

FCP_FAZ_AD-7.4 Dumps

FCP - FortiAnalyzer 7.4 Administrator

https://www.certleader.com/FCP_FAZ_AD-7.4-dumps.html



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

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 3

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

- 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.

NEW QUESTION 4

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 5

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

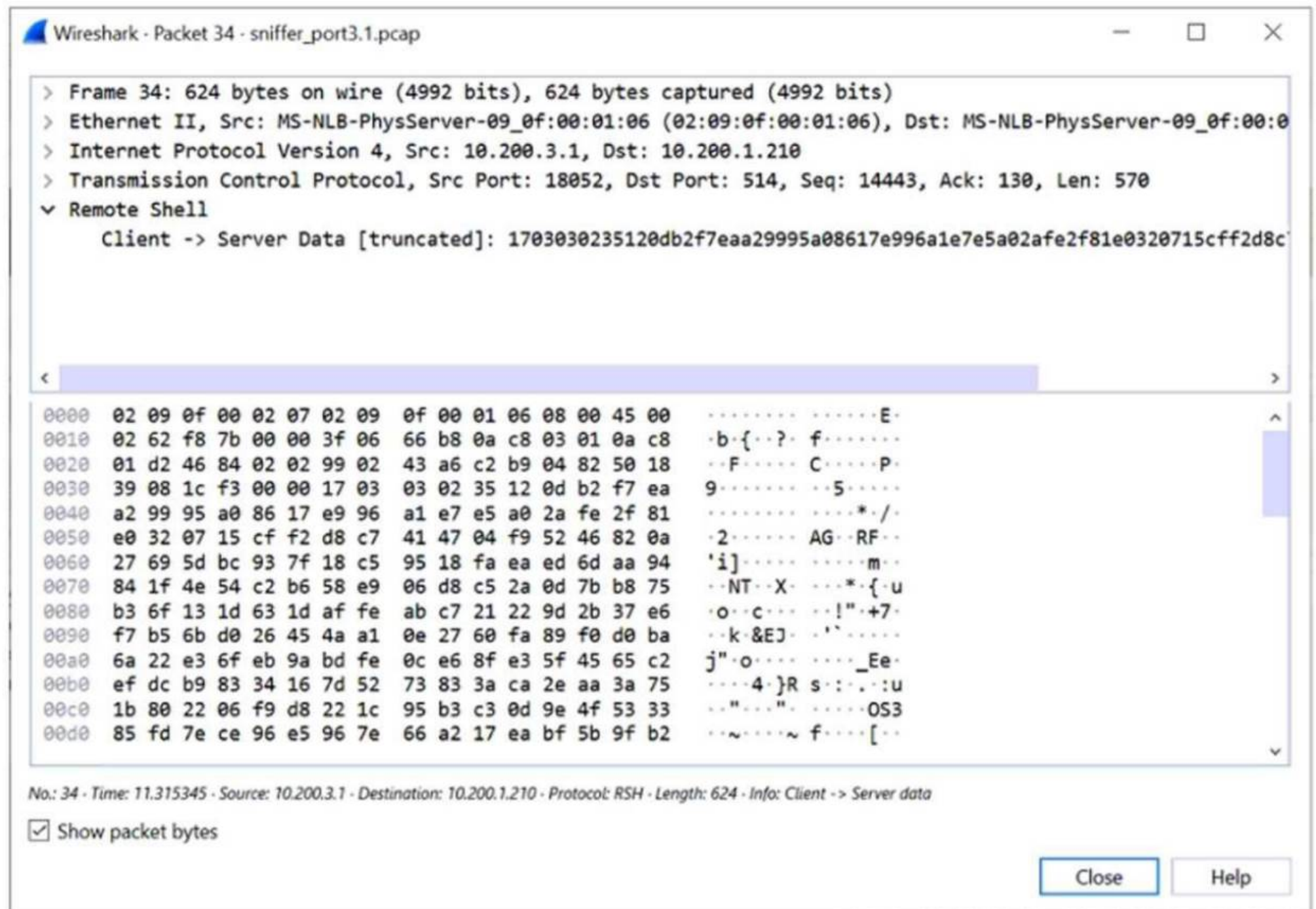
Explanation:

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 6

Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark



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

A)

					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)

					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)

Edit

Delete

Table View

More

Show Charts

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)

Edit

Delete

Table View

More

Show Charts

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 7

What are analytics logs on FortiAnalyzer?

- A. Logs that are compressed and saved to a log file
- B. Logs that roll over when the log file reaches a specific size
- C. Logs that are indexed and stored in the SQL
- D. Logs classified as type Traffic, or type Security

Answer: C

Explanation:

On FortiAnalyzer, analytics logs refer to the logs that have been processed, indexed, and then stored in the SQL database. This process allows for efficient data retrieval and analytics. Unlike basic log storage, which might involve simple compression and storage in a file system, analytics logs in FortiAnalyzer undergo an indexing process. This enables advanced features such as quick search, report generation, and detailed analysis, making it easier for administrators to gain insights into network activities and security incidents.

Reference: FortiAnalyzer 7.2 Administrator Guide - "Log Management" and "Data Analytics" sections.

