



Fortinet

Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator

NEW QUESTION 1

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 2

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 3

Refer to the exhibit.

```
FortiGate # diagnose test application fgtlogd 4
Queues in all miglogds: cur:31 total-so-far:4642589
global log dev statistics:
faz=180191781, faz_cloud=0, fds_log=0
faz 0: sent=180189698, failed=4507, cached=0, dropped=0
```

Based on the output, what can you conclude about the FortiAnalyzer logging status?

- A. The connection between FortiGate and FortiAnalyzer is overloaded.
- B. FortiGate has logs to send, but FortiAnalyzer is unavailable.
- C. FortiGate is configured to send logs in batches.
- D. FortiGate is sending logs again after it performed a reboot.

Answer: B

Explanation:

The output shows that FortiGate has sent a large number of logs (sent=180189698), but some logs have failed to be sent (failed=4507). This suggests that FortiAnalyzer was temporarily unavailable or had an issue receiving logs, leading to the failure count. There are no logs cached or dropped, indicating FortiGate is still attempting to send logs but with some failures.

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	<div>✕</div> <div>+</div>

Cluster Settings

Peer IP and Peer SN

Peer IP	Peer SN	Action
10.0.1.210	FAZ-VM0000065040	<div>✕</div> <div>+</div>

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

You are trying to initiate an authorization request from FortiGate to FortiAnalyzer, but the Security Fabric window does not open when you click Authorize. Which two reasons can cause this to happen? (Choose two.)

- A. A pre-shared key needs to be established on both sides.
- B. The management computer does not have connectivity to the authorization IP address and port combination.
- C. The Security Fabric root is unauthorized and needs to be added as a trusted host.
- D. The fabric authorization settings on FortiAnalyzer are misconfigured.

Answer: BD

Explanation:

The management computer does not have connectivity to the authorization IP address and port combination.

If there is no network connectivity between the management computer and the FortiAnalyzer on the specific IP address and port used for authorization, the Security Fabric window will not open.

The fabric authorization settings on FortiAnalyzer are misconfigured.

If the fabric authorization settings on FortiAnalyzer are not properly configured, FortiGate will not be able to initiate the authorization request, preventing the Security Fabric window from opening.

The other options are not applicable because:

Pre-shared keys are not required for initial authorization between FortiGate and FortiAnalyzer; they are typically used for establishing VPN tunnels.

The Security Fabric root does not need to be added as a trusted host to open the authorization window. Trusted hosts are more relevant to FortiGate's access control for management interfaces.

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

The connection status of a new device on FortiAnalyzer is listed as Unauthorized. What does that status mean?

- A. It is a device whose registration has not yet been accepted in FortiAnalvzer.
- B. It is a device that has not yet been assigned an ADOM.
- C. It is a device that is waiting for you to configure a pre-shared key.
- D. It is a device that FortiAnalvzer does not support.

Answer: A

Explanation:

The "Unauthorized" status indicates that the device has been discovered or attempted to connect but has not yet been authorized for management by FortiAnalyzer. It requires an administrator to approve or authorize the device before it can be fully managed.

NEW QUESTION 8

Refer to the exhibit.

Cluster Settings

Operation Mode

StandaloneHigh Availability

Preferred Role

SecondaryPrimary

Cluster Virtual IP

IP Address and Interface

IP Address

Interface

192.168.101.222

port1

+

Cluster Settings

Peer IP and Peer SN

Peer IP

Peer SN

10.0.1.210

FAZ-VM0000065040

+

Group Name

NSE6

Group ID

1

(1-255)

Password

.....

🔑

Heart Beat Interval

10

Seconds

Failover Threshold

30

Prio

120

🔍

The image displays "he configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster.

What can you conclude from the configuration displayed?

- A. After joining to the cluster, this FortiAnalyzer will keep an updated log database.
- B. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
- C. This FortiAnalyzer will join to the existing HA cluster as the primary.
- D. This FortiAnalyzer is configured to receive logs in its port1.

Answer: A

Explanation:

Operation Mode: The mode is set to "High Availability" which indicates that this FortiAnalyzer is intended to be part of an HA cluster.

Preferred Role: The "Primary" role is selected, meaning this device is configured to act as the primary unit in the HA cluster. This is a crucial setting as it determines the device's behavior and responsibilities within the cluster.

Cluster Virtual IP: A specific IP address (192.168.101.222) is assigned to be used by devices in the network to communicate with the cluster. This Virtual IP will be shared between the units in the cluster.

Cluster Settings: These include configurations for heartbeat interval, failover threshold, and priority which are crucial for maintaining cluster health and managing failover scenarios.

