Fortinet

Exam Questions NSE5_FAZ-7.0

Fortinet NSE 5 - FortiAnalyzer 7.0

NEW QUESTION 1
Which SQL query is in the correct order to query the database in the FortiAnslyzer?

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:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 259: The main clauses FortiAnalyzer reports use are as follows:
•FROM
•WHERE
•GROUP BY
•ORDER BY
• LIMIT
• OFFSET
Accordingly, following the SELECT keyword, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide.

NEW QUESTION 2
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

NEW QUESTION 3
What must you consider when using log fetching? (Choose two.)

A. The fetch client can retrieve logs from devices that are not added to its local Device Manager
B. You can use filters to include only logs from a single device.
C. The fetching profile must include a user with the Super_User profile.
D. The archive logs retrieved from the server become archive logs in the client.

Answer: BC

NEW QUESTION 4
A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed by that rogue administrator on FortiAnalyzer.
What can you do on FortiAnalyzer to accomplish this?

A. Click FortiView and generate a report for that administrator.
B. Click Task Monitor and view the tasks performed by that administrator.
C. Click Log View and generate a report for that administrator.
D. View the tasks performed by the rogue administrator in Fabric View.

Answer: B

NEW QUESTION 5
What is the purpose of using prefilters when configuring event handlers?

A. They limit which logs are checked for matches by the other filters.
B. They can filter the logs before they are processed by FortiAnalyzer
C. They download new filters to be used in event handlers.
D. They are common filters applied simultaneously to all event handlers.

Answer: A

NEW QUESTION 6
What statements are true regarding the "store and upload" log transfer option between FortiAnalyzer and FortiGate? (Choose three.)

A. All FortiGates can send logs to FortiAnalyzer using the store and upload option.
B. Only FortiGate models with hard disks can send logs to FortiAnalyzer using the store and upload option.
C. Both secure communications methods (SSL and IPsec) allow the store and upload option.
D. Disk logging is enabled on the FortiGate through the CLI only.
E. Disk logging is enabled by default on the FortiGate.

Answer: BCD

NEW QUESTION 7

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 8
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 9
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 10
Which statement describes online logs on FortiAnalyzer?

A. Logs that reached a specific size and were rolled over
B. Logs that can be used to create reports
C. Logs that can be viewed using Log Browse
D. Logs that are saved to disk, compressed, and available in FortiView

Answer: C

NEW QUESTION 10
After generating a report, you notice the information you were expecting to see is not included in it. What are two possible reasons for this scenario? (Choose two.)

A. You enabled auto-cache with extended log filtering.
B. The logfiled service has not indexed all the expected logs.
C. The logs were overwritten by the data retention policy.
D. The time frame selected in the report is wrong.

Answer: BC

NEW QUESTION 13
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 16
Which two statement are true regardless initial Logs sync and Log Data Sync for Ha on FortiAnalyzer?

A. By default, Log Data Sync is disabled on all backup devise.
B. Log Data Sync provides real-time log synchronization to all backup devices.
C. With initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.
D. When Logs Data Sync is turned on, the backup device will reboot and then rebuilt the log database with the synchronized logs.

Answer: CD

NEW QUESTION 18
Which statement describes a dataset in FortiAnalyzer?

A. They determine what data is retrieved from the databas
B. They provide the layout used for reports.
C. They are used to set the data included in template
D. They define the chart types to be used in report

Answer: A

NEW QUESTION 19
Which statement about the FortiSOAR management extension is correct?

A. It requires a FortiManager configured to manage FortiGate
B. It requires a dedicated FortiSOAR device or VM.
C. It does not include a limited trial by default.
D. It runs as a docker container on FortiAnalyzer

Answer: D

NEW QUESTION 23
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 28
Logs are being deleted from one of your ADOMs earlier that the configured setting for archiving in your data policy. What is the most likely problem?

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

Answer: C

Explanation:
https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG FAZ/1100_Storage/0017_Deleted%20device%20logs.htm
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automatic-deletion

NEW QUESTION 29
Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

A. FortiAnalyzer HA can function without VRR
B. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
C. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
D. All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
E. FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

Answer: BC

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 32

Why run the command diagnose sql status sqlplugind?