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\002S\
132	9.114245	10.0.1.200	10.0.1.210	Syslog	1115	22486	514	@\020\020\017\003\0aBeJ\004FGVM010000064692Local-FortiGateroot\002\002S\
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\002\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\002\024date
153	20.0576...	10.0.1.200	10.0.1.210	Syslog	1025	7262	514	@\000\020\004\003\0068eJ\017FGVM010000077646ISFWroot\003\002\002\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\002\024da
155	20.0577...	10.0.1.200	10.0.1.210	Syslog	317	7262	514	@\001\020\004\000\000\teJ\017FGVM010000077646ISFWroot\000\002\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\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-FGM
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 9

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

- 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.

NEW QUESTION 10

Which statement about the communication between FortiGate high availability (HA) clusters and FortiAnalyzer is true?

- A. If devices were registered to FortiAnalyzer before forming a cluster, you can manually add them together
- B. FortiAnalyzer distinguishes each cluster member by the IP addresses in log message header
- C. If the HA primary device becomes unavailable, you must remove it from the HA cluster list on FortiAnalyzer
- D. The FortiGate HA cluster must be in active-passive mode in order to avoid conflict.

Answer: B

Explanation:

This allows FortiAnalyzer to correctly identify and process logs from different members of the HA cluster.

NEW QUESTION 10

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 14

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 18

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 22

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 25

Which SQL query is in the correct order to query the database in the FortiAnalyzer?

- 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

Explanation:

C is correct because it follows the proper SQL query structure:

SELECT: Specifies the column(s) to retrieve.

FROM: Indicates the table to query (Slog in this case).

WHERE: Adds a condition to filter the results (user = 'USERI').

GROUP BY: Groups the results by the specified column (devid).

A, B, and D are incorrect because they do not follow the correct SQL query order:

A is incorrect because the GROUP BY clause is incorrectly placed before the WHERE clause.

B is incorrect because the WHERE clause is incorrectly placed before the FROM clause.

D is incorrect because the SELECT clause is incorrectly placed after the FROM and WHERE clauses.

NEW QUESTION 28

Refer to the exhibit.

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

Which statement is correct regarding the event displayed?

- A. An incident was created from this event.
- B. The security risk was blocked or dropped.
- C. The security event risk is considered open.
- D. The risk source is isolated.

Answer: B

Explanation:

The event status is "Mitigated", which indicates that the insecure SSL connection was successfully blocked or prevented.

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.

NEW QUESTION 29

What are two potential advantages of deploying RAID on FortiAnalyzer? (Choose two.)

- A. It provides redundancy.
- B. It improves performance.
- C. It provides backups.
- D. It reduces system resource usage.

Answer: AB

Explanation:

Here are two potential advantages of deploying RAID on FortiAnalyzer:

RAID configurations can mirror or stripe data across multiple disks. This redundancy helps ensure

that even if one disk fails, the data remains accessible and recoverable. This is crucial for FortiAnalyzer as it stores security logs which are critical for analysis and forensic investigations.

Certain RAID configurations, like RAID 0 (striping) can improve read performance by distributing data reads across multiple disks. This can be beneficial for FortiAnalyzer when performing faster searches or retrieving large log sets.

Here's why the other options are not necessarily advantages:

While RAID can improve data availability in case of disk failures, it's not a replacement for proper backups. Backups should be done regularly to a separate location to ensure data recovery in case of catastrophic events like hardware failures or ransomware attacks. RAID itself doesn't necessarily reduce system resource usage. In fact, some RAID configurations can introduce additional overhead for managing the redundant data.

NEW QUESTION 33

What are two of the key features of FortiAnalyzer? (Choose two.)

- A. Centralized log repository
- B. Cloud-based management
- C. Reports
- D. Virtual domains (VDOMs)

Answer: AC

Explanation:

FortiAnalyzer acts as a central repository for collecting and storing logs from multiple Fortinet devices. This centralized log management facilitates efficient analysis, search, and correlation of logs from across the network.

FortiAnalyzer provides robust reporting capabilities, allowing users to generate detailed reports based on collected logs and data. These reports can include insights on security events, network performance, and compliance.

Cloud-based management is not a primary feature of FortiAnalyzer, as it is typically an on-premises appliance, although it can integrate with cloud services.

Virtual domains (VDOMs) are a feature of FortiGate devices, allowing them to be partitioned into multiple virtual domains for administrative and policy separation. FortiAnalyzer itself does not provide VDOMs.

NEW QUESTION 35

What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

Answer: D

Explanation:

The miglogd process on FortiGate is responsible for caching logs when FortiAnalyzer is unreachable. It temporarily stores logs in memory and, if the memory buffer fills up, it starts storing logs on disk. Once the connection to FortiAnalyzer is restored, miglogd sends the cached logs to the FortiAnalyzer.

NEW QUESTION 37

How do you restrict an administrator's access to a subset of your organization's ADOMs?

- A. Set the ADOM mode to Advanced
- B. Assign the ADOMs to the administrator's account
- C. Configure trusted hosts
- D. Assign the default Super_User administrator profile

Answer: B

Explanation:

To restrict an administrator's access to a subset of your organization's ADOMs (Administrative Domains) in FortiAnalyzer, you need to assign the specific ADOMs to the administrator's account. Here's how this works:

Assign the ADOMs to the Administrator's Account (Option B):

In FortiAnalyzer, you can configure which ADOMs an administrator has access to by assigning them directly to the administrator's account. This allows you to control and limit the administrator's access to only the ADOMs they are authorized to manage or view.

NEW QUESTION 38

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCP_FAZ_AD-7.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FAZ_AD-7.4-dumps.html