

Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator

https://www.2passeasy.com/dumps/FCP_FAZ_AD-7.4/



NEW QUESTION 1

An administrator has moved a FortiGate device from the root ADOM to ADOM1. Which two statements are true regarding logs? (Choose two.)

- A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.
- B. Archived logs will be moved to ADOM1 from the root ADOM automatically.
- C. Logs will be present in both ADOMs immediately after the move.
- D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the database.

Answer: AD

Explanation:

When a device is moved from one ADOM to another, analytics logs can be moved automatically, but you may need to rebuild the database for the logs to be fully transferred and usable in the new ADOM. Archived logs, however, do not move automatically between ADOMs.

NEW QUESTION 2

Which process is responsible for enforcing the log file size?

- A. oftpd
- B. miglogd
- C. sqlplugind
- D. logfiled

Answer: D

Explanation:

The logfiled process is responsible for enforcing log file size and managing log rotation on FortiAnalyzer. It ensures that log files do not exceed the configured size limits and handles the creation and rotation of new log files when necessary.

NEW QUESTION 3

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

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

Answer: C

Explanation:

RAID level affects how much disk space is reserved for redundancy and fault tolerance. For example, RAID 1 mirrors data, meaning you need more space for redundancy, while RAID 5 or RAID 6 reserves space for parity.

Disk size directly influences the total available and reserved space since the larger the disk, the more space may need to be reserved for system functions, logs, and other operations.

The total quota and license type do not directly impact the reserved disk space, though they do influence other aspects of capacity and functionality.

NEW QUESTION 4

Refer to the exhibit, which shows the HA configuration settings of a FortiAnalyzer device.

FortiAnalyzer HA cluster settings

Cluster Settings

Operation Mode

Standalone

Active-Passive

Active-Active

Preferred Role

Secondary

Primary

Cluster Virtual IP

IP Address and Interface

IP Address

Interface

Action

192.168.101.222

port1

✕

+

Cluster Settings

Peer IP and Peer SN

Peer IP

Peer SN

Action

10.0.1.210

FAZ-VM0000065040

✕

+

Group Name

Training

Group ID

1

(1-255)

Password

••••••••

🔑

Heart Beat Interval

10

Seconds

Heart Beat Interface

port1

▼

Failover Threshold

30

Priority

120

(80-120)

Log Data Sync

🔵

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

- A. After joining the cluster, this FortiAnalyzer will forward received logs to its peers.
- B. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
- C. This FortiAnalyzer is configured to route HA traffic through a gateway.
- D. This FortiAnalyzer will join the existing HA cluster as the secondary.

Answer: B

Explanation:

The "Preferred Role" is set to Secondary, which means this FortiAnalyzer is configured to join the cluster as the secondary unit in an Active-Passive HA configuration. Other settings, such as the peer IP and serial number, confirm its setup to communicate with the primary unit.

NEW QUESTION 5

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

- A. When in collector mode, FortiAnalyzer offloads the log receiving task to the analyzer.
- B. When in analyzer mode, FortiAnalyzer supports event management and reporting features.
- C. For the collector, you should allocate most of the disk space to analytics logs.
- D. Analyzer mode is the default operating mode.

Answer: B

Explanation:

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

In analyzer mode, FortiAnalyzer provides full support for log analysis, event management, and reporting capabilities.

Analyzer mode is the default operating mode.

By default, FortiAnalyzer operates in analyzer mode, which allows for log analysis and reporting. The other options are incorrect because:

In collector mode, the FortiAnalyzer primarily stores logs and forwards them to another FortiAnalyzer in analyzer mode, not the other way around.

In collector mode, most disk space is usually allocated to storage rather than analytics, as the logs are primarily stored for forwarding.

NEW QUESTION 6

What is the purpose of the FortiAnalyzer command diagnose system print netstat?

- A. It provides network statistics for active connections, including the protocols, IP addresses, and connection states.
- B. It provides the complete routing table, including directly connected routes.
- C. It provides the static DNS table, including the host names and their expiration timers.

- D. It provides NTP server information, including server IP
E. stratum, poll time, and latency.

Answer: A

Explanation:

The diagnose system print netstat command in FortiAnalyzer provides detailed information on active network connections, similar to the netstat command found in many operating systems.

