Number: NSE5_FAZ-7.2
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: NSE5_FAZ-7.2

Exam Name: Fortinet NSE 5 - FortiAnalyzer 7.2

Exam A

QUESTION 1
What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

A. Log correlation
B. Host name resolution
C. Log collection
D. Real-time forwarding

Correct Answer: A
Section:

QUESTION 2
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

Correct Answer: A, C
Section:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-asecurity-fabric-adom

QUESTION 3
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

Correct Answer: B
Section:
Explanation:
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMGFAZ/2300_Reports/0010_Predefined_reports.htm#:~:text=FortiAnalyzer%20includes%20a%20number%20of,create%20and%2For%20build%20reports.&text=A%20template%20populates%20the%20Layout,that%20is%20to%20be%20created.
https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMGFAZ/2300_Reports/0010_Predefined_reports.htm
Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.8/administrationguide/618245/predefined-reports-templates-charts-and-macros

QUESTION 4
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

Correct Answer: D
Section:

QUESTION 5
What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

Correct Answer: D
Section:
Explanation:
Reference: https://forum.fortinet.com/tm.aspx?m=143106

QUESTION 6
FortiAnalyzer uses the Optimized Fabric Transfer Protocok (OFTP) over SSL for what purpose?

A. To upload logs to an SFTP server
B. To prevent log modification during backup
C. To send an identical set of logs to a second logging server
D. To encrypt log communication between devices

Correct Answer: D
Section:

QUESTION 7
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

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

QUESTION 8

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.

Correct Answer: C
Section:
Explanation:
https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMGFAZ/1100_Storage/0017_Deleted%20device%20logs.htm
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automaticdeletion

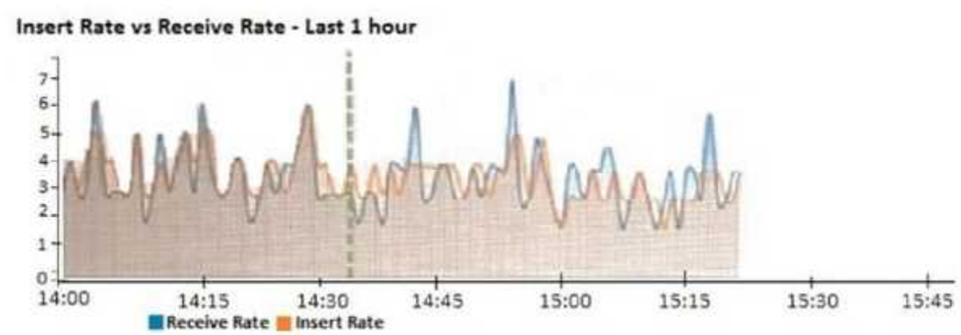
QUESTION 9
What is the purpose of the following CLI command?

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

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

Correct Answer: A
Section:
Explanation:
https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global

QUESTION 10
View the exhibit.



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.

Correct Answer: B
Section:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vsreceive-rate-widget

QUESTION 11
Which two methods are the most common methods to control and restrict administrative access on FortiAnalyzer? (Choose two.)

A. Virtual domains
B. Administrative access profiles
C. Trusted hosts
D. Security Fabric

Correct Answer: B, C
Section:
Explanation:
Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administrationguide/ 219292/administrator-profiles
https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/581222/trustedhosts

QUESTION 12
Which daemon is responsible for enforcing raw log file size?

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

Correct Answer: A
Section:

QUESTION 13
FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for analytics logs is 60 days.
What is the most likely problem?

A. Quota enforcement is acting on analytical data before a report is complete
B. Logs are rolling before the report is run
C. CPU resources are too high
D. Disk utilization for archive logs is set for 15 days

Correct Answer: B
Section:
Explanation:
Reference: https://forum.fortinet.com/tm.aspx?m=138806

QUESTION 14
Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

A. Antivirus logs
B. Web filter logs
C. IPS logs
D. Application control logs

Correct Answer: B
Section:
Explanation:
Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_hosts_page.htm?TocPath=FortiView%7CUsing%20FortiView%7C_____6

QUESTION 15
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

Correct Answer: A, B
Section:
Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD38567

