Fortinet

Exam Questions NSE5_FAZ-7.0

Fortinet NSE 5 - FortiAnalyzer 7.0

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
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 2
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 3
When working with FortiAnalyzer reports, what is the purpose of a dataset?

A. To provide the layout used for reports
B. To define the chart type to be used
C. To retrieve data from the database
D. To set the data included in templates

Answer: C

NEW QUESTION 4
Which two statements express the advantages of grouping similar reports? (Choose two.)

A. Improve report completion time.
B. Conserve disk space on FortiAnalyzer by grouping multiple similar reports.
C. Reduce the number of hcache tables and improve auto-hcache completion time.
D. Provides a better summary of reports.

Answer: AC

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
What statements are true regarding FortiAnalyzer 's treatment of high availability (HA) dusters? (Choose two)

A. FortiAnalyzer distinguishes different devices by their serial number.
B. FortiAnalyzer receives logs from d devices in a duster.
C. FortiAnalyzer receives bgs only from the primary device in the cluster.
D. FortiAnalyzer only needs to know (he serial number of the primary device in the cluster-it automaticaly discovers the other devices.

Answer: AB

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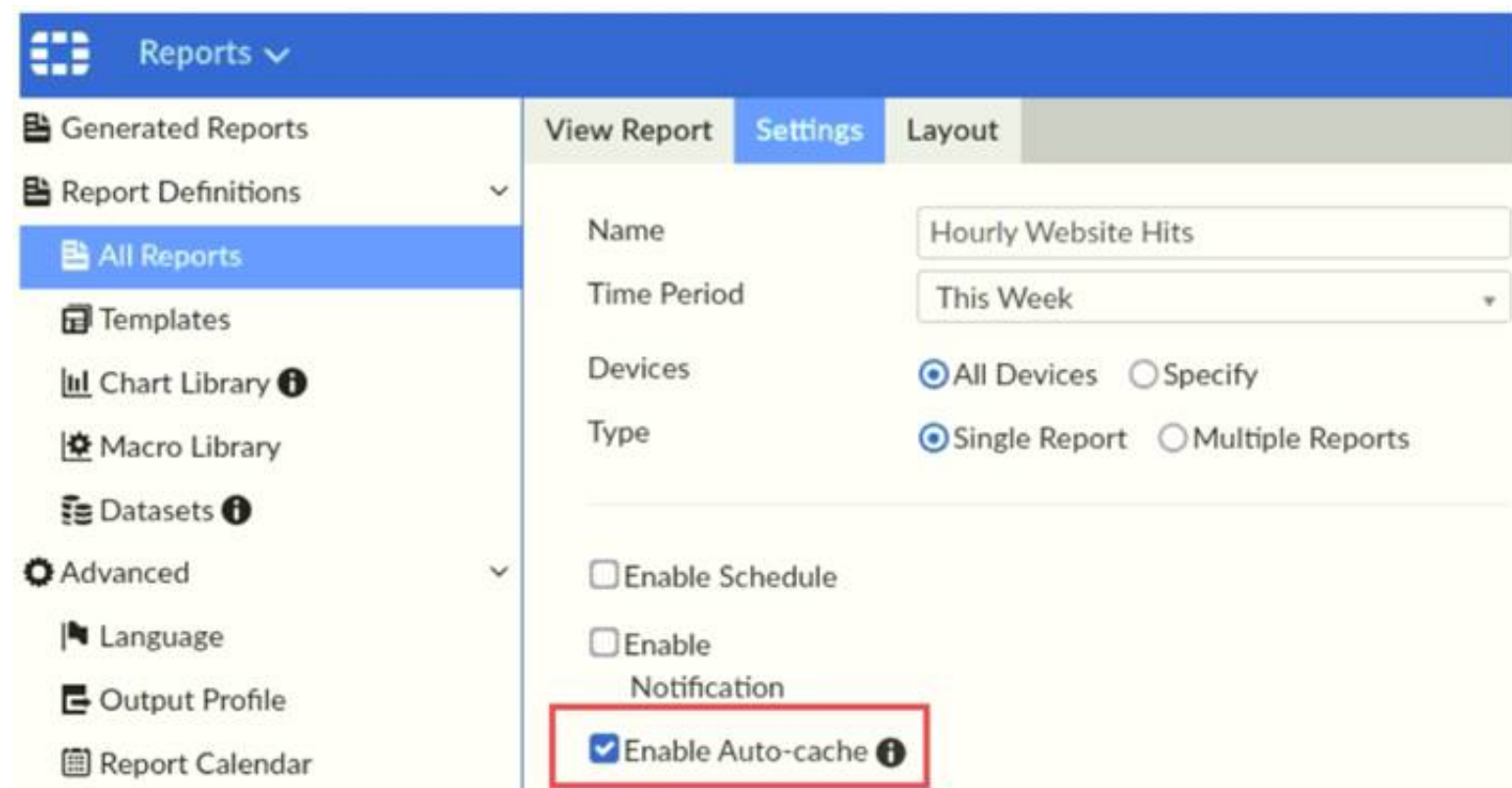
A. License type
B. Disk size
C. Total quota
D. RAID level

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.)