NEW QUESTION 7

Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark

Wireshark - Packet 34 - sniffer_port3.1.pcap

> Frame 34: 624 bytes on wire (4992 bits), 624 bytes captured (4992 bits)
> Ethernet II, Src: MS-NLB-PhysServer-09_0f:00:01:06 (02:09:0f:00:01:06), Dst: MS-NLB-PhysServer-09_0f:00:01:06 (02:09:0f:00:01:06)
> Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210
> Transmission Control Protocol, Src Port: 18052, Dst Port: 514, Seq: 14443, Ack: 130, Len: 570
v Remote Shell
Client -> Server Data [truncated]: 1703030235120db2f7eaa29995a08617e996a1e7e5a02afe2f81e0320715cff2d8c

0000 02 09 0f 00 02 07 02 09 0f 00 01 06 08 00 45 00E.
0010 02 62 f8 7b 00 00 3f 06 66 b8 0a c8 03 01 0a c8 -b-{-? f.....
0020 01 d2 46 84 02 02 99 02 43 a6 c2 b9 04 82 50 18 --F-----C---P.
0030 39 08 1c f3 00 00 17 03 03 02 35 12 0d b2 f7 ea 9-----5-----
0040 a2 99 95 a0 86 17 e9 96 a1 e7 e5 a0 2a fe 2f 81*/.
0050 e0 32 07 15 cf f2 d8 c7 41 47 04 f9 52 46 82 0a -2-----AG--RF--
0060 27 69 5d bc 93 7f 18 c5 95 18 fa ea ed 6d aa 94 'i]-----m--
0070 84 1f 4e 54 c2 b6 58 e9 06 d8 c5 2a 0d 7b b8 75 --NT--X- --*-{u
0080 b3 6f 13 1d 63 1d af fe ab c7 21 22 9d 2b 37 e6 -o-c- -!"-+7-
0090 f7 b5 6b d0 26 45 4a a1 0e 27 60 fa 89 f0 d0 ba -k-&EJ- -''-----
00a0 6a 22 e3 6f eb 9a bd fe 0c e6 8f e3 5f 45 65 c2 j"-o-----_Ee-
00b0 ef dc b9 83 34 16 7d 52 73 83 3a ca 2e aa 3a 75 ----4-}R s:-:u
00c0 1b 80 22 06 f9 d8 22 1c 95 b3 c3 0d 9e 4f 53 33 --"---"-----OS3
00d0 85 fd 7e ce 96 e5 96 7e 66 a2 17 ea bf 5b 9f b2 --~---~ f---[

No.: 34 - Time: 11.315345 - Source: 10.200.3.1 - Destination: 10.200.1.210 - Protocol: RSH - Length: 624 - Info: Client -> Server data

☒ Show packet bytes

Close Help

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

A)

		Table View v	More v	Show Charts v	Search...
<input type="checkbox"/>	Device Name	IP Address	Connectivity	Logging Mode	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-FortiGate	10.200.3.1	Connection Up	Real Time	0

B)

		Table View v	More v	Show Charts v	Search...
<input type="checkbox"/>	Device Name	IP Address	Connectivity	Logging Mode	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-FortiGate	10.200.3.1	Connection Up	Real Time	0

C)

					Search...
<input type="checkbox"/>	Device Name	IP Address	Connectivity	Logging Mode	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-FortiGate	10.200.3.1	Connection Down	Real Time	0

D)

					Search...
<input type="checkbox"/>	Device Name	IP Address	Connectivity	Logging Mode	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-FortiGate	10.200.3.1	Connection Down	Real Time	0

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Chosen image shows the device Remote-FortiGate with the IP 10.200.3.1 and a connection status of "Connection Up," which is consistent with the packet capture details showing active communication between the client and server.