QUESTION 16
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

Correct Answer: B, D
Section:
Explanation:
https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400_execute/backup.htm
Reference: https://help.fortinet.com/fauth/5-2/Content/Admin%20Guides/5_2%20Admin%20Guide/300/301_Dashboard.htm

QUESTION 17
Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

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

Correct Answer: A
Section:
Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD48500

`FROM` is the only mandatory clause required to form a `SELECT` statement; the rest of the clauses are optional and serve to filter or limit, aggregate or combine, and control the sort. It is also important to note that the clauses must be coded in a specific sequence. 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. For example, you can't use the `WHERE` clause before the `FROM` clause. You don't have to use all optional clauses, but whichever ones you do use must be in the correct sequence.

QUESTION 18
What is the purpose of a dataset query in FortiAnalyzer?

A. It sorts log data into tables
B. It extracts the database schema
C. It retrieves log data from the database
D. It injects log data into the database

Correct Answer: C
Section:
Explanation:
Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.4/administrationguide/148744/creating-datasets

QUESTION 19
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

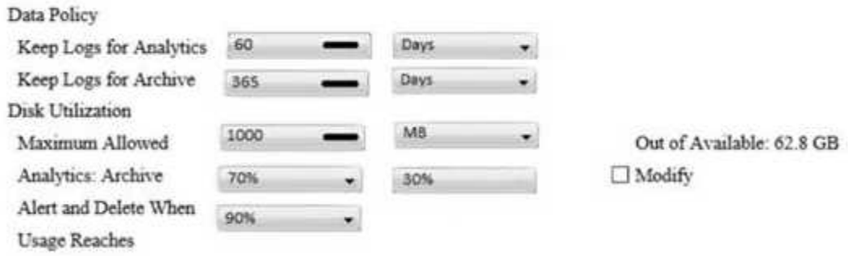
Correct Answer: D
Section:
Explanation:
Reference: https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMGFAZ/1100_Storage/0017_Deleted%20device%20logs.htm

QUESTION 20
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

Correct Answer: B, D
Section:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-spaceallocation

QUESTION 21
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

Correct Answer: B
Section:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuringlog-storage-policy

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.

Correct Answer: C
Section:
Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD40383

QUESTION 23
What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

A. The log file is stored as a raw log and is available for analytic support.
B. The log file rolls over and is archived.
C. The log file is purged from the database.
D. The log file is overwritten.

Correct Answer: B
Section:
Explanation:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6d9f8fb5-6cf4-11e9-81a4-00505692583a/FortiAnalyzer-6.0.5-Administration-Guide.pdf
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/355632/log-browse

QUESTION 24
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

Correct Answer: A
Section:
Explanation:
https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20(%22Redundant%20Array%20of%20Inexpensive,%2C%20performance%20improvement%2C%20or%20both.

QUESTION 25
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

Correct Answer: D
Section:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetchermanagement

QUESTION 26
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

Correct Answer: A
Section:
Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD40848

QUESTION 27
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.

Correct Answer: B
Section:
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
Reference: https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is-thedifference-between-log-forward-and-log-aggregation-modes

QUESTION 28
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

Correct Answer: B
Section:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigningadministrators-to-an-adom

QUESTION 29
In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required?
(Choose two.)

A. Remote logging must be enabled on FortiGate
B. Log encryption must be enabled
C. ADOMs must be enabled
D. FortiGate must be registered with FortiAnalyzer

Correct Answer: A, D
Section:
Explanation:
Pg 70: "after you add and register a FortiGate device with the FortiAnalyzer unit, you must also ensure that the FortiGate device is configured to send logs to the FortiAnalyzer unit."
https://docs.fortinet.com/uploaded/files/4614/FortiAnalyzer-5.4.6-Administration%20Guide.pdf
Pg 45: "ADOMs must be enabled to support the logging and reporting of NON-FORTIGATE devices, such as FortiCarrier, FortiClientEMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox."

QUESTION 30
What can the CLI command # diagnose test application oftpd 3 help you to determine?

