

NSE5_FAZ-7.2 Dumps

Fortinet NSE 5 - FortiAnalyzer 7.2

https://www.certleader.com/NSE5_FAZ-7.2-dumps.html



NEW QUESTION 1

What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

- A. Hot swap the disk.
- B. There is no need to do anything because the disk will self-recover.
- C. Run execute format disk to format and restart the FortiAnalyzer device.
- D. Shut down FortiAnalyzer and replace the disk

Answer: D

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiMana> If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the unit is still running – known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

NEW QUESTION 2

Consider the CLI command:

```
# configure system global
  set log-checksum md5
end
```

What is the purpose of the command?

- A. To add a unique tag to each log to prove that it came from this FortiAnalyzer
- B. To add the MD5 hash value and authentication code
- C. To add a log file checksum
- D. To encrypt log communications

Answer: C

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/849211/global>

NEW QUESTION 3

Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally? (Choose two.)

- A. Mail server
- B. Output profile
- C. SFTP server
- D. Report scheduling

Answer: AB

NEW QUESTION 4

On the RAID management page, the disk status is listed as Initializing.

What does the status Initializing indicate about what the FortiAnalyzer is currently doing?

- A. FortiAnalyzer is ensuring that the parity data of a redundant drive is valid
- B. FortiAnalyzer is writing data to a newly added hard drive to restore it to an optimal state
- C. FortiAnalyzer is writing to all of its hard drives to make the array fault tolerant
- D. FortiAnalyzer is functioning normally

Answer: C

NEW QUESTION 5

Which two methods can you use to send event notifications when an event occurs that matches a configured event handler? (Choose two.)

- A. SMS
- B. Email
- C. SNMP
- D. IM

Answer: BC

NEW QUESTION 6

If a hard disk fails on a FortiAnalyzer that supports software RAID, what should you do to bring the FortiAnalyzer back to functioning normally, without losing data?

- A. Hot swap the disk
- B. Replace the disk and rebuild the RAID manually
- C. Take no action if the RAID level supports a failed disk
- D. Shut down FortiAnalyzer and replace the disk

Answer: D

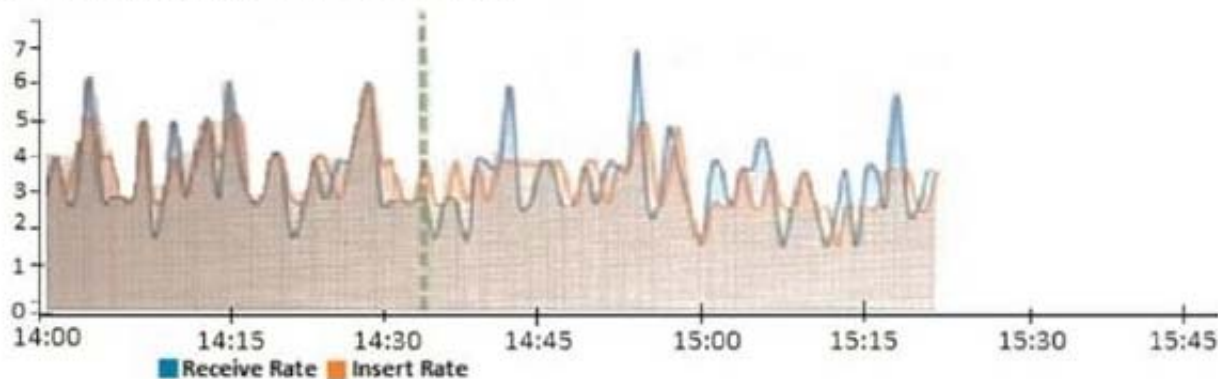
Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiMana> If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the unit is still running – known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

NEW QUESTION 7

View the exhibit.

Insert Rate vs Receive Rate - Last 1 hour



What does the data point at 14:35 tell you?

- A. FortiAnalyzer is dropping logs.
- B. FortiAnalyzer is indexing logs faster than logs are being received.
- C. FortiAnalyzer has temporarily stopped receiving logs so older logs' can be indexed.
- D. The sqlplugind daemon is ahead in indexing by one log.

