Fortinet

Exam Questions NSE5_FAZ-7.2

Fortinet NSE 5 - FortiAnalyzer 7.2

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
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

Answer: D

NEW QUESTION 2
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 3
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

Answer: AC

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creating-output-profiles

NEW QUESTION 4
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

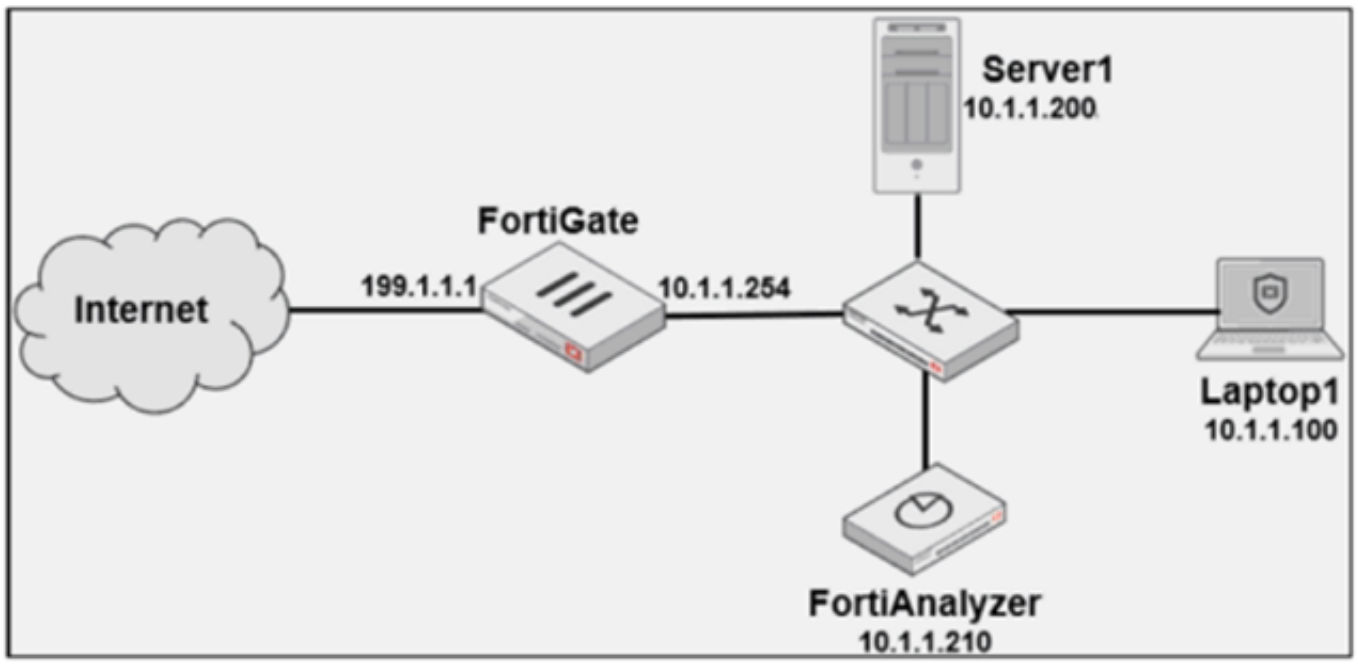
NEW QUESTION 5
For which two purposes would you use the command set log checksum? (Choose two.)

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

Answer: AB

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

NEW QUESTION 6
Refer to the exhibit.



Laptop1 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 & dstip==10.1.1.210 & user!-admin
B. operation-login & srcip==10.1.1.100 & dstip==10.1.1.210 & user==admin
C. operation-login & performed_on=="GUI(10.1.1.210)" & user!=admin
D. operation-login & performed_on=="GUI(10.1.1.100)" & user!=admin

Answer: D

NEW 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

Answer: C

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

NEW QUESTION 8
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.

Answer: D

NEW QUESTION 9
By default, what happens when a log file reaches its maximum file size?

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

Answer: C

NEW QUESTION 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 10
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: BD

Explanation:
Option B is correct because you must establish an IPsec tunnel ID and pre-shared key to secure the communication between FortiAnalyzer and FortiGate with IPsec12. The tunnel ID is a unique identifier for each tunnel and the pre-shared key is a secret passphrase that authenticates the peers.
Option D is correct because IPsec is only enabled through the CLI on FortiAnalyzer1. You cannot configure IPsec settings through the GUI on FortiAnalyzer.

NEW QUESTION 15
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 17
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

Answer: BC

NEW QUESTION 18
Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

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

Answer: A

NEW QUESTION 20
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 21
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 25
Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

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

Answer: B

NEW QUESTION 27
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

Answer: B

NEW QUESTION 31
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 36
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

Answer: C

NEW QUESTION 41
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 45
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

Answer: C

NEW QUESTION 48
Which statement is true regarding Macros on FortiAnalyzer?

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

Answer: A

Explanation:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 283: Note that macros are ADOM-specific and supported in FortiGate and FortiCarrier ADOMs only.

NEW QUESTION 52
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 56
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 60
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

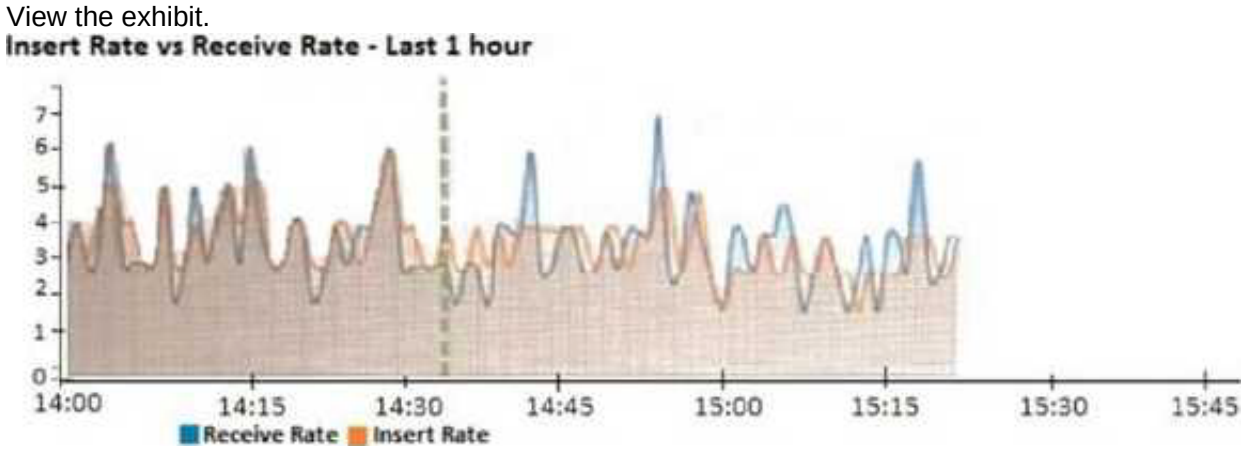
Explanation:
https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20(%22Redundant%20Array%20of%20Inexpensive,%2C%

NEW QUESTION 62
Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)

A. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.
B. Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.
C. Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.
D. Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.

Answer: BD

NEW QUESTION 66
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.

Answer: B

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

NEW QUESTION 69
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: B

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.

NEW QUESTION 74
Which statement correctly describes the management extensions available on FortiAnalyzer?

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

Answer: D

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.

NEW QUESTION 79
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 83
Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate to FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

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

Answer: AB

NEW QUESTION 88
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

Answer: B

NEW QUESTION 89
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 93
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 94
You crested a playbook on FortiAnalyzer that uses a FortiOS connector
When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?

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

Answer: B

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

NEW QUESTION 96
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 98
An administrator has moved FortiGate A from the root ADOM to ADOM1. However, the administrator is not able to generate reports for FortiGate A in ADOM1.
What should the administrator do to solve this issue?

A. Use the execute sql-local rebuild-db command to rebuild all ADOM databases.
B. Use the execute sql-local rebuild-adom ADOM1 command to rebuild the ADOM database.
C. Use the execute sql-report run ADOM1 command to run a report.
D. Use the execute sql-local rebuild-adom root command to rebuild the ADOM database.

Answer: B

NEW QUESTION 103
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 106
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 110
Refer to the exhibit.

Event	Event Status	Event Type	Count	Severity
151.101.54.62 (1)				
Insecure SSL Connection blocked from 10.0.3.20	Mitigated	SSL	1	Low

Which statement is correct regarding the event displayed?

A. The security risk was blocked or dropped.
B. The security event risk is considered open.
C. An incident was created from this event.
D. The risk source is isolated.

Answer: A

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. 206

NEW QUESTION 115
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.