A. What devices and IP addresses are connecting to FortiAnalyzer
B. What logs, if any, are reaching FortiAnalyzer
C. What ADOMs are enabled and configured

D. What devices are registered and unregistered

Correct Answer: A
Section:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/395556/test#test_application

QUESTION 31
What are the operating modes of FortiAnalyzer? (Choose two)

A. Standalone
B. Manager
C. Analyzer
D. Collector

Correct Answer: C, D
Section:

QUESTION 32
Which statements are correct regarding FortiAnalyzer reports? (Choose two)

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

Correct Answer: A, B
Section:

QUESTION 33
Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

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

Correct Answer: B
Section:

QUESTION 34
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

Correct Answer: B, C, E
Section:

QUESTION 35
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.

Correct Answer: C, D
Section:

QUESTION 36
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.

Correct Answer: A, D
Section:

QUESTION 37
What does the disk status Degraded mean for RAID management?

A. One or more drives are missing from the FortiAnalyzer unit. The drive is no longer available to the operating system.
B. The FortiAnalyzer device is writing to all the hard drives on the device in order to make the array fault tolerant.
C. The FortiAnalyzer device is writing data to a newly added hard drive in order to restore the hard drive to an optimal state.
D. The hard driveIs no longer being used by the RAID controller

Correct Answer: D
Section:

QUESTION 38
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.

Correct Answer: A

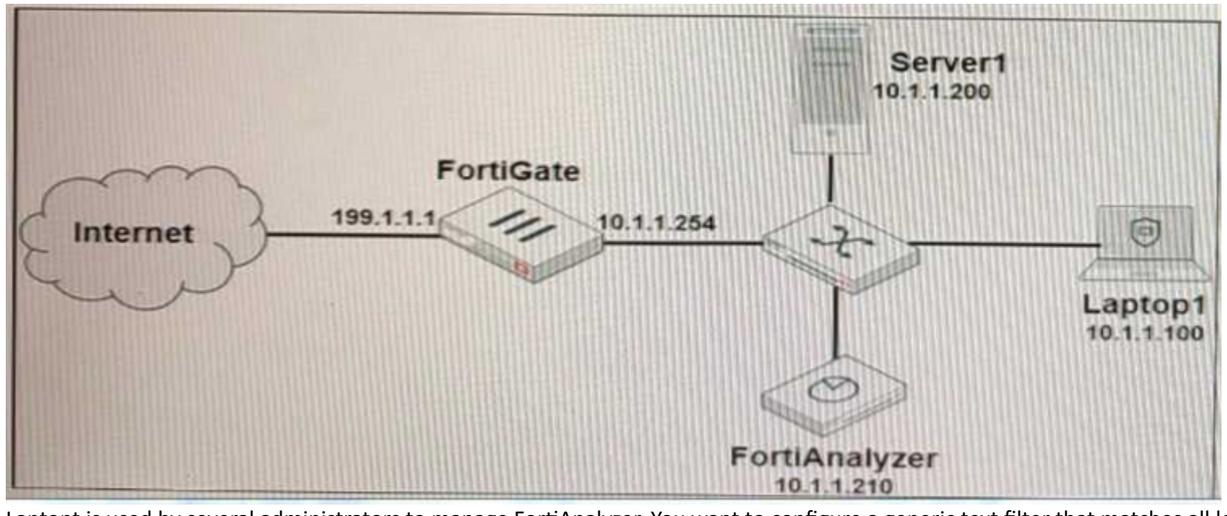
Section:
Explanation:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 64: To upgrade FortiAnalyzer HA cluster firmware:
1. Log in to each secondary device.
2. Upgrade the firmware of all secondary devices.
3. Wait for the upgrades to complete and verify that all secondary devices joined the cluster.
4. Verify that logs on all secondary devices are synchronized with the primary device.
5. Upgrade the primary device.
https://docs.fortinet.com/document/fortianalyzer/7.2.0/upgrade-guide/262607/upgrading-fortianalyzer-firmware

QUESTION 39
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

Correct Answer: B
Section:
Explanation:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 242: Output variables allow you to use the output from a preceding task as an input to the current task.
"Output variables allow you to use the output from a preceding task as an input to the current task." FortiAnalyzer_7.0_Study_Guide-Online page 242

QUESTION 40
Refer to the exhibit.



Laptopt is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin" and coming from Laptop1:
Which filter will achieve the desired result?