NEW QUESTION 8

Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
131	9.114194	10.0.1.200	10.0.1.210	Syslog	1003	22486	514	@\000\020\017\003\006eJ\004FGVM010000064692Local-FortiGateroot\002\0025\
132	9.114245	10.0.1.200	10.0.1.210	Syslog	1115	22486	514	@\020\020\017\003\0aBeJ\004FGVM010000064692Local-FortiGateroot\002\0025\
133	9.114311	10.0.1.200	10.0.1.210	Syslog	1135	22486	514	@\002\020\017\004\b\b\reJ\004FGVM010000064692Local-FortiGateroot\002\0025\
134	10.0013...	10.0.1.200	10.0.1.210	Syslog	871	7262	514	\$@\000\020\004\002\0tJeJ\000FGVM010000077646ISFWroot\001\001\002\017\00
135	11.1086...	10.0.1.200	10.0.1.210	Syslog	872	22486	514	\$@\000\020\017\003\001\004JeJ\004FGVM010000064692Local-FortiGateroot\002\0025\
142	15.0058...	10.0.1.200	10.0.1.210	Syslog	572	7262	514	\$@\000\020\004\001\003JeJ\006FGVM010000077646ISFWroot\001\001\000\000\
143	16.1088...	10.0.1.200	10.0.1.210	Syslog	555	22486	514	\$@\000\020\017\001\002\017eJ\bFGVM010000064692Local-FortiGateroot\002\017\
150	20.0103...	10.0.1.200	10.0.1.210	Syslog	639	7262	514	\$@\000\020\004\002\033\0aJeJ\nFGVM010000077646ISFWroot\001\001\001\001\
151	20.0574...	10.0.1.200	10.0.1.210	Syslog	332	7262	514	@\001\020\004\000\000JeJ\017FGVM010000077646ISFWroot\000\000\024date=2024
152	20.0575...	10.0.1.200	10.0.1.210	Syslog	907	7262	514	@\000\020\004\003\0a\032eJ\017FGVM010000077646ISFWroot\003\003\002\024date
153	20.0576...	10.0.1.200	10.0.1.210	Syslog	1025	7262	514	@\000\020\004\003\006&eJ\017FGVM010000077646ISFWroot\003\002\002\024date
154	20.0576...	10.0.1.200	10.0.1.210	Syslog	648	7262	514	@\000\020\004\002\005\004eJ\017FGVM010000077646ISFWroot\002\002\002\024date
155	20.0577...	10.0.1.200	10.0.1.210	Syslog	317	7262	514	@\001\020\004\000\000JeJ\017FGVM010000077646ISFWroot\000\000\024date=2024
156	20.0577...	10.0.1.200	10.0.1.210	Syslog	555	7262	514	@\b\020\004\001\002\003eJ\017FGVM010000077646ISFWroot\002\003\002\024date=20

Frame 131: 1003 bytes on wire (8024 bits), 1003 bytes captured (8024 bits)
 Ethernet II, Src: Fortinet_09:01:00 (00:09:0f:09:01:00), Dst: VMware_a9:73:0f (00:0c:29:a9:73:0f)
 Internet Protocol Version 4, Src: 10.0.1.200, Dst: 10.0.1.210
 User Datagram Protocol, Src Port: 22486, Dst Port: 514
 Source Port: 22486
 Destination Port: 514
 Length: 969

0000	00 0c 29 a9 73 0f 00 09 0f 09 01 00 08 00 45 00	..).s... ..E.
0010	03 dd fe 51 00 00 40 11 61 25 0a 00 01 c8 0a 00	...Q. @ a%.....
0020	01 d2 57 d6 02 02 03 c9 a1 55 ec cf 20 40 00 10	..W.....U. @..
0030	0f 04 00 03 03 86 06 f0 65 c1 4a 04 46 47 56 4de-J-FGVM
0040	30 31 30 30 30 30 36 34 36 39 32 4c 6f 63 61	01000006 4692Loca
0050	6c 2d 46 6f 72 74 69 47 61 74 65 72 6f 6f 74 02	l-FortiG ateroot-
0060	92 02 2f 02 2f f2 14 64 61 74 65 3d 32 30 32 34	..-/-..d ate=2024
0070	2d 30 32 2d 30 35 20 74 69 6d 65 3d 31 32 3a 35	-02-05 t ime=12:5
0080	30 3a 31 32 20 65 76 65 6e 74 13 00 f3 17 37 30	0:12 eve nt....70

The capture displayed was taken on a FortiAnalyzer.

Why is a single IP address shown as the source for all logs received?

- A. FortiAnalyzer is using the device MAC addresses to differentiate their logs.
 B. The logs belong to devices that are part of a high availability (HA) cluster.
 C. FortiAnalyzer is receiving logs from the root FortiGate of a Security Fabric.
 D. The device sending logs has two VDOMs in the same ADOM.

Answer: C

Explanation:

In a Fortinet Security Fabric, logs from downstream devices can be sent to FortiAnalyzer through the root FortiGate. This is why all the logs have the same source IP address (the root FortiGate). The root FortiGate aggregates and forwards the logs from all downstream devices, so the source IP in the log capture will appear to be from the root FortiGate itself, even though the logs originate from multiple devices within the fabric.

NEW QUESTION 9

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

Answer: B

Explanation:

When the upstream FortiGate is performing Network Address Translation (NAT), it creates new session entries for traffic passing through it. As a result, it generates its own traffic logs for those sessions, even if the sessions were initiated on a downstream FortiGate. This is because the upstream FortiGate is altering the source IP address, making it responsible for tracking the session details.

NEW QUESTION 10

Refer to the exhibit.

Create New Administrator

User Name

Remote-Admin

Avatar

R

+ Add Photo

- Remove Photo

Description

Admin Type

LDAP

LDAP Server

External_Server

Match all users on remote server

☐

New Password

.....

ⓧ

👁

!

Confirm Password

.....

ⓧ

👁

!

FortiToken Cloud

Disable

FortiToken Mobile

Email

SMS

Administrative Domain

All ADOMs

All ADOMs except specified ones

Specify

Admin Profile

Restricted_User

The exhibit shows the creation of a new administrator on FortiAnalyzer. The new account uses the credentials stored on an LDAP server. Why would an administrator configure a password for this account?

- A. This password is used if the authentication server becomes unreachable.
- B. This password authenticates FortiAnalyzer against the LDAP server.
- C. This password is set to comply with FortiAnalyzer password policy
- D. This password is required because this is a restricted user.

Answer: A

Explanation:

When using LDAP for authentication, a password can be set locally on FortiAnalyzer as a fallback option in case the LDAP server becomes unreachable. This ensures that the administrator can still log in if there are issues with the LDAP server.

NEW QUESTION 10

View the exhibit:

Data Policy

Keep Logs for Analytics

60

Days

Keep Logs for Archive

365

Days

Disk Utilization

Maximum Allowed

1000

MB

Analytics: Archive

70%

30%

Alert and Delete When Usage Reaches

90%

Out of Available: 62.8 GB

☐ Modify

What does the 1000MB maximum for disk utilization refer to?

- A. The disk quota for the FortiAnalyzer model
- B. The disk quota for all devices in the ADOM
- C. The disk quota for each device in the ADOM
- D. The disk quota for the ADOM type

Answer: B

Explanation:

The 1000MB maximum for disk utilization refers to the total disk quota allocated for storing logs from all devices within the specific ADOM (Autonomous Domain) you're configuring.

NEW QUESTION 14

What is the purpose of employing RAID with FortiAnalyzer?

- A. To introduce redundancy to your log data
- B. To provide data separation between ADOMs
- C. To separate analytical and archive data
- D. To back up your logs

Answer: A

Explanation:

RAID (Redundant Array of Independent Disks) is used in FortiAnalyzer primarily to provide data redundancy and ensure data integrity. Here,s how it relates to each option:

To Introduce Redundancy to Your Log Data (Option A):

The main purpose of employing RAID in FortiAnalyzer is to add redundancy to the storage system. By using RAID configurations (such as RAID 1, RAID 5, or RAID 6), data is replicated across multiple disks, which helps in protecting against disk failures and ensures that log data is not lost if a disk fails. This redundancy enhances the reliability and availability of the log data.

NEW QUESTION 18

It is a best practice to upload FortiAnalyzer local logs to a remote server.Which two remote servers are supported for the upload? (Choose two.)

- A. FTP
- B. SFTP
- C. UDP
- D. TFTP

Answer: AB

Explanation:

When it's considered a best practice to upload FortiAnalyzer local logs to a remote server, the following two remote server protocols are commonly supported: These protocols provide secure and reliable ways to transfer logs and data to remote servers for storage and analysis while maintaining data integrity and confidentiality.

NEW QUESTION 23

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FAZ_AD-7.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FAZ_AD-7.4 Product From:

https://www.2passeasy.com/dumps/FCP_FAZ_AD-7.4/

Money Back Guarantee

FCP_FAZ_AD-7.4 Practice Exam Features:

- * FCP_FAZ_AD-7.4 Questions and Answers Updated Frequently
- * FCP_FAZ_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FAZ_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCP_FAZ_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year