Answer: B

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-wi>

NEW QUESTION 8

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

NEW QUESTION 9

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

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

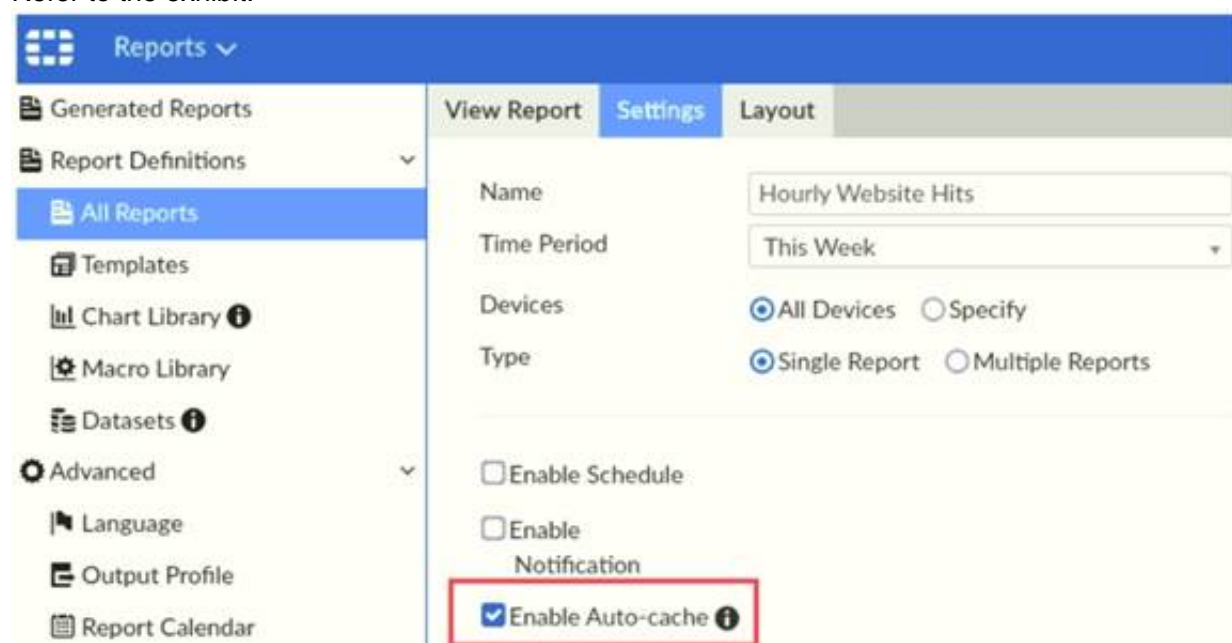
Answer: BD

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation>

NEW QUESTION 10

Refer to the exhibit.



Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)

- Answer: CD**

View the exhibit.

```
Total Quota Summary:
      Total Quota    Allocated    Available    Allocate%
      63.7GB        12.7GB        51.0GB        19.9%

System Storage Summary:
      Total      Used      Available      Use%
      78.7GB    2.9GB      75.9GB      3.6%

Reserved space: 15.0GB (19.0% of total space).
```

A. 3.6% of the system storage is already being used.
B. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files
C. The oftpd process has not archived the logs yet
D. The logfiled process is just estimating the total quota

Answer: B

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation>


A. SELECT devid FROM Slog GROOP BY devid WHERE * user' =* USER!
B. SELECT devid WHERE 'u3er'='USER!' FROM \$ log GROUP BY devid
C. SELECT devid FROM Slog- WHERE *user' = ' USER!' GROUP BY devid
D. FROM Slog WHERE 'user* = ' USER!' SELECT devid GROUP BY devid

Answer: C

Refer to the exhibit.

[illegible]


A)



The screenshot shows the FortiGate Device Manager interface. At the top, there is a navigation bar with 'Device Manager' and a menu icon. Below this is a toolbar with buttons for '+ Add Device', 'Edit', 'Delete', 'More', and 'Column Settings'. The main area displays a table with the following columns: 'Device Name', 'IP Address', 'Platform', 'Logs', and 'Average Log Rate(Logs/Sec)'. There is one row in the table with the following data: 'Remote-Fortigate' (Device Name), '10.200.3.1' (IP Address), 'FortiGate-VM64' (Platform), 'Real Time' (Logs), and '0' (Average Log Rate). The 'Logs' column has a green status icon next to the text 'Real Time'.

Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
Remote-Fortigate	10.200.3.1	FortiGate-VM64	Real Time	0

B)



The screenshot shows the FortiGate Device Manager interface. At the top, there is a blue header bar with the text "Device Manager" and a hamburger menu icon. Below the header, there is a toolbar with buttons for "Add Device", "Edit", "Delete", "More", and "Column Settings". The main area displays a table with the following columns: "Device Name", "IP Address", "Platform", "Logs", and "Average Log Rate(Logs/Sec)". The table contains one row for a device named "Remote-Fortigate" with IP address "10.200.3.1" and platform "FortiGate-VM64". The "Logs" column for this device shows a green dot and the text "Real Time". The "Average Log Rate(Logs/Sec)" column shows the value "0".

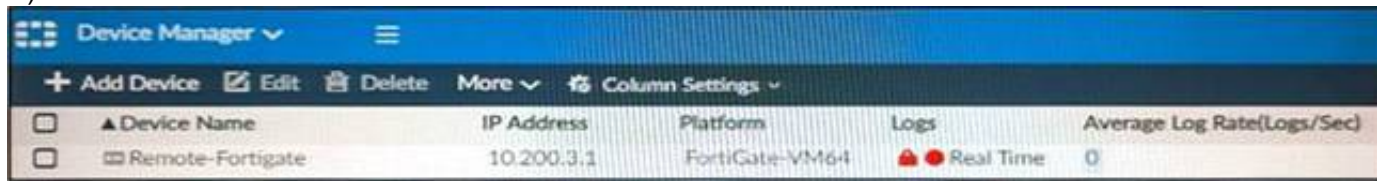
Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
Remote-Fortigate	10.200.3.1	FortiGate-VM64	Real Time	0

C)



Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
Remote-Fortigate	10.200.3.1	FortiGate-VM64	Real Time	0

D)



Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
Remote-Fortigate	10.200.3.1	FortiGate-VM64	Real Time	0

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

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:

[https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20\(%22Redundant%20Array%20of%20Inexpensive,%2C%](https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20(%22Redundant%20Array%20of%20Inexpensive,%2C%)

NEW QUESTION 21

Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?

- A. Log upload
- B. Indicators of Compromise
- C. Log forwarding an aggregation mode
- D. Log fetching

Answer: D

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetcher-management>

NEW QUESTION 23

You've moved a registered logging device out of one ADOM and into a new ADOM. What happens when you rebuild the new ADOM database?

- A. FortiAnalyzer resets the disk quota of the new ADOM to default.
- B. FortiAnalyzer migrates archive logs to the new ADOM.
- C. FortiAnalyzer migrates analytics logs to the new ADOM.
- D. FortiAnalyzer removes logs from the old ADOM.

Answer: C

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD40383>

NEW QUESTION 28

You crested a playbook on FortiAnalyzer that uses a FortiOS connector

When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?

- A. FortiAnalyzer Event Handler
- B. Incoming webhook
- C. FortiOS Event Log
- D. Fabric Connector event

Answer: D

NEW QUESTION 30

How does FortiAnalyzer retrieve specific log data from the database?

- A. SQL FROM statement
- B. SQL GET statement
- C. SQL SELECT statement
- D. SQL EXTRACT statement

Answer: A

Explanation:

<https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/137bb60e-ff37-11e8-8524-f8bc1258b8>

NEW QUESTION 31

Which two statements about log forwarding are true? (Choose two.)

- A. Forwarded logs cannot be filtered to match specific criteria.
- B. Logs are forwarded in real-time only.
- C. The client retains a local copy of the logs after forwarding.
- D. You can use aggregation mode only with another FortiAnalyzer.

Answer: CD

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/420493/modes> <https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/621804/log-forwarding>

NEW QUESTION 35

An administrator has configured the following settings: config system fortiview settings

set resolve-ip enable end

What is the significance of executing this command?

- A. Use this command only if the source IP addresses are not resolved on FortiGate.
- B. It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.
- C. You must configure local DNS servers on FortiGate for this command to resolve IP addresses on Forti Analyzer.
- D. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

Answer: D

NEW QUESTION 40

Which statement is true regarding Macros on FortiAnalyzer?

- A. Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.
- B. Macros are supported only on the FortiGate ADOM.
- C. Macros are useful in generating excel log files automatically based on the reports settings.
- D. Macros are predefined templates for reports and cannot be customized.

Answer: A

NEW QUESTION 41

What is the purpose of output variables?

- A. To store playbook execution statistics
- B. To use the output of the previous task as the input of the current task
- C. To display details of the connectors used by a playbook
- D. To save all the task settings when a playbook is exported

Answer: A

NEW QUESTION 43

Which statements are correct regarding FortiAnalyzer reports? (Choose two)

- A. FortiAnalyzer provides the ability to create custom reports.
- B. FortiAnalyzer allows you to schedule reports to run.
- C. FortiAnalyzer includes pre-defined reports only.
- D. FortiAnalyzer allows reporting for FortiGate devices only.

Answer: AB

NEW QUESTION 48

Which statement is true when you are upgrading the firmware on an HA cluster made up of two FortiAnalyzer devices?

- A. First, upgrade the secondary device, and then upgrade the primary device.
- B. Both FortiAnalyzer devices will be upgraded at the same time.
- C. You can enable uninterruptible-upgrade so that the normal FortiAnalyzer operations are not interrupted while the cluster firmware upgrades.
- D. You can perform the firmware upgrade using only a console connection.

Answer: D

NEW QUESTION 53

You need to upgrade your FortiAnalyzer firmware.

What happens to the logs being sent to FortiAnalyzer from FortiGate during the time FortiAnalyzer is temporarily unavailable?

- A. FortiAnalyzer uses log fetching to retrieve the logs when back online
- B. FortiGate uses the miglogd process to cache the logs
- C. The logfiled process stores logs in offline mode
- D. Logs are dropped

Answer: B

Explanation:

If FortiAnalyzer becomes unavailable to FortiGate for any reason, FortiGate uses its *miglogd* process to cache the logs. There is a maximum value to the cache size, and the miglogd process will drop cached logs. When the connection between the two devices is restored, the miglogd process begins to send the cached logs to FortiAnalyzer. Therefore, the FortiGate buffer will keep logs long enough to sustain a reboot of your FortiAnalyzer (if you are upgrading the firmware, for example). But it is not intended for a lengthy FortiAnalyzer outage.

NEW QUESTION 54

In the FortiAnalyzer FortiView, source and destination IP addresses from FortiGate devices are not resolving to a hostname. How can you resolve the source and destination IP addresses, without introducing any additional performance impact to FortiAnalyzer?

- A. Resolve IP addresses on a per-ADOM basis to reduce delay on FortiView while IPs resolve
- B. Configure # set resolve-ip enable in the system FortiView settings
- C. Configure local DNS servers on FortiAnalyzer
- D. Resolve IP addresses on FortiGate

Answer: D

Explanation:

<https://packetplant.com/fortigate-and-fortianalyzer-resolve-source-and-destination-ip/>

“As a best practice, it is recommended to resolve IPs on the FortiGate end. This is because you get both source and destination, and it offloads the work from FortiAnalyzer. On FortiAnalyzer, this IP resolution does destination IPs only”

NEW QUESTION 56

Which statement correctly describes the management extensions available on FortiAnalyzer?

- A. Management extensions do not require additional licenses.
- B. Management extensions allow FortiAnalyzer to act as a ForbSIEM supervisor.
- C. Management extensions require a dedicated VM for best performance.
- D. Management extensions may require a minimum number of CPU cores to run.

Answer: A

NEW QUESTION 59

What is required to authorize a FortiGate on FortiAnalyzer using Fabric authorization?

- A. A FortiGate ADOM
- B. The FortiGate serial number
- C. A pre-shared key
- D. Valid FortiAnalyzer credentials

Answer: C

NEW QUESTION 64

If the primary FortiAnalyzer in an HA cluster fails, how is the new primary elected?

- A. The configured IP address is checked first.
- B. The active port number is checked first.
- C. The firmware version is checked first.
- D. The configured priority is checked first

Answer: C

NEW QUESTION 69

What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

- A. Chart Builder
- B. Export to Report Chart
- C. Dataset Library
- D. Custom View

Answer: A

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/989203/building-charts-with-chart-builder>

NEW QUESTION 72

Which daemon is responsible for enforcing raw log file size?

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

Answer: A

NEW QUESTION 74

Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

- A. FortiView
- B. Event Management
- C. Device Manger
- D. Reporting

Answer: B

NEW QUESTION 76

Which two statements are correct regarding the export and import of playbooks? (Choose two.)

- A. You can export only one playbook at a time.
- B. You can import a playbook even if there is another one with the same name in the destination.
- C. Playbooks can be exported and imported only within the same FortiAnaryzer.
- D. A playbook that was disabled when it was exported, will be disabled when it is imported.

Answer: BD

NEW QUESTION 80

The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device. What can be the reason for this failure?