A. Report size will be optimized to conserve disk space on FortiAnalyzer.
B. Reports will be cached in the memory.
C. This feature is automatically enabled for scheduled reports.
D. Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.
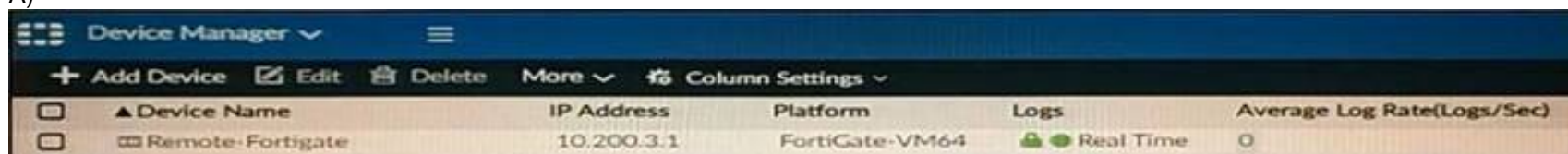
Answer: CD

NEW QUESTION 10
Refer to the exhibit.

```
Wireshark - Packet 50 - sniffer_port1.1.pcap

> Frame 50: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits)
> Ethernet II, Src: VMware_a8:79:e6 (00:0c:29:a8:79:e6), Dst: VMware_c0:81:79 (00:0c:29:c0:81:79)
> Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210
> User Datagram Protocol, Src Port: 15864, Dst Port: 514
v  [truncated]Syslog message: (unknown): �� @\001\020\020\004\000\001\000�\000�a�7\FGVM010000065036Remote\
   > Message: �� @\001\020\020\004

0000  00 0c 29 c0 81 79 00 0c  29 a8 79 e6 08 00 45 00    )  y    ) y   E
0010  01 4b fb 88 00 00 3f 11  64 b7 0a c8 03 01 0a c8    K    ?  d
0020  01 d2 3d f8 02 02 01 37  7c 24 ec cf 20 40 01 10    -    7 |$   @
0030  10 04 00 01 00 f7 00 fe  61 a7 37 5c 46 47 56 4d    a 7\FGVM
0040  30 31 30 30 30 30 30 36  35 30 33 36 52 65 6d 6f    01000006 5036Remo
0050  74 65 2d 46 6f 72 74 69  47 61 74 65 72 6f 6f 74    te-Forti Gateroot
0060  00 fe f1 14 64 61 74 65  3d 32 30 32 31 2d 31 32    date =2021-12
0070  2d 30 31 20 74 69 6d 65  3d 30 30 3a 35 30 3a 33    -01 time =00:50:3
0080  36 20 65 76 65 6e 74 13  00 f1 29 31 36 33 38 33    6 event  )16383
0090  34 38 36 33 36 39 34 39  32 36 35 35 36 35 20 74    48636949 265565 t
00a0  7a 3d 22 2d 30 38 30 30  22 20 6c 6f 67 69 64 3d    z=" -0800 " logid=
00b0  22 30 31 30 30 30 32 30  30 31 34 22 20 74 79 70    "0100020 014" typ
00c0  65 3d 22 42 00 52 22 20  73 75 62 10 00 f1 11 73    e="B R" sub    s
00d0  79 73 74 65 6d 22 20 6c  65 76 65 6c 3d 22 77 61    ystem" l evel="wa
00e0  72 6e 69 6e 67 22 20 76  64 3d 22 72 6f 6f 74 4b    rning" v d="rootK
00f0  00 f0 12 64 65 73 63 3d  22 54 65 73 74 22 20 75    desc= "Test" u
0100  73 65 72 3d 22 61 64 6d  69 6e 22 20 61 63 74 69    ser="adm in" acti
0110  6f 6e 3d 22 6f 00 f0 0a  6e 22 20 73 74 61 74 75    on="o   n" statu
0120  73 3d 22 73 75 63 63 65  73 73 22 20 6d 73 67 3d    s="succe ss" msg=
0130  22 32 00 11 20 31 00 00  97 00 f0 0e 67 65 64 20    "2   1      ged
0140  69 6e 74 6f 20 74 68 65  20 66 77 20 2d 20 31 36    into the  fw - 16
0150  33 38 33 34 38 36 33 36  22                         38348636 "
```