A. To list the current SQL processes running
B. To check what is the database log insertion status
C. To display the SOL query connections and hcache status
D. To view the current hcache size

Answer: C

NEW QUESTION 35
What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)

A. RADIUS
B. Local
C. LDAP
D. PKI
E. TACACS+

Answer: ACE

NEW QUESTION 38
After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the purpose of running the following CLI command?
execute sql-local rebuild-adom <new-ADOM-name>

A. To reset the disk quota enforcement to default
B. To remove the analytics logs of the device from the old database
C. To migrate the archive logs to the new ADOM
D. To populate the new ADOM with analytical logs for the moved device, so you can run reports

Answer: D

Explanation:

- Are the device's analytics logs required for reports in the *new* ADOM? If so, rebuild the new ADOM database:

```
# exe sql-local rebuild-adom <new-ADOM-name>
```

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 128: Are the device analytics logs required for reports in the new ADOM? If so, rebuild the new ADOM database

NEW QUESTION 40
What happens when the IOC breach detection engine on FortiAnalyzer finds web logs that match a blocklisted IP address?

A. The endpoint is marked as Compromised an
B. optionally, can be put in quarantine.
C. FortiAnalyzer flags the associated host for further analysis.
D. A new Infected entry is added for the corresponding endpoint.
E. The detection engine classifies those logs as Suspicious

Answer: A

NEW QUESTION 44
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 46
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?

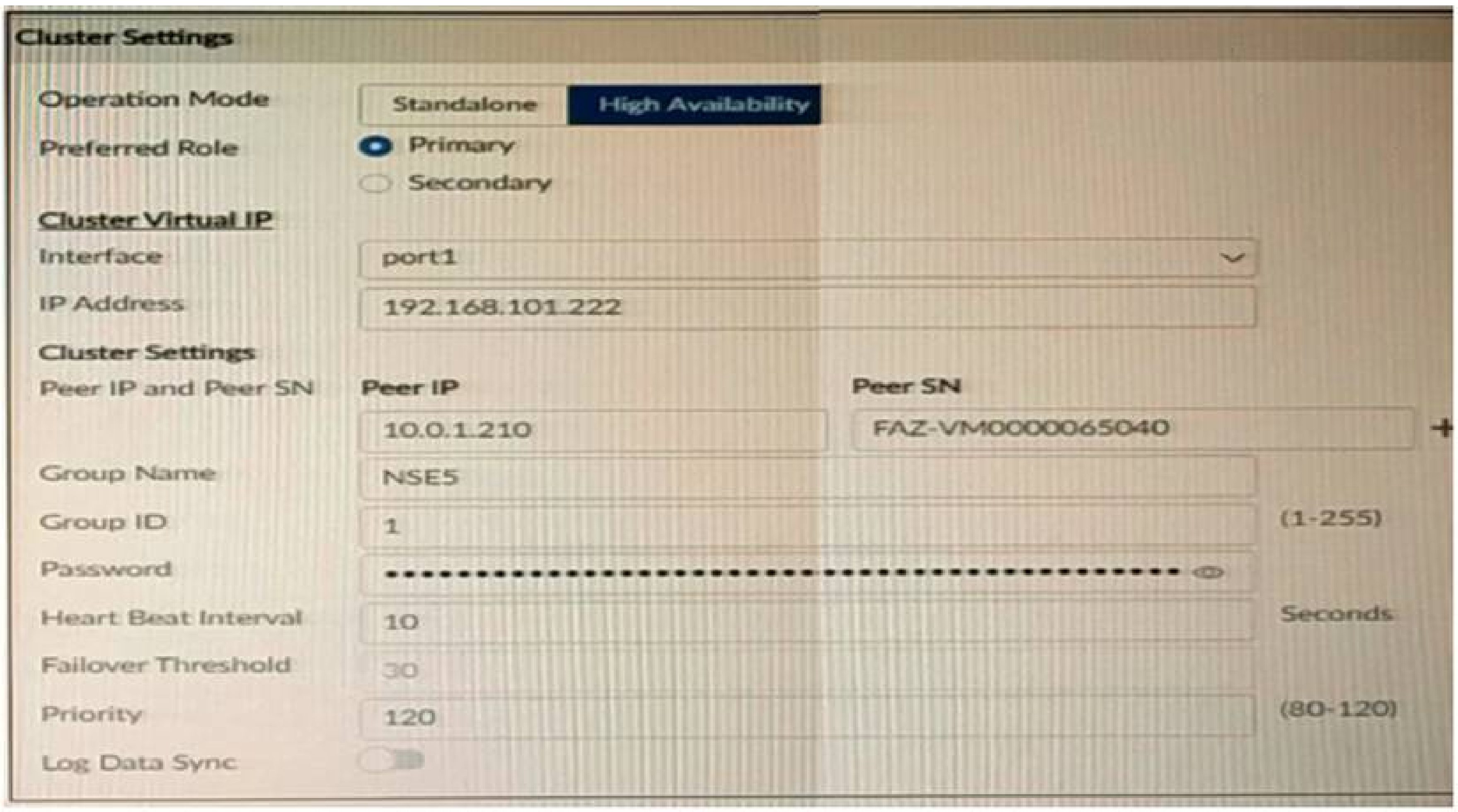
A. Fortinet is assigned the Standard_ User administrator profile.
B. A trusted host is configured.
C. ADOM mode is configured with Advanced mode.
D. Fortinet is assigned the Restricted_ User administrator profile.