Answer: CD

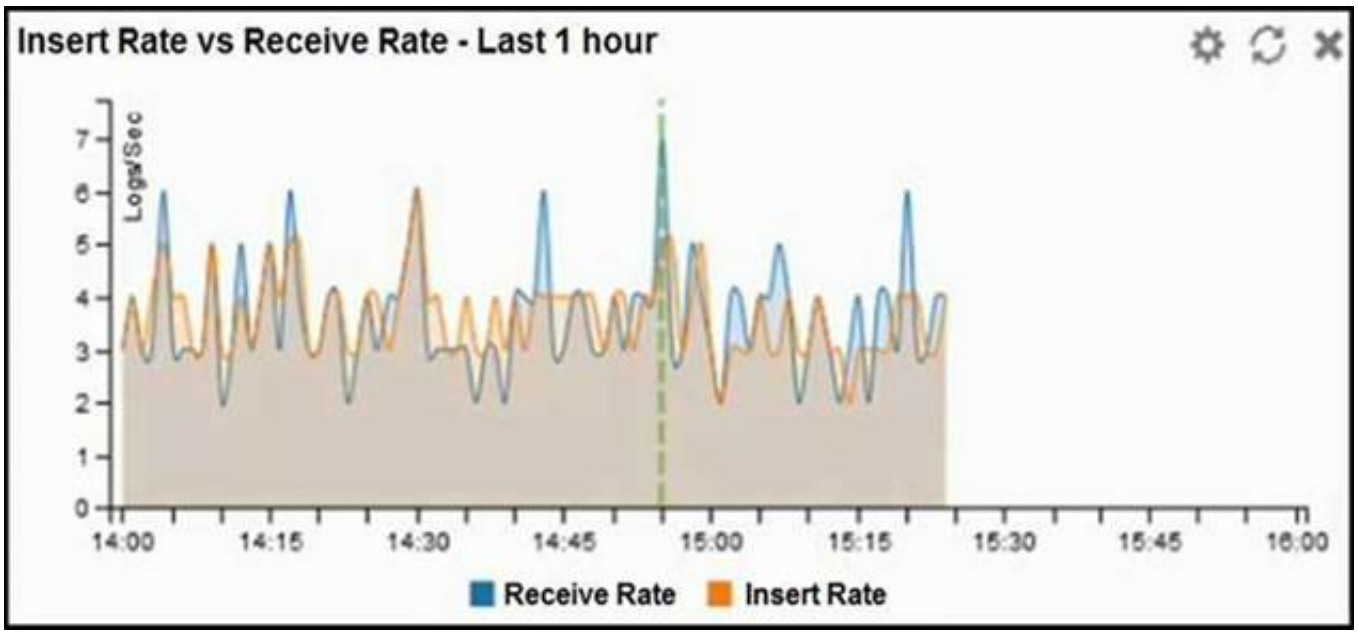
NEW QUESTION 117
For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:

A. Use DNS
B. Use host name resolution
C. Use real-time forwarding

D. Use an NTP server

Answer: D

NEW QUESTION 122
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 123
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.

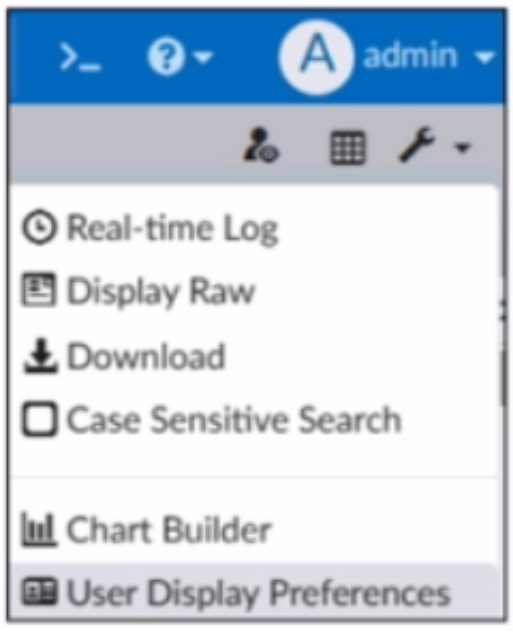
Answer: D

NEW QUESTION 124
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 126
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 127
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

Answer: A

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

NEW QUESTION 132
.....

Relate Links

100% Pass Your NSE5_FAZ-7.2 Exam with Exambible Prep Materials

https://www.exambible.com/NSE5_FAZ-7.2-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/