A. operation-login & performed_on=="GUI(10.1.1.100)" & user!=admin
B. operation-login & srcip==10.1.1.100 & dstip==10.1.1.210 & user==admin
C. operation-login & dstip==10.1.1.210 & userl-admin
D. operation-login & performed_on=="GUI(10.1.1.210)' & user!=admin

Correct Answer: A
Section:
Explanation:
On there the task was to create a filter for failed logins from any other location but the local computer: "Add the text performed_on!~10.0.1.10. This includes any attempts coming from devices with an IP address that is not the one configured on the Local-Client computer."

QUESTION 41
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

Correct Answer: D
Section:
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

QUESTION 42
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

Correct Answer: A
Section:
Explanation:
https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMGFAZ/0700_RAID/0800_Swapping%20Disks.htm#:~:text=If%20a%20hard%20disk%20on,to%20exchanging%20the%20hard%20disk.

QUESTION 43
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

Correct Answer: D
Section:
Explanation:

You can add more than one fabric connector, each with the same or different notification settings.
The receiving side of the connector must be configured for the notifications to be sent successfully.
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 34: Fabric connectors also enable FortiAnalyzer to send notifications to ITSM platforms when a new incident is created or for any subsequent updates.

QUESTION 44
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.

Correct Answer: D
Section:
Explanation:
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.
(Blank): Other scenarios.
FortiAnalyzer_7.0_Study_Guide-Online pag. 189.
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 189: Review the hardware requirements before you enable a management extension application. Some of them require a minimum amount of memory or a minimum number of CPU cores.

QUESTION 45
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

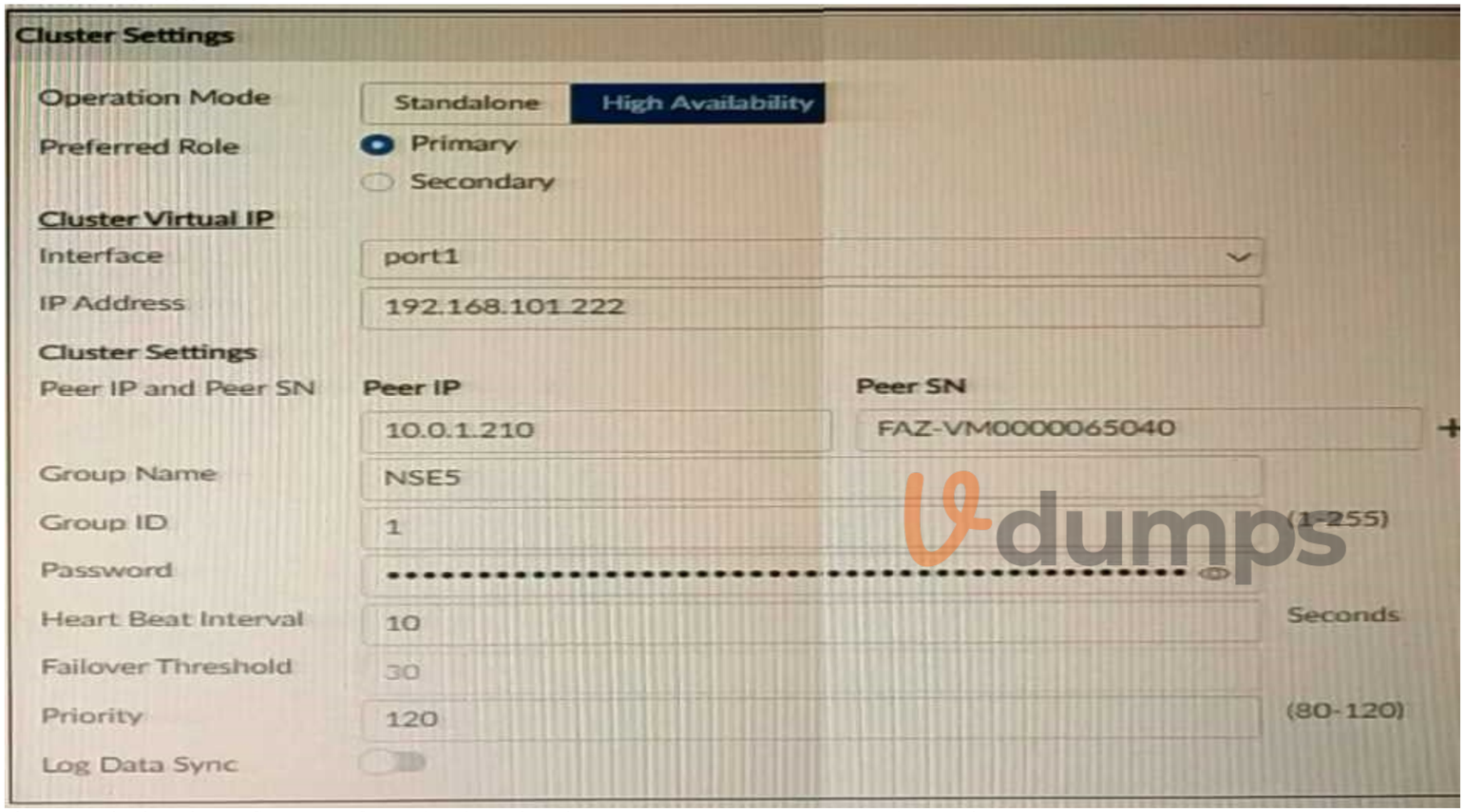
Correct Answer: B
Section:
Explanation:
Playbook jobs that include one or more failed tasks are labeled as Failed in Playbook Monitor.
FortiAnalyzer_7.0_Study Guide page No: 247
Playbook jobs that include one or more failed tasks are labeled as Failed in Playbook Monitor. A failed status, however, does not mean that all tasks failed. Some individual actions may have been completed successfully.