- A. FortiAnalyzer is in an HA cluster.
- B. ADOM mode should be set to advanced, in order to register the FortiClient EMS device.
- C. ADOMs are not enabled on FortiAnalyzer.
- D. A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.

Answer: C

NEW QUESTION 84

When you perform a system backup, what does the backup configuration contain? (Choose two.)

- A. Generated reports
- B. Device list
- C. Authorized devices logs
- D. System information

Answer: BD

Explanation:

https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400_execute/backup.htm

NEW QUESTION 88

On FortiAnalyzer, what is a wildcard administrator account?

- A. An account that permits access to members of an LDAP group
- B. An account that allows guest access with read-only privileges
- C. An account that requires two-factor authentication
- D. An account that validates against any user account on a FortiAuthenticator

Answer: A

Explanation:

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/747268/configuring-wildcard-admin-accounts>

NEW QUESTION 93

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec? (Choose two.)

- A. Must configure the FortiAnalyzer end of the tunnel only--the FortiGate end is auto-negotiated.
- B. Must establish an IPsec tunnel ID and pre-shared key.
- C. IPsec cannot be enabled if SSL is enabled as well.
- D. IPsec is only enabled through the CLI on FortiAnalyzer.

Answer: C

NEW QUESTION 98

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

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

Answer: BC

NEW QUESTION 100

A play book contains five tasks in total. An administrator executed the playbook and four out of five tasks finished successfully, but one task failed. What will be the status of the playbook after its execution?

- A. Success
- B. Failed
- C. Running
- D. Upstream_failed

Answer: A

NEW QUESTION 104

By default, what happens when a log file reaches its maximum file size?

- A. FortiAnalyzer overwrites the log files.
- B. FortiAnalyzer stops logging.
- C. FortiAnalyzer rolls the active log by renaming the file.
- D. FortiAnalyzer forwards logs to syslog.

Answer: C

NEW QUESTION 109

Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate to FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

- A. A local wildcard administrator account
- B. A remote LDAP server
- C. A trusted host profile that restricts access to the LDAP group
- D. An administrator group

Answer: AB

NEW QUESTION 113

Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

- A. FROM
- B. LIMIT
- C. WHERE
- D. ORDER BY

Answer: A

NEW QUESTION 117

Refer to the exhibit.

The screenshot shows the 'New Administrator' configuration page in FortiAnalyzer. The left sidebar contains a menu with 'System Settings' at the top, followed by 'Dashboard', 'Logging Topology', 'All ADOMs', 'Storage Info', 'Network', 'HA', 'Admin', and 'Administrators'. The 'Administrators' section is expanded, showing 'Profile', 'Remote Authentication Server', 'Admin Settings', 'SAML SSO', 'Certificates', 'Local Certificates', and 'CA Certificates'. The main content area is titled 'New Administrator' and contains the following fields: 'User Name' (remoteadmin), 'Avatar' (with a green 'R' icon and buttons for '+ Change Photo' and '- Remove Photo'), 'Comments' (empty text area), 'Admin Type' (GROUP), 'GROUP' (remoteservergroup), 'Match all users on remote server' (checked checkbox, highlighted with a red box), 'Admin Profile' (Super_User), 'Administrative Domain' (All ADOMs), 'JSON API Access' (None), 'Trusted Hosts' (OFF), 'Meta Fields' (expandable), and 'Advanced Options' (expandable).

The exhibit shows “remoteservergroup” is an authentication server group with LDAP and RADIUS servers. Which two statements express the significance of enabling “Match all users on remote server” when configuring a new administrator? (Choose two.)

- A. It creates a wildcard administrator using LDAP and RADIUS servers.
- B. Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.
- C. Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at anytime.
- D. It allows administrators to use two-factor authentication.

Answer: AB

NEW QUESTION 118

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 extend <disk number> command 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 # execute format 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:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD40848>

NEW QUESTION 123

What is the purpose of a predefined template on the FortiAnalyzer?

- A. It can be edited and modified as required
- B. It specifies the report layout which contains predefined texts, charts, and macros
- C. It specifies report settings which contains time period, device selection, and schedule
- D. It contains predefined data to generate mock reports

Answer: B

NEW QUESTION 126

In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results. Similarly, which feature you can use for FortiView?

- A. Export to Report Chart
- B. Export to PDF
- C. Export to Chart Builder
- D. Export to Custom Chart

Answer: A

NEW QUESTION 131

.....

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 NSE5_FAZ-7.2 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE5_FAZ-7.2-dumps.html