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

A)

	▲ Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
☐	🔲 Remote-Fortigate	10.200.3.1	FortiGate-VM64	🔒● Real Time	O

B)

	▲ Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
☐	🔲 Remote-Fortigate	10.200.3.1	FortiGate-VM64	● Real Time	O

C)

	▲ Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
☐	🔲 Remote-Fortigate	10.200.3.1	FortiGate-VM64	● Real Time	O

D)

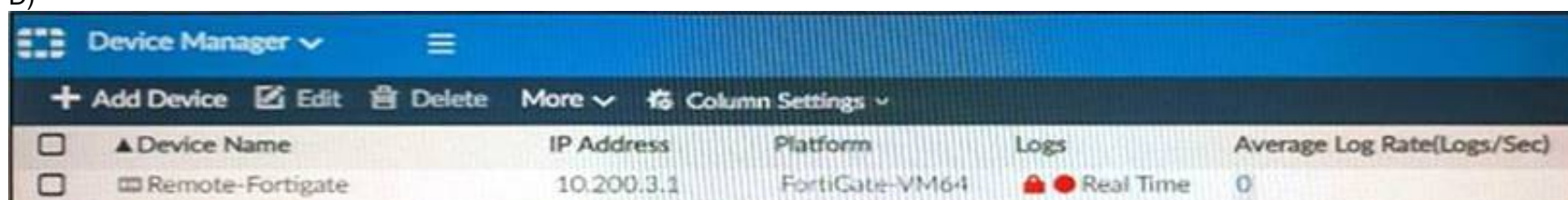|	▲ Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
☐	🔲 Remote-Fortigate	10.200.3.1	FortiGate-VM64	🔒● Real Time	O

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

Answer: D

NEW QUESTION 13
Which statement is true about sending notifications with incident updates?

A. Notifications can be sent only when an incident is updated or deleted.
B. If you use multiple fabric connectors, all connectors must have the same notification settings
C. Notifications can be sent only by email.
D. You can send notifications to multiple external platforms

Answer: A

NEW QUESTION 17
What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

Answer: D

NEW QUESTION 21
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%

NEW QUESTION 22
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 23
Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

A. Incidents dashboards
B. Threat hunting
C. FortiView Monitor
D. Outbreak alert services

Answer: B

NEW QUESTION 27
Which two statements are true regarding ADOM modes? (Choose two.)

A. You can only change ADOM modes through CLI.
B. In normal mode, the disk quota of the ADOM is fixed and cannot be modified, but in advance mode, the disk quota of the ADOM is flexible because new devices are added to the ADOM.
C. In an advanced mode ADO
D. you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.
E. Normal mode is the default ADOM mode.

