73 67 3d	s="succe ss" msg=
0130	22 32 00 11 20 31 00 00 97 00 f0 0e 67 65 64 20	"2.. 1.. ...ged
0140	69 6e 74 6f 20 74 68 65 20 66 77 20 2d 20 31 36	into the fw - 16
0150	37 31 35 31 37 30 38 32 22	71517082 "

Which image corresponds to the packet capture shown in the exhibit?

A)

Device Name	Platform	Logs	Average Log Rate(Logs/Sec)
Remote-FortiGate	FortiGate-VM64	Real Time	0

B)

Device Name	Platform	Logs	Average Log Rate(Logs/Sec)
Remote-FortiGate	FortiGate-VM64	Real Time	0

C)

Device Name	Platform	Logs	Average Log Rate(Logs/Sec)
Remote-FortiGate	FortiGate-VM64	Real Time	0

- A. Option A
- B. Option B
- C. Option A

Answer: D

Explanation:

The exhibit shows a packet capture with a syslog message containing a log event from a FortiGate device. This log event includes several details such as the date, time, and event message. The corresponding image that matches this packet capture would be the one which shows that the FortiGate device has logs being received in real-time, as indicated by the highlighted section in the packet capture where it mentions "real-time". Therefore, Option A is the correct answer because it shows logs with "Real Time" status for the FortiGate-VM64 device, indicating that this FortiAnalyzer is currently receiving real-time logs from the device, matching the activity in the packet capture.

Reference: Based on the provided exhibits and the real-time logging information, correlated with the knowledge from the FortiAnalyzer 7.2 Administrator documentation regarding log reception and device management.

NEW QUESTION 10

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE6_FAZ-7.2 Practice Exam Features:

- * NSE6_FAZ-7.2 Questions and Answers Updated Frequently
- * NSE6_FAZ-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE6_FAZ-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE6_FAZ-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE6_FAZ-7.2 Practice Test Here](#)