Answer: A

Explanation:
• Super_User, which, like in FortiGate, provides access to all device and system privileges.
• Standard_User, which provides read and write access to device privileges, but not system privileges.
• Restricted_User, which provides read access only to device privileges, but not system privileges. Access to the Management extensions is also removed.

• No_Permissions_User, which provides no system or device privileges. Can be used, for example, to temporarily remove access granted to existing admins.
FortiAnalyzer_7.0_Study_Guide-Online page 42

NEW QUESTION 51
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 10.0.1.210 Peer SN 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

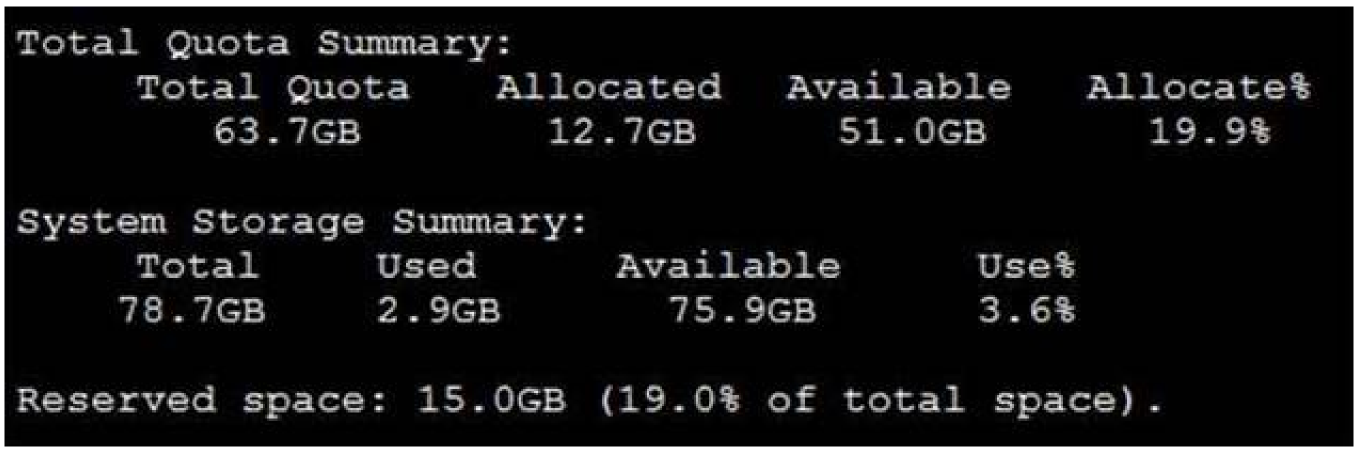
The image displays the configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster.
What can you conclude from the configuration displayed?