Answer: CD

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.
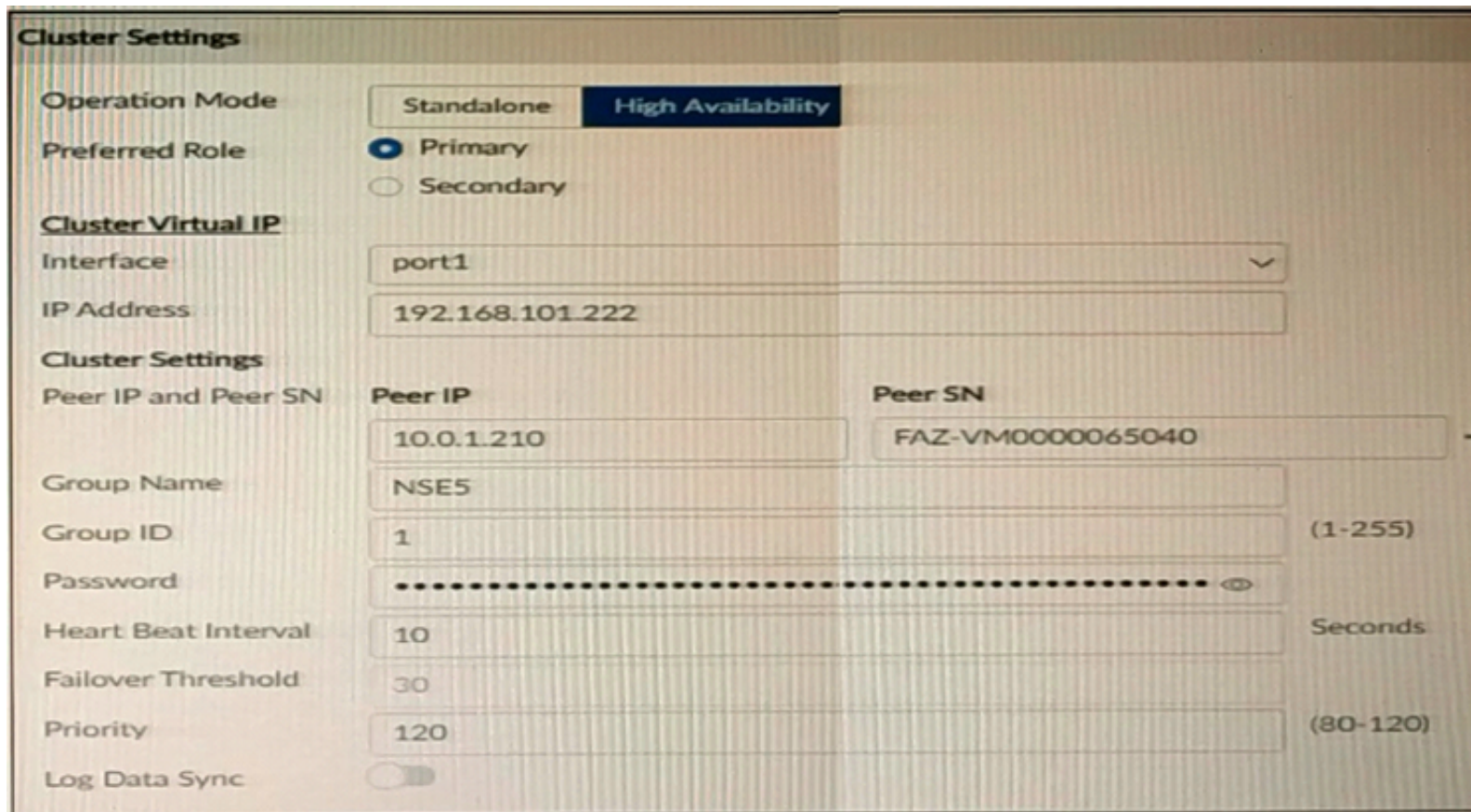D. You can use aggregation mode only with another FortiAnalyzer.

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 34
Refer to the exhibit.

Cluster Settings

Operation Mode	Standalone	High Availability

Preferred Role ● Primary
                    ○ Secondary

Cluster Virtual IP

Interface	port1	
IP Address	192.168.101.222	

Cluster Settings

Peer IP and Peer SN	**Peer IP**	**Peer SN**
	10.0.1.210	FAZ-VM0000065040

Group Name	NSE5	
Group ID	1	(1-255)
Password	•• ⊙	
Heart Beat Interval	10	Seconds
Failover Threshold	30	
Priority	120	(80-120)
Log Data Sync	⬤	

The image displays the configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster.
What can you conclude from the configuration displayed?

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

Answer: D

NEW QUESTION 38
What are offline logs on FortiAnalyzer?

A. Compressed logs, which are also known as archive logs, are considered to be offline logs.
B. When you restart FortiAnalyze
C. all stored logs are considered to be offline logs.
D. Logs that are indexed and stored in the SQL database.
E. Logs that are collected from offline devices after they boot up.

Answer: A

NEW QUESTION 42
You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used.
What does the disk quota refer to?

A. The maximum disk utilization for each device in the ADOM
B. The maximum disk utilization for the FortiAnalyzer model
C. The maximum disk utilization for the ADOM type
D. The maximum disk utilization for all devices in the ADOM

Answer: D

NEW QUESTION 44
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 49
How are logs forwarded when FortiAnalyzer is using aggregation mode?

A. Logs are forwarded as they are received and content files are uploaded at a scheduled time.
B. Logs and content files are stored and uploaded at a scheduled time.
C. Logs are forwarded as they are received.
D. Logs and content files are forwarded as they are received.

Answer: B

Explanation:
https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/ https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes

NEW QUESTION 51
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 55
Refer to the exhibits.

How many events will be added to the incident created after running this playbook?

A. Ten events will be added.
B. No events will be added.
C. Five events will be added.
D. Thirteen events will be added.

Answer: C

NEW QUESTION 57
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 keeps 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 60
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 62
How can you configure FortiAnalyzer to permit administrator logins from only specific locations?

A. Use static routes
B. Use administrative profiles
C. Use trusted hosts
D. Use secure protocols

Answer: C

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/186508/trusted-hosts

NEW QUESTION 67
Which daemon is responsible for enforcing the log file size?

A. sqlplugind
B. logfiled
C. miglogd
D. ofrpd

Answer: B

NEW QUESTION 72
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 74
Which two purposes does the auto cache setting on reports serve? (Choose two.)