QUESTION 46
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

Correct Answer: C
Section:
Explanation:
Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.4/administrationguide/148744/creating-datasets
Datasets: Structured Query Language (SQL) SELECT queries that extract specific data from the database

QUESTION 47
Refer to the exhibit.



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.

Correct Answer: B
Section:
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)

QUESTION 48

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

Correct Answer: B
Section:
Explanation:
"One possible scenario is shown on the slide:
1. Traffic flows through the FortiGate
2. FortiGate sends logs to FortiAnalyzer
3. FortiAnalyzer detects some suspicious traffic and generates an event
4. The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate so that it runs an automation stitch
5. FortiGate runs the automation stitch with the corrective or preventive actions" FortiAnalyzer_7.0_Study_Guide-Online page 228 In order to see the actions related to the FOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on the FortiGate side. FortiAnalyzer_7.0_Study Guide page no 233

QUESTION 49
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

Correct Answer: B
Section:
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.

QUESTION 50
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.

Correct Answer: B, C
Section:

QUESTION 51
Which two statements are true regarding the outbreak detection service? (Choose two.)

A. New alerts are received by email.

B. Outbreak alerts are available on the root ADOM only.
C. An additional license is required.
D. It automatically downloads new event handlers and reports.

Correct Answer: C, D
Section:

QUESTION 52
What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

A. The size of newly generated reports is optimized to conserve disk space.
B. FortiAnalyzer local cache is used to store generated reports.
C. When new logs are received, the hard-cache data is updated automatically.
D. The generation time for reports is decreased.

Correct Answer: C, D
Section:

QUESTION 53
Why must you wait for several minutes before you run a playbook that you just created?

A. FortiAnalyzer needs that time to parse the new playbook.
B. FortiAnalyzer needs that time to back up the current playbooks.
C. FortiAnalyzer needs that time to ensure there are no other playbooks running.
D. FortiAnalyzer needs that time to debug the new playbook.

Correct Answer: A
Section:

QUESTION 54
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

Correct Answer: C
Section:

QUESTION 55
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

Correct Answer: B
Section:

QUESTION 56
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

Correct Answer: B
Section:

QUESTION 57
What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server?
(Choose two.)

A. SFTP, FTP, or SCP server
B. Mail server
C. Output profile
D. Report scheduling

Correct Answer: A, C
Section:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creatingoutput-profiles

QUESTION 58
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

Correct Answer: B
Section:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-spaceallocation

QUESTION 59
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+

Correct Answer: A, C, E
Section:

QUESTION 60
What statements are true regarding disk log quota? (Choose two)

A. The FortiAnalyzer stops logging once the disk log quota is met.
B. The FortiAnalyzer automatically sets the disk log quota based on the device.
C. The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.
D. The FortiAnalyzer disk log quota is configurable, but has a minimum o 100mb a maximum based on the reserved system space.

