Fortinet

Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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 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 3
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 4
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 5
Which two methods can you use to restrict administrative access on FortiAnalyzer? (Choose two.)

A. Configure trusted hosts.
B. Limit access to specific virtual domains.
C. Fabric connectors to external LDAP servers.
D. Use administrator profiles.

Answer: AD

Explanation:

Configure trusted hosts.
Trusted hosts restrict administrative access to FortiAnalyzer by limiting the IP addresses or subnets from which administrators can log in.
Use administrator profiles.
Administrator profiles define roles and permissions, restricting what specific administrators can access and manage on FortiAnalyzer.
The other options are not applicable because:
Limiting access to specific virtual domains is not applicable to FortiAnalyzer, as virtual domains (VDOMs) are a concept used in FortiGate, not FortiAnalyzer.
Fabric connectors to external LDAP servers are used for authentication purposes but do not directly restrict administrative access based on roles or IP addresses.

NEW QUESTION 6
What does the disk status Degraded mean for RAID management?

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.

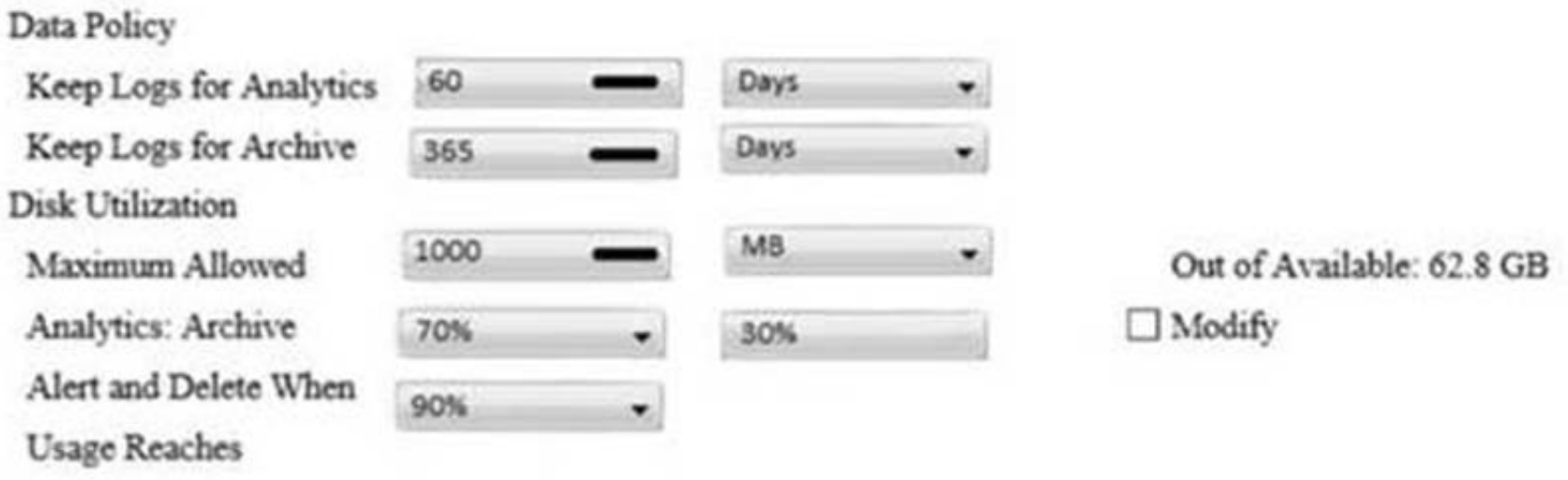
NEW QUESTION 7
In a Fortinet Security Fabric, what can make an upstream FortiGate create traffic logs associated with sessions initiated on downstream FortiGate devices?

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 8
View the exhibit:



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 9
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' =* USERl'
B. SELECT devid WHERE 'u3er'='USERl' FROM $ log GROUP BY devid
C. SELECT devid FROM Slog- WHERE *user' =' USERl' GROUP BY devid
D. FROM Slog WHERE 'user* =' USERl' 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 = 'USERl').
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 10
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 10
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 12
.....

Relate Links

100% Pass Your FCP_FAZ_AD-7.4 Exam with Exambible Prep Materials

https://www.exambible.com/FCP_FAZ_AD-7.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/