A. It automatically updates the hcache when new logs arrive.
B. It provides diagnostics on report generation time.
C. It reduces the log insert lag rate.
D. It reduces report generation time.

Answer: AD

NEW QUESTION 77
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 79
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 84
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 85
What are two advantages of setting up fabric ADOM? (Choose two.)

A. It can be used for fast data processing and log correlation
B. It can be used to facilitate communication between devices in same Security Fabric
C. It can include all Fortinet devices that are part of the same Security Fabric
D. It can include only FortiGate devices that are part of the same Security Fabric

Answer: AC

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-a

NEW QUESTION 89
An administrator has moved FortiGate A 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 presented in both ADOMs immediately after the move.
D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the ADOM1 SQL database.

Answer: BD

NEW QUESTION 92
Logs are being deleted from one of the ADOMs earlier than the configured setting for archiving in the data policy.
What is the most likely problem?

A. CPU resources are too high
B. Logs in that ADOM are being forwarded, in real-time, to another FortiAnalyzer device
C. The total disk space is insufficient and you need to add other disk
D. The ADOM disk quota is set too low, based on log rates

Answer: D

NEW QUESTION 94
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 98
What can you do on FortiAnalyzer to restrict administrative access from specific locations?

A. Configure trusted hosts for that administrator.
B. Enable geo-location services on accessible interface.
C. Configure two-factor authentication with a remote RADIUS server.
D. Configure an ADOM for respective location.

Answer: A

NEW QUESTION 100
For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

A. Principal
B. Service provider
C. Identity collector
D. Identity provider

Answer: BD

NEW QUESTION 103
For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:

A. Use DNS

B. Use host name resolution
C. Use real-time forwarding
D. Use an NTP server

Answer: D

NEW QUESTION 104

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

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

Answer: B

NEW QUESTION 105

What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)

A. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
B. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer.
C. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date.
D. Make sure all endpoints are reachable by FortiAnalyzer.

Answer: BC

NEW QUESTION 107

An administrator fortinet, is able to view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mall server that can be used to send email.
What could be the problem?

A. Fortinet is assigned the Standard_ User administrator profile.
B. A trusted host is configured.
C. ADOM mode is configured with Advanced mode.
D. Fortinet is assigned the Restricted_ User administrator profile.

Answer: A

NEW QUESTION 112

Refer to the exhibit.
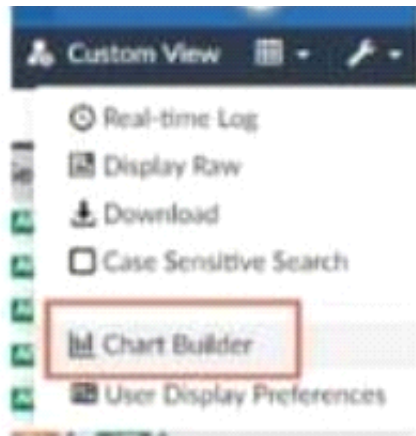
What is the purpose of using the Chart Builder feature on FortiAnalyzer?

A. In Log View, this feature allows you to build a dataset and chart automatically, based on the filtered search results.
B. In Log View, this feature allows you to build a chart and chart automatically, on the top 100 log entries.
C. This feature allows you to build a chart under FortiView.
D. You can add charts to generated reports using this feature.

Answer: A

NEW QUESTION 116

You are using RAID with a FortiAnalyzer that supports software RAID, and one of the hard disks on FortiAnalyzer has failed.
What is the recommended method to replace the disk?

A. Shut down FortiAnalyzer and then replace the disk
B. Downgrade your RAID level, replace the disk, and then upgrade your RAID level
C. Clear all RAID alarms and replace the disk while FortiAnalyzer is still running
D. Perform a hot swap

Answer: A

Explanation:

supports hot swapping on hardware RAID only, so it is recommended that on FortiAnalyzer devices with software RAID you should shutdown FortiAnalyzer prior to exchanging the hard disk.

https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta-

NEW QUESTION 117
FortiAnalyzer centralizes which functions? (Choose three)

A. Network analysis
B. Graphical reporting
C. Content archiving / data mining
D. Vulnerability assessment
E. Security log analysis / forensics

Answer: BCE

NEW QUESTION 118
......

Relate Links

100% Pass Your NSE5_FAZ-7.0 Exam with Exambible Prep Materials

https://www.exambible.com/NSE5_FAZ-7.0-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/

Relate Links

100% Pass Your NSE5_FAZ-7.0 Exam with Exambible Prep Materials

https://www.exambible.com/NSE5_FAZ-7.0-exam/