Correct Answer: C, D
Section:

QUESTION 61
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.

Correct Answer: A, B
Section:

QUESTION 62
How can you attach a report to an incident?

A. By attaching it to an event handler alert
B. By editing the settings of the desired report
C. From the properties of an existing incident
D. Saving it in JSON format, and then importing it

Correct Answer: C
Section:

QUESTION 63
Which item must you configure on FortiAnalyzer to email generated reports automatically?

A. Output profile
B. Report scheduling
C. SFTP server
D. SNMP server

Correct Answer: A
Section:

QUESTION 64
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

Correct Answer: D
Section:

QUESTION 65
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.

Correct Answer: B, C
Section:

QUESTION 66
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.

Correct Answer: A
Section:

QUESTION 67
Which statement describes a dataset in FortiAnalyzer?

Correct Answer: A
Section:

QUESTION 68
A playbook contains five tasks in total. An administrator runs the playbook and four out of five tasks finish successfully, but one task fails. What will be the status of the playbook after it is run?

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

Correct Answer: B
Section:

QUESTION 69
What is the purpose of trigger variables?

A. To display statistics about the playbook runtime
B. To use information from the trigger to filter the action in a task
C. To provide the trigger information to make the playbook start running
D. To store the start times of playbooks with On_Schedule triggers

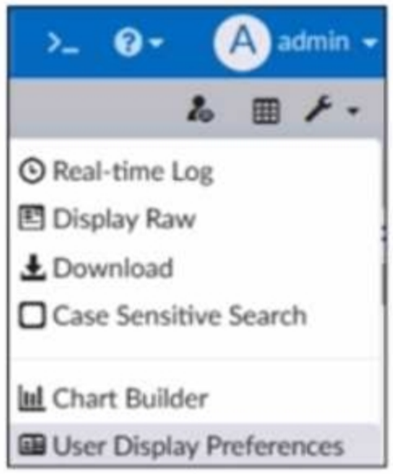
Correct Answer: B
Section:

QUESTION 70
Which statement about sending notifications with incident updates is true?

A. Notifications can be sent only when an incident is created or deleted.
B. You must configure an output profile to send notifications by email.
C. Each incident can send notifications to a single external platform.
D. Each connector used can have different notification settings.

Correct Answer: D
Section:

QUESTION 71
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

Correct Answer: B
Section:

QUESTION 72
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 and. optionally, can be put in quarantine.
B. FortiAnalyzer flags the associated host for further analysis.
C. A new Infected entry is added for the corresponding endpoint.
D. The detection engine classifies those logs as Suspicious

Correct Answer: A
Section:

QUESTION 73
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

Correct Answer: C
Section:

QUESTION 74
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.

Correct Answer: C
Section:

QUESTION 75
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.

Correct Answer: A
Section:
Explanation:

QUESTION 76
An administrator has configured the following settings:
config system global
set log-checksum md5-auth
end
What is the significance of executing this command?

A. This command records the log file MD5 hash value.
B. This command records passwords in log files and encrypts them.
C. This command encrypts log transfer between FortiAnalyzer and other devices.
D. This command records the log file MD5 hash value and authentication code.

Correct Answer: D
Section:
Explanation:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.4.6/administrationguide/410387/appendix-b-log-integrity-and-secure-log-transfer

QUESTION 77
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

Correct Answer: A, B
Section:
Explanation:
Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.2/administrationguide/598322/creating-output-profiles