Given these points, the correct conclusion from the options provided is:

* C. This FortiAnalyzer will join the existing HA cluster as the primary.

NEW QUESTION 9

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.

Reference: The FortiAnalyzer 7.4.1 Administration Guide explains the concept of link aggregation and its relevance to

NEW QUESTION 10

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

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

Answer: AD

Explanation:

Both modes, forwarding and aggregation, support encryption of logs between devices.

Both forwarding and aggregation modes can use encryption to securely transfer logs between FortiAnalyzer devices.

Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.

In aggregation mode, logs are stored and then transferred to another FortiAnalyzer at a scheduled time, rather than in real-time. This mode is typically used when consolidating logs from multiple devices into a central FortiAnalyzer.

The other options are incorrect because:

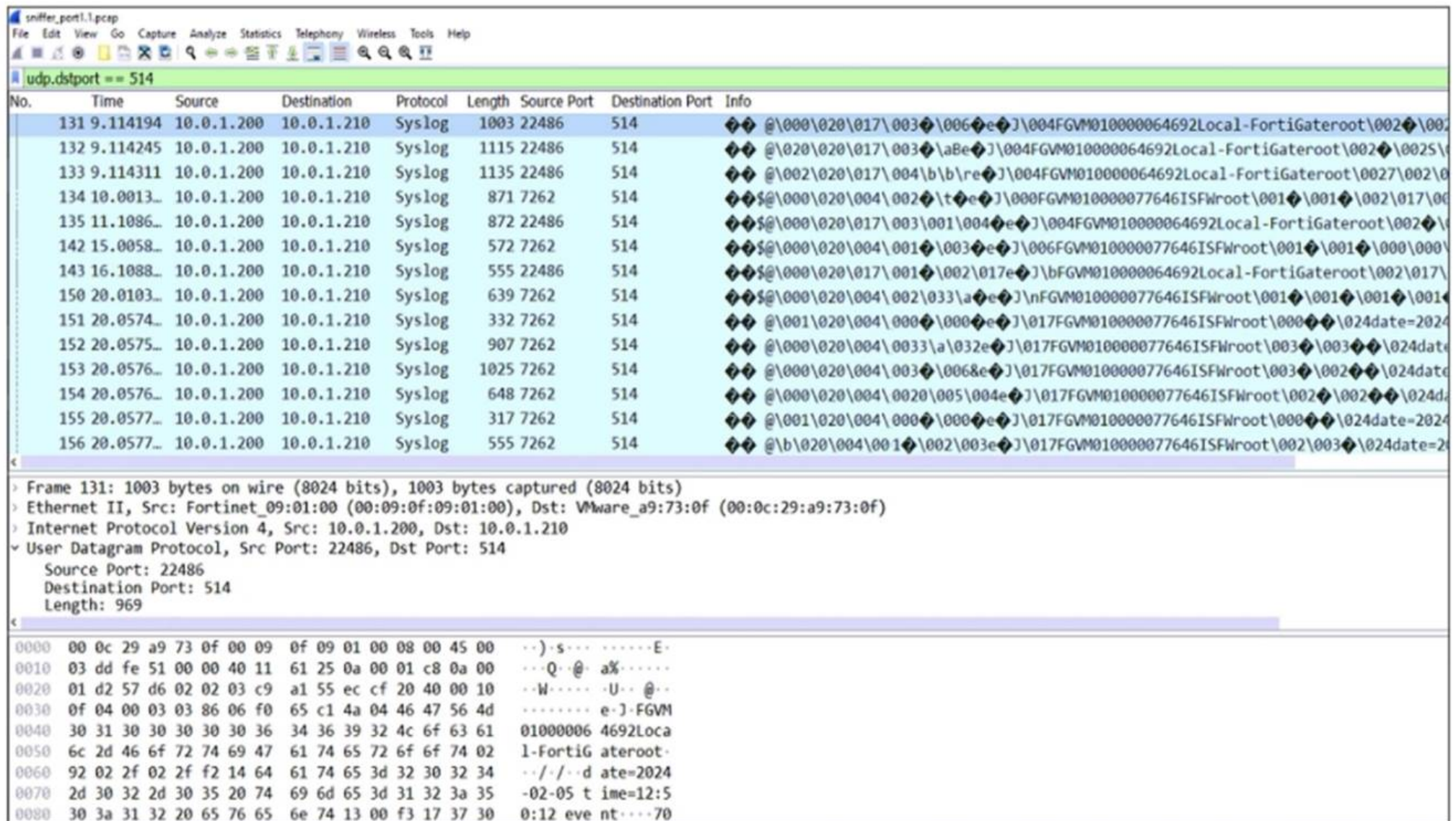
Forwarding mode sends logs in real-time but not exclusively to other FortiAnalyzer devices; it can also send logs to external systems like syslog servers.