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: B

Explanation:
"If the preferred role is Primary, then this unit becomes the primary unit if it is configured first in a new HA cluster. If there is an existing primary unit, then this unit becomes a secondary unit." (https://docs.fortinet.com/document/fortianalyzer/7.0.5/administration-guide/275104)

NEW QUESTION 53
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).
```

Why is the total quota less than the total system storage?

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

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

NEW QUESTION 54
Which statement about the FortiSIEM management extension is correct?

A. Allows you to manage the entire life cycle of a threat or breach.
B. Its use of the available disk space is capped at 50%.
C. It requires a licensed FortiSIEM supervisor.

D. It can be installed as a dedicated VM.

Answer: A

NEW QUESTION 56
Which two statements are true regarding fabric connectors? (Choose two.)

A. Configuring fabric connectors to send notification to ITSM platform upon incident creation Is more efficient than third-party information from the FortiAnalyzer API.
B. Fabric connectors allow to save storage costs and improve redundancy.
C. Storage connector service does not require a separate license to send logs to cloud platform.
D. Cloud-Out connections allow you to send real-time logs to pubic cloud accounts like Amazon S3, Azure Blob , and Google Cloud.

Answer: AD

NEW QUESTION 60
Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

A. System information
B. Logs from registered devices
C. Report information
D. Database snapshot

Answer: AC

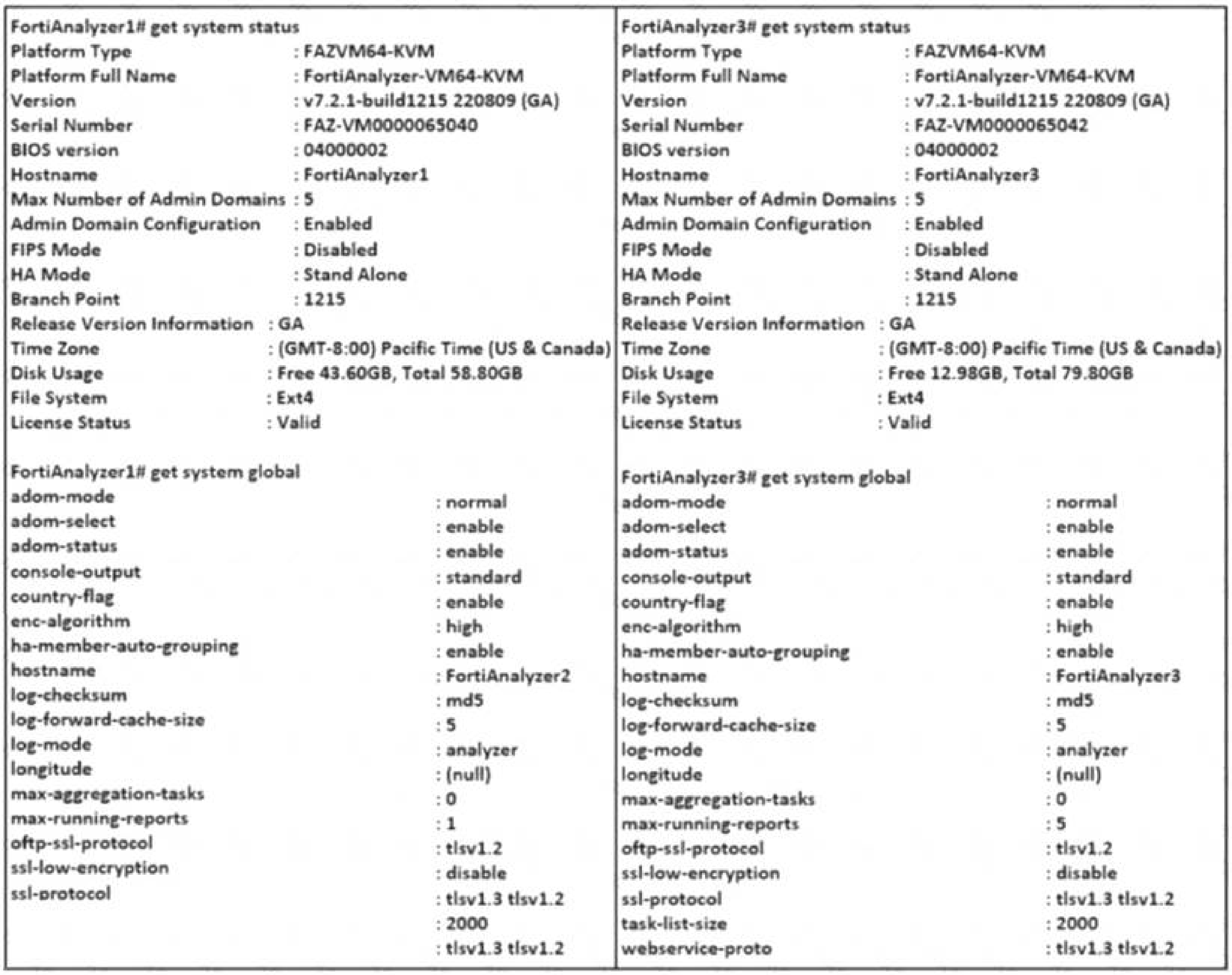
Explanation:
What does the System Configuration backup include?
System information, such as the device IP address and administrative user information. Device list, such as any devices you configured to allow log access. Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.
FortiAnalyzer_7.0_Study_Guide-Online pag. 29
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 29: What does the System Configuration backup include?
- System information, such as the device IP address and administrative user information
- Device list, such as any devices you configured to allow log access
- Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

NEW QUESTION 61
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 65
Refer to the exhibit.



```
FortiAnalyzer1# get system status
Platform Type                  : FAZVM64-KVM
Platform Full Name             : FortiAnalyzer-VM64-KVM
Version                        : v7.2.1-build1215 220809 (GA)
Serial Number                  : FAZ-VM0000065040
BIOS version                   : 04000002
Hostname                       : FortiAnalyzer1
Max Number of Admin Domains    : 5
Admin Domain Configuration     : Enabled
FIPS Mode                      : Disabled
HA Mode                        : Stand Alone
Branch Point                   : 1215
Release Version Information  : GA
Time Zone                    : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage                   : Free 43.60GB, Total 58.80GB
File System                  : Ext4
License Status               : Valid

FortiAnalyzer1# get system global
adom-mode                                 : normal
adom-select                               : enable
adom-status                               : enable
console-output                            : standard
country-flag                              : enable
enc-algorithm                             : high
ha-member-auto-grouping                   : enable
hostname                                  : FortiAnalyzer2
log-checksum                              : md5
log-forward-cache-size                    : 5
log-mode                                  : analyzer
longitude                                 : (null)
max-aggregation-tasks                     : 0
max-running-reports                       : 1
oftp-ssl-protocol                         : tlsv1.2
ssl-low-encryption                        : disable
ssl-protocol                              : tlsv1.3 tlsv1.2
                                          : 2000
                                          : tlsv1.3 tlsv1.2
```

```
FortiAnalyzer3# get system status
Platform Type                  : FAZVM64-KVM
Platform Full Name             : FortiAnalyzer-VM64-KVM
Version                        : v7.2.1-build1215 220809 (GA)
Serial Number                  : FAZ-VM0000065042
BIOS version                   : 04000002
Hostname                       : FortiAnalyzer3
Max Number of Admin Domains    : 5
Admin Domain Configuration     : Enabled
FIPS Mode                      : Disabled
HA Mode                        : Stand Alone
Branch Point                   : 1215
Release Version Information  : GA
Time Zone                    : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage                   : Free 12.98GB, Total 79.80GB
File System                  : Ext4
License Status               : Valid

FortiAnalyzer3# get system global
adom-mode                                 : normal
adom-select                               : enable
adom-status                               : enable
console-output                            : standard
country-flag                              : enable
enc-algorithm                             : high
ha-member-auto-grouping                   : enable
hostname                                  : FortiAnalyzer3
log-checksum                              : md5
log-forward-cache-size                    : 5
log-mode                                  : analyzer
longitude                                 : (null)
max-aggregation-tasks                     : 0
max-running-reports                       : 5
oftp-ssl-protocol                         : tlsv1.2
ssl-low-encryption                        : disable
ssl-protocol                              : tlsv1.3 tlsv1.2
task-list-size                            : 2000
webservice-proto                          : tlsv1.3 tlsv1.2
```

Based on the partial outputs displayed, which devices can be members of a FortiAnalyzer Fabric?

A. FortiAnalyzerl and FortiAnalyzer3
B. FortiAnalyzer1 and FortiAnalyzer2
C. All devices listed can be members
D. FortiAnalyzer2 and FortiAnalyzer3

Answer: C

NEW QUESTION 67
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:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigning-administrators-to

NEW QUESTION 70
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 71
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 75
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 80
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.

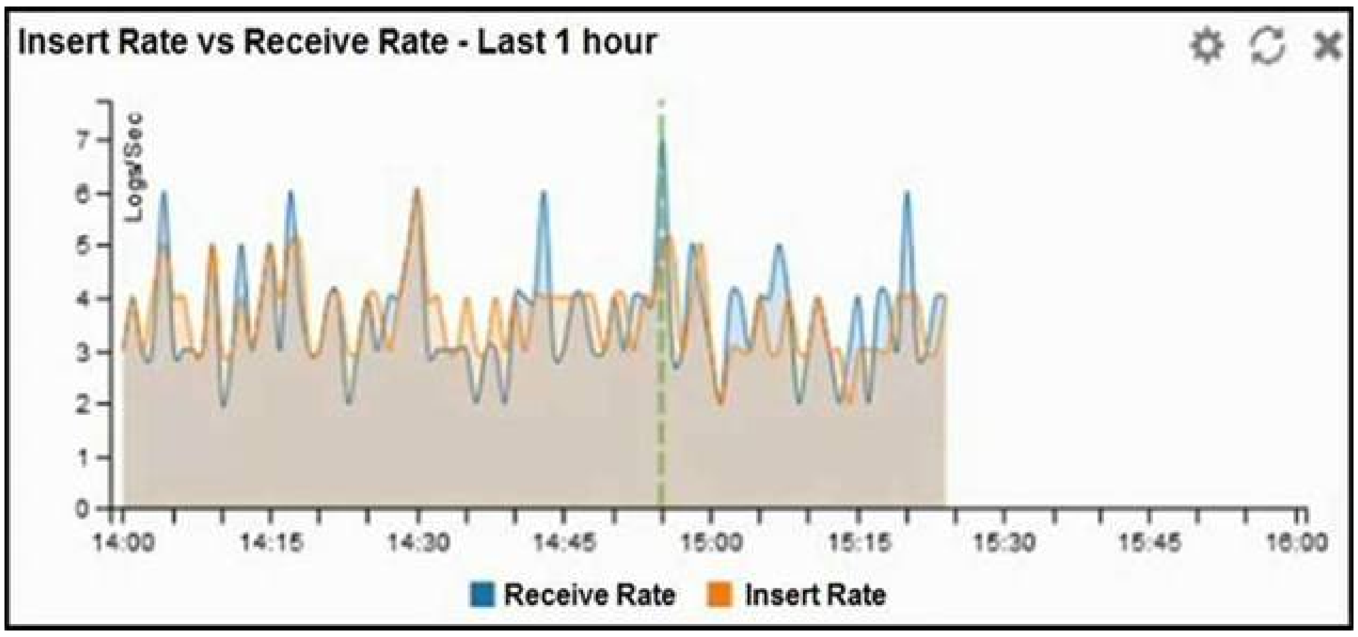
Answer: D

NEW QUESTION 81
What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

Answer: D

NEW QUESTION 86
Refer to the exhibit.

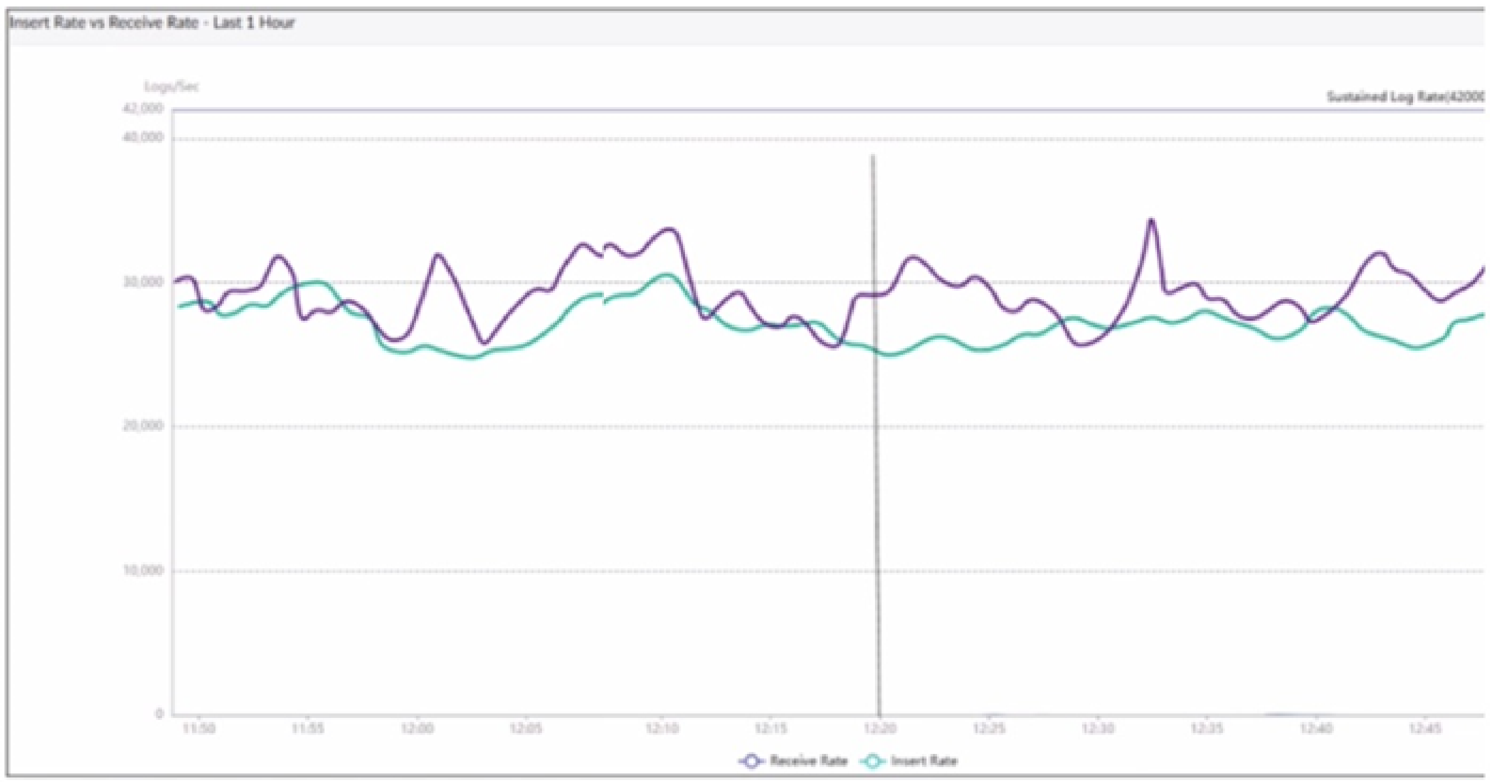


What does the data point at 14:55 tell you?

A. The received rate is almost at its maximum for this device
B. The sqlplugind daemon is behind in log indexing by two logs
C. Logs are being dropped
D. Raw logs are reaching FortiAnalyzer faster than they can be indexed

Answer: D

NEW QUESTION 90
Refer to the exhibit.

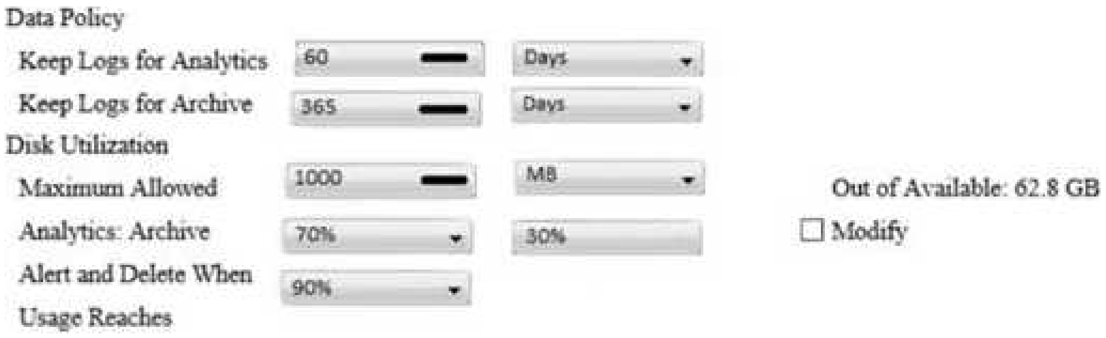


What does the data point at 12:20 indicate?

A. The performance of FortiAnalyzer is below the baseline.
B. FortiAnalyzer is using its cache to avoid dropping logs.
C. The log insert lag time is increasing.
D. The sqlplugind service is caught up with new logs.

Answer: C

NEW QUESTION 95
View the exhibit:



Data Policy

Keep Logs for Analytics	60	Days
Keep Logs for Archive	365	Days

Disk Utilization

Maximum Allowed	1000	MB	Out of Available: 62.8 GB
Analytics: Archive	70%	30%	□ Modify
Alert and Delete When Usage Reaches	90%		

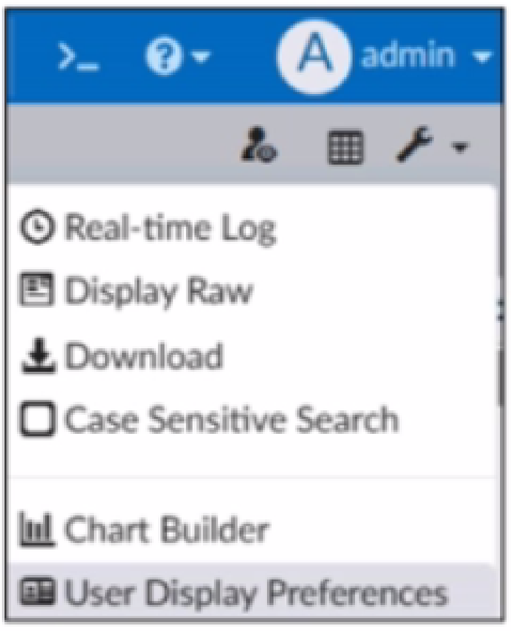
What does the 1000MB maximum for disk utilization refer to?

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:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-pol

NEW QUESTION 99
Refer to the exhibit.



What is the purpose of using the Chart Builder feature on FortiAnalyzer?

A. To add a new chart under FortiView to be used in new reports
B. To build a dataset and chart automatically, based on the filtered search results
C. To add charts directly to generate reports in the current ADOM

D. To build a chart automatically based on the top 100 log entries

Answer: B

NEW QUESTION 103
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

Explanation:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 217: Threat hunting consists in proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach will help administrator find any threats that might have eluded detection by the current security solutions or configurations.

NEW QUESTION 107
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: D

Explanation:
In the case of a primary device failure, FortiAnalyzer HA uses the following rules to select a new primary:
• All cluster devices are assigned a priority from 80 to 120. The default priority is 100. If the primary device becomes unavailable, the device with the highest priority is selected as the new primary device. For example, a device with a priority of 110 is selected over a device with a priority of 100.
• If multiple devices have the same priority, the device whose primary IP address has the greatest value is selected as the new primary device. For example, 123.45.67.124 is selected over 123.45.67.123.
• If a new device with a higher priority or a greater value IP address joins the cluster, the new device does not replace (or pre-empt) the current primary device automatically.
FortiAnalyzer_7.0_Study_Guide-Online page 62

NEW QUESTION 110
......