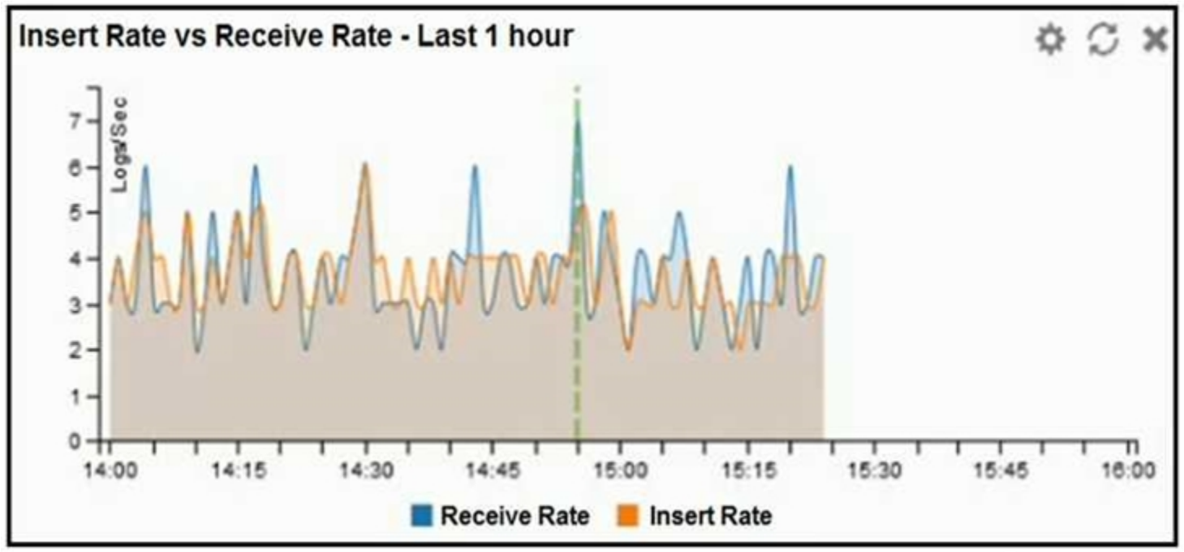
QUESTION 78
For which two purposes would you use the command set log checksum? (Choose two.)

A. To help protect against man-in-the-middle attacks during log upload from FortiAnalyzer to an SFTP server
B. To prevent log modification or tampering
C. To encrypt log communications
D. To send an identical set of logs to a second logging server

Correct Answer: A, B
Section:
Explanation:
To prevent logs from being tampered with while in storage, you can add a log checksum using the config system global command. You can configure FortiAnalyzer to record a log file hash value, timestamp, and authentication

code when the log is rolled and archived and when the log is uploaded (if that feature is enabled). This can also help against man-in-the-middle only for the transmission from FortiAnalyzer to an SSH File Transfer Protocol (SFTP) server during log upload.
FortiAnalyzer_7.0_Study_Guide-Online page 149

QUESTION 79
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

Correct Answer: D
Section:

QUESTION 80
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

Correct Answer: A
Section:
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/tap/194997?externalID=FD41397#:~:text=If%20a%20hard%20disk%20on,process%20known%20as%20hot%20swapping

QUESTION 81
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

Correct Answer: C
Section:
Explanation:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4cb0dce6-dbef-11e9-8977-00505692583a/FortiAnalyzer-5.6.10-Administration-Guide.pdf (40)

QUESTION 82
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

Correct Answer: D
Section:
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"

QUESTION 83
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

Correct Answer: D
Section:

QUESTION 84
Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?

A. To properly correlate logs
B. To use real-time forwarding

C. To resolve host names
D. To improve DNS response times

Correct Answer: A
Section:
Explanation:

- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server for proper log correlation

QUESTION 85
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

Correct Answer: B
Section:
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.

QUESTION 86
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

Correct Answer: D
Section:
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

QUESTION 87
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

Correct Answer: D
Section:
Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiManager%20devices%20that,to%20exchanging%20the%20hard%20disk.
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.
Reference: https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/tap/194997?externalID=FD41397#:~:text=If%20a%20hard%20disk%20on,process%20known%20as%20hot%20swapping

QUESTION 88
If you upgrade the FortiAnalyzer firmware, which report element can be affected?

A. Custom datasets
B. Report scheduling
C. Report settings
D. Output profiles

Correct Answer: A
Section:
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/upgrade-guide/669300/checking-reports

QUESTION 89
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

Correct Answer: C
Section:

QUESTION 90
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

Correct Answer: A, C
Section:
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.

QUESTION 91
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.

Correct Answer: B, D
Section:
Explanation:
If the imported playbook has the same name as an existing one, FortiAnalyzer will create a new name that includes a timestamp to avoid conflicts.
Playbooks are imported with the same status they had (enabled or disabled) when they were exported.
Playbooks set to run automatically should be exported while they are disabled to avoid unintended runs on the destination.