Aggregation mode is primarily for consolidating logs to another FortiAnalyzer and doesn't focus on forwarding logs to syslog or CEF servers.

NEW QUESTION 10

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\0027\002\0
134	10.0013...	10.0.1.200	10.0.1.210	Syslog	871	7262	514	@\000\020\004\002\t\teJ\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\004\teJ\004FGVM010000064692Local-FortiGateroot\002\0
142	15.0058...	10.0.1.200	10.0.1.210	Syslog	572	7262	514	@\000\020\004\001\003\teJ\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\aeJ\nFGVM010000077646ISFWroot\001\001\001\001\
151	20.0574...	10.0.1.200	10.0.1.210	Syslog	332	7262	514	@\001\020\004\000\000\teJ\017FGVM010000077646ISFWroot\000\000\024date=2024
152	20.0575...	10.0.1.200	10.0.1.210	Syslog	907	7262	514	@\000\020\004\0033\aeJ\017FGVM010000077646ISFWroot\003\003\000\024date
153	20.0576...	10.0.1.200	10.0.1.210	Syslog	1025	7262	514	@\000\020\004\003\0068eJ\017FGVM010000077646ISFWroot\003\002\000\024date
154	20.0576...	10.0.1.200	10.0.1.210	Syslog	648	7262	514	@\000\020\004\0020\005\004eJ\017FGVM010000077646ISFWroot\002\002\000\024da
155	20.0577...	10.0.1.200	10.0.1.210	Syslog	317	7262	514	@\001\020\004\000\000\teJ\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\000\024date=2

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 4d  ....e-J-FGVM
0040  30 31 30 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 15

An administrator has configured the following settings:

```
#config system global
set log-checksum md5-auth
end
```

What is the purpose of executing these commands?

- A. To record the hash value and authentication code of log file
- B. To encrypt log transfer between FortiAnalyzer and other device
- C. To create the secure channel used by the OFTP proces
- D. To verify the integrity of the log files received.

Answer: A

Explanation:

The command set log-checksum md5-auth configures FortiAnalyzer to generate an MD5 hash for each log file, along with an authentication code. This ensures that the integrity of the logs can be verified, confirming that the logs have not been tampered with.

NEW QUESTION 19

Which statement correctly describes RAID 10 (1+0) on FortiAnalyzer?

- A. A configuration with four disks, each with 2 TB of capacity, provides a total space of 4 T
- B. 11 combines mirroring striping and distributed parity to provide performance and fault toleranc
- C. A configuration with four disks, each with 2 TB of capacity, provides a total space of 2 T
- D. It uses striping to provide performance and fault tolerance.

Answer: A

Explanation:

RAID 10 combines mirroring (RAID 1) and striping (RAID 0). In a RAID 10 setup with four disks, data is mirrored across two pairs of disks, and those pairs are striped for performance. This results in improved performance and fault tolerance, but the total usable storage is 50% of the total raw storage, meaning four 2 TB disks provide 4 TB of usable space.

NEW QUESTION 22

You finished registering a FortiGate device. After traffic starts to flow through FortiGate, you notice that only some of the logs expected are being received on FortiAnalyzer.

What could be the reason for the logs not arriving on FortiAnalyzer?

- A. This FortiGate is part of an HA cluster but it is the secondary device.
- B. This FortiGate model is not fully supported.
- C. FortiGate does not have logging configured correctly.
- D. FortiGate was added to the wrong ADOM type.

Answer: C

Explanation:

When only some of the expected logs from a FortiGate device are being received on FortiAnalyzer, it often indicates a configuration issue on the FortiGate side. Proper logging configuration on FortiGate involves specifying what types of logs to generate (e.g., traffic, event, security logs) and ensuring that these logs are directed to the FortiAnalyzer unit for storage and analysis. If the logging settings on FortiGate are not correctly configured, it could result in incomplete log data being sent to FortiAnalyzer. This might include missing logs for certain types of traffic or events that are not enabled for logging on the FortiGate device. Ensuring comprehensive logging is enabled and correctly directed to FortiAnalyzer is crucial for full visibility into network activities and for the effective analysis and reporting of security incidents and network performance.

NEW QUESTION 25

What is the recommended method of expanding disk space on a FortiAnalyzer VM?

- A. From the VM host manager, add an additional virtual disk and use the #execute lvm extendcommand to expand the storage.
- B. From the VM host manager, expand the size of the existing virtual disk.
- C. From the VM host manager, expand the size of the existing virtual disk and use the # executeformat disk command to reformat the disk.
- D. From the VM host manager, add an additional virtual disk and rebuild your RAID array.

Answer: A

Explanation:

Adding an Additional Virtual Disk:

From the VM host manager (such as VMware vSphere or Hyper-V), you can add a new virtual disk to the FortiAnalyzer VM.

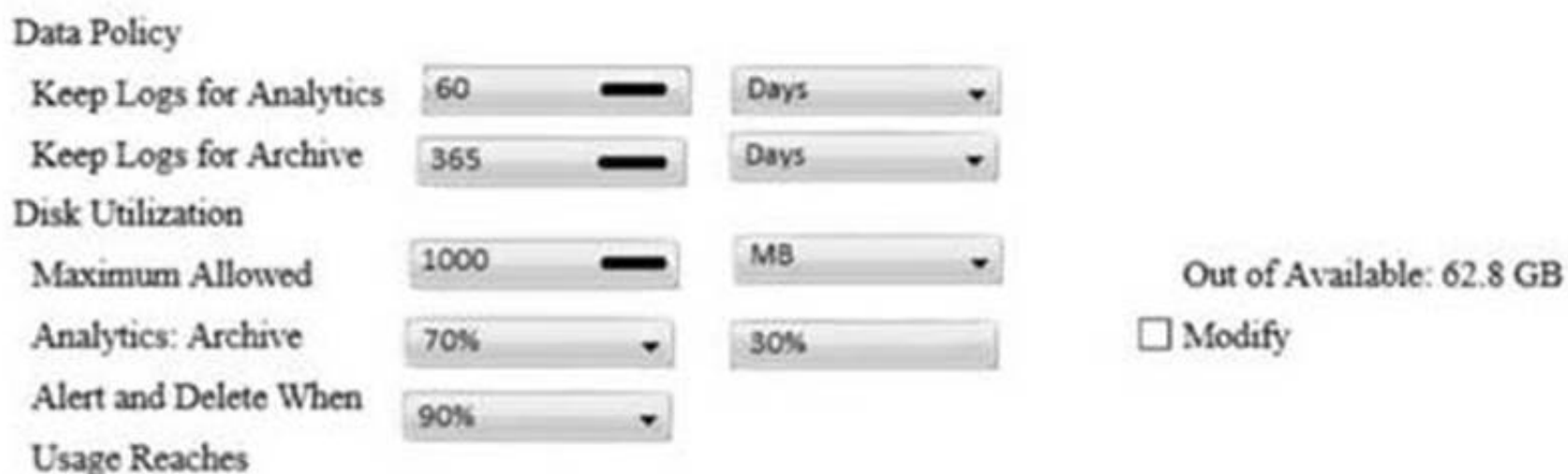
Extending the Logical Volume:

After adding the new disk, use commands like #execute lvm extend within the FortiAnalyzer to extend the logical volume, making the additional storage available to the VM. This is particularly useful when you need to add more storage without disrupting existing data.

This approach is recommended when you need to ensure the FortiAnalyzer VM can handle more storage without reformatting or affecting existing data.

NEW QUESTION 28

View the exhibit:



The screenshot shows the 'Data Policy' configuration page in FortiAnalyzer. It includes sections for 'Keep Logs for Analytics' (60 days), 'Keep Logs for Archive' (365 days), 'Disk Utilization' (Maximum Allowed: 1000 MB), 'Analytics: Archive' (70%), and 'Alert and Delete When Usage Reaches' (90%). There is a 'Modify' button and a status indicator 'Out of Available: 62.8 GB'.

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 31

Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

- A. ADOMs are enabled by default.
- B. ADOMs constrain other administrator's access privileges to a subset of devices in the device list.
- C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
- D. All administrators can create ADOMs--not just the admin administrator.

Answer: BC

Explanation:

ADOMs constrain other administrators' access privileges to a subset of devices in the device list: ADOMs allow you to partition the FortiAnalyzer's management capabilities by restricting access to certain devices and logs based on the administrator's role. This segmentation helps in managing large deployments with different administrative needs.

Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM: When ADOMs are enabled, the FortiAnalyzer interface segments the Device Manager, FortiView, Event Management, and Reports tabs based on the selected ADOM. This allows administrators to work within their specific ADOM context.

ADOMs are enabled by default: This is incorrect because ADOMs are not enabled by default. They must be manually configured and enabled according to the organization's needs.

All administrators can create ADOMs--not just the admin administrator: This is not correct. Typically, creating and managing ADOMs requires administrative privileges, often restricted to the main admin or specific roles with sufficient permissions.

NEW QUESTION 33

.....

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

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

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FAZ_AD-7.4 Practice Test Here](#)