

Free Questions for FCP_FAZ_AD-7.4

Shared by Hampton on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which process is responsible for enforcing the log file size?

Options:

- 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.

Question 2

Question Type: MultipleChoice

What does the disk status Degraded mean for RAID management?

Options:

- A- The hard drive is no longer being used by the RAID controller.
- B- One or more drives are missing from the FortiAnalyzer unit.
- C- The device is writing data to the disk to restore the volume to an optimal state.
- D- FortiAnalyzer determined that the parity data in the disk is not valid.

Answer:

B

Explanation:

When the RAID status is Degraded, it typically indicates that one or more drives in the RAID array have failed or are missing, causing the RAID array to operate with reduced redundancy. In this state, the array is still functioning, but it's at risk because the fault tolerance provided by RAID is compromised.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark

sniffer_port1.1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.dstport == 514

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\004
132	9.114245	10.0.1.200	10.0.1.210	Syslog	1115	22486	514	@\020\020\017\003\0aBeJ\004FGV
133	9.114311	10.0.1.200	10.0.1.210	Syslog	1135	22486	514	@\002\020\017\004\b\b\reJ\004F
134	10.0013...	10.0.1.200	10.0.1.210	Syslog	871	7262	514	\$_\000\020\004\002\0t\0eJ\000FG
135	11.1086...	10.0.1.200	10.0.1.210	Syslog	872	22486	514	\$_\000\020\017\003\001\004eJ\0
142	15.0058...	10.0.1.200	10.0.1.210	Syslog	572	7262	514	\$_\000\020\004\001\003eJ\006
143	16.1088...	10.0.1.200	10.0.1.210	Syslog	555	22486	514	\$_\000\020\017\001\002\017eJ\b
150	20.0103...	10.0.1.200	10.0.1.210	Syslog	639	7262	514	\$_\000\020\004\002\033\0a\0eJ\nF
151	20.0574...	10.0.1.200	10.0.1.210	Syslog	332	7262	514	@\001\020\004\000\000eJ\017
152	20.0575...	10.0.1.200	10.0.1.210	Syslog	907	7262	514	@\000\020\004\0033\0a\032eJ\017
153	20.0576...	10.0.1.200	10.0.1.210	Syslog	1025	7262	514	@\000\020\004\003\006&eJ\017F
154	20.0576...	10.0.1.200	10.0.1.210	Syslog	648	7262	514	@\000\020\004\0020\005\004eJ\0
155	20.0577...	10.0.1.200	10.0.1.210	Syslog	317	7262	514	@\001\020\004\000\000eJ\017
156	20.0577...	10.0.1.200	10.0.1.210	Syslog	555	7262	514	@\b\020\004\001\002\003eJ\017

> 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 02 c0 c1 55 ee ef 20 40 00 10 ...M...H...0...

The capture displayed was taken on a FortiAnalyzer.

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

Options:

- 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.

Question 4

Question Type: MultipleChoice

Which two statements about deleting ADOMs are true? (Choose two.)

Options:

- A- Logs must be purged or migrated before you can delete an ADOM.
- B- ADOMs with registered devices cannot be deleted.
- C- Default ADOMs cannot be deleted.
- D- The status of the ADOMs must be unlocked.

Answer:

B

Explanation:

DOMs with registered devices cannot be deleted.

An ADOM cannot be deleted if it has registered devices. You must first remove or deregister the devices before deleting the ADOM.

The status of the ADOMs must be unlocked.

An ADOM must be in an unlocked state before it can be deleted. If the ADOM is locked, it will not allow deletion.

Question 5

Question Type: MultipleChoice

Which two statements about high availability (HA) on FortiAnalyzer are true? (Choose two.)

Options:

- A-** FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
- B-** FortiAnalyzer HA active-passive mode can function without VRRP.
- C-** All devices in a FortiAnalyzer HA cluster must run in the same operation mode, either analyzer mode or collector mode.
- D-** All devices in a FortiAnalyzer HA cluster must have the same available disk space.

Answer:

A

Explanation:

The two correct statements about high availability (HA) on FortiAnalyzer are:

FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.

FortiAnalyzer HA synchronizes both logs and certain system configuration settings between the units in the cluster to ensure consistent operation.

All devices in a FortiAnalyzer HA cluster must run in the same operation mode, either analyzer mode or collector mode.

In an HA cluster, all devices must be configured to operate in the same mode --- either analyzer mode or collector mode---to ensure consistency and proper functionality across the cluster.

The other options, such as VRRP, are not required for HA in FortiAnalyzer, and disk space can vary between nodes but may impact log storage capacity.

Question 6

Question Type: MultipleChoice

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

Options:

- 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.

Question 7

Question Type: MultipleChoice

Refer to the exhibit.

Create New Administrator	
User Name	Remote-Admin
Avatar	R <input type="button" value="+ Add Photo"/> <input type="button" value="- Remove Photo"/>
Description	
Admin Type	LDAP <input type="button" value="v"/>
LDAP Server	External_Server <input type="button" value="v"/>
Match all users on remote server	<input type="checkbox"/>
New Password <input type="button" value="x"/> <input type="button" value="eye"/> <input type="button" value="i"/>
Confirm Password <input type="button" value="x"/> <input type="button" value="eye"/> <input type="button" value="i"/>
FortiToken Cloud	<input type="button" value="Disable"/> <input type="button" value="FortiToken Mobile"/> <input type="button" value="Email"/> <input type="button" value="SMS"/>
Administrative Domain	<input type="button" value="All ADOMs"/> <input type="button" value="All ADOMs except specified ones"/> <input type="button" value="Specify"/>
Admin Profile	Restricted_User <input type="button" value="v"/>

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?

Options:

- 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.

Question 8

Question Type: MultipleChoice

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

Options:

- 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.

To Get Premium Files for FCP_FAZ_AD-7.4 Visit

https://www.p2pexams.com/products/fcp_faz_ad-7.4

For More Free Questions Visit

<https://www.p2pexams.com/fortinet/pdf/fcp-faz-ad-7.4>