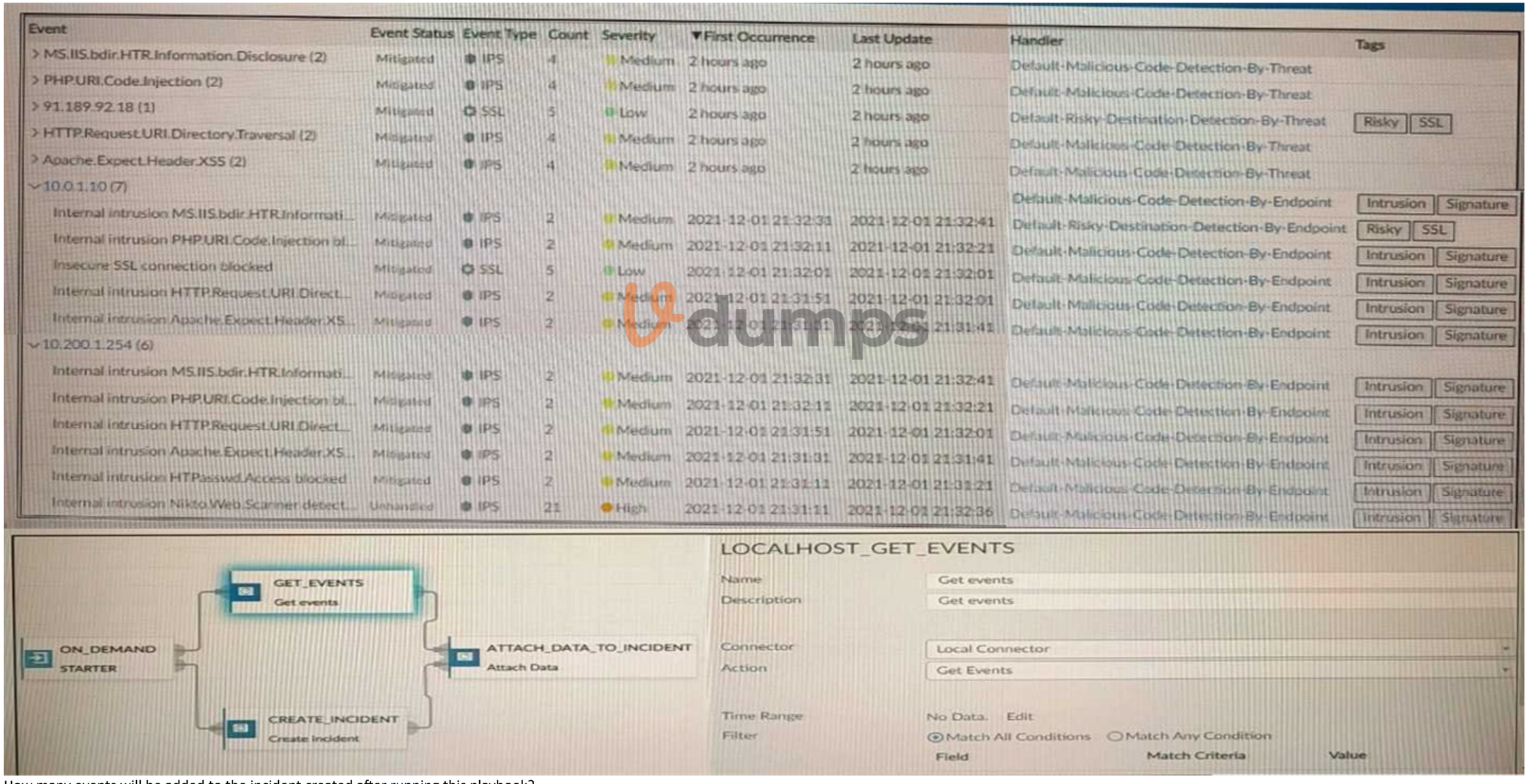
QUESTION 92
Which SQL query is in the correct order to query the database in the FortiAnslyzer?

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

Correct Answer: C
Section:
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.

QUESTION 93
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.

Correct Answer: A
Section: