Number: NSE5_FAZ-7.2
Passing Score: 800
Time Limit: 120 min
File Version: 3.0

Exam Code: NSE5_FAZ-7.2

Exam Name: Fortinet NSE 5 - FortiAnalyzer 7.2

Exam A

QUESTION 1
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 ADOM. you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.
D. Normal mode is the default ADOM mode.

Correct Answer: C, D
Section:
Explanation:
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-1/FMGFAZ/0800_ADOMs/0400_ADOM%20Device%20Modes.htm

QUESTION 2
Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two.)
A. Both modes, forwarding and aggregation, support encryption of logs between devices.
B. In aggregation mode, you can forward logs to syslog and CEF servers as well.
C. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
D. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.

Correct Answer: A, C
Section:
Explanation:
A) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 148: The log communication between devices can be protected by encryption, with the desired encryption level, using the commands shown on the slide. (You need to interpret this. "Real time" and "aggregation" is about the "moment" when Fortigate sends the logs. However, no matter the moment, Fortigate will upload logs encrypted or unencrypted based on previous / differente config).
C) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 147: Aggregation: Logs and content files stored and uploaded at scheduled time.

QUESTION 3
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.

Correct Answer: B
Section:
Explanation:
Reference: https://help.fortinet.com/fmgr/cli/5-6-1/FortiManager_CLI_Reference/700_execute/sqllocal+.
htm

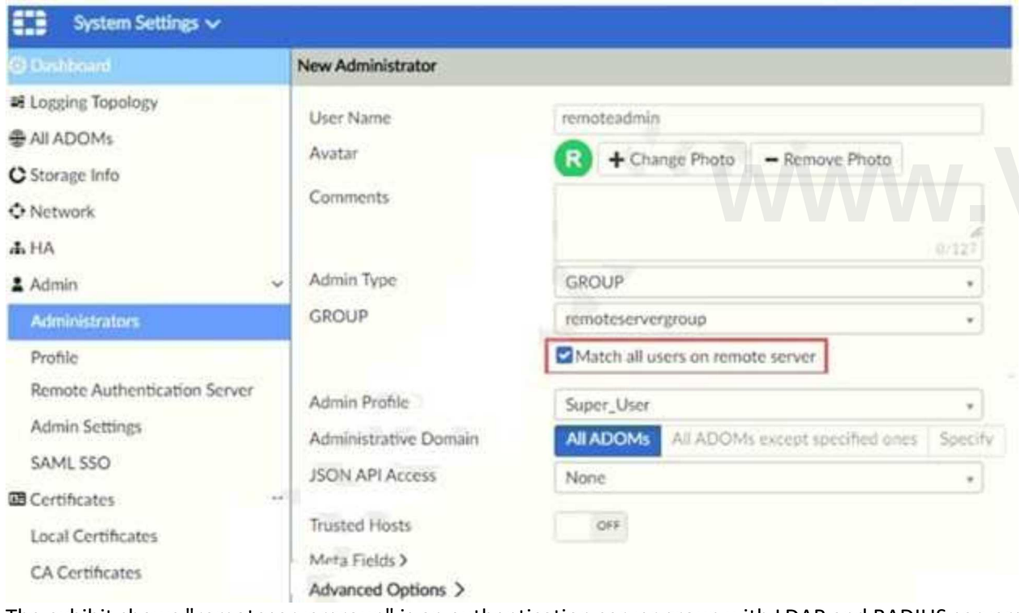
QUESTION 4
Which statement is true regarding Macros on FortiAnalyzer?
A. Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.
B. Macros are supported only on the FortiGate ADOM.
C. Macros are useful in generating excel log files automatically based on the reports settings.
D. Macros are predefined templates for reports and cannot be customized.

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

QUESTION 5
Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)
A. When in collector mode, FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.
B. Collector mode is the default operating mode.
C. When in collector mode. FortiAnalyzer supports event management and reporting features.
D. By deploying different FortiAnalyzer devices with collector and analyzer mode in a network, you can improve the overall performance of log receiving, analysis, and reporting

Correct Answer: A, D
Section:
Explanation:
Reference: https://docs.fortinet.com/document/fortianalyzer/7.0.0/administrationguide/227478/collector-mode
https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/312644/analyzercollector-collaboration

QUESTION 6
Refer to the exhibit.



The exhibit shows "remoteservergroup" is an authentication server group with LDAP and RADIUS servers.
Which two statements express the significance of enabling "Match all users on remote server" when configuring a new administrator? (Choose two.)
A. It creates a wildcard administrator using LDAP and RADIUS servers.
B. Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.
C. Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at anytime.
D. It allows administrators to use two-factor authentication.

Correct Answer: A, B
Section:
Explanation:
Reference: https://docs.fortinet.com/document/fortimanager/7.0.1/administrationguide/858351/creating-administrators

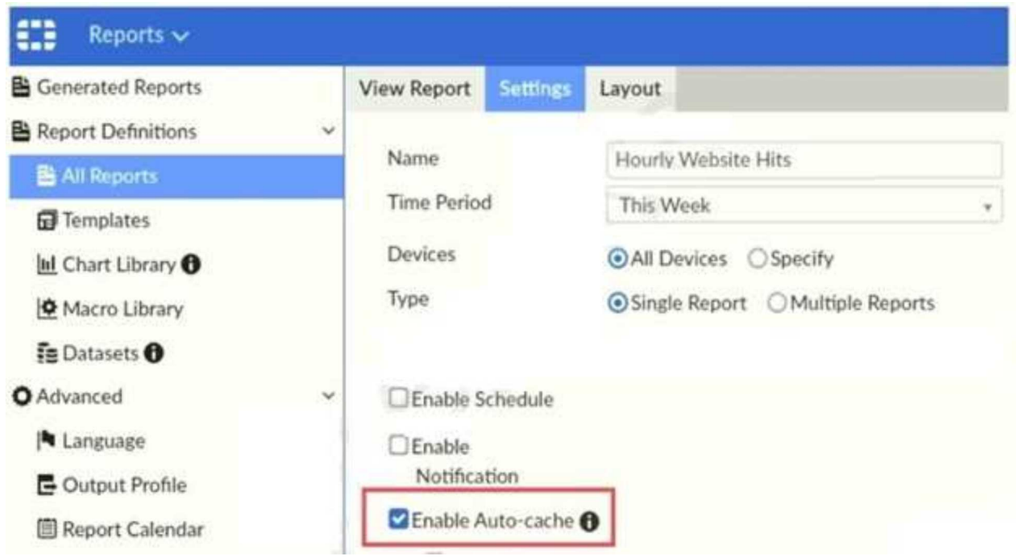
QUESTION 7
A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed by that rogue administrator on FortiAnalyzer.
What can you do on FortiAnalyzer to accomplish this?
A. Click FortiView and generate a report for that administrator.
B. 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.

Correct Answer: B
Section:
Explanation:
Reference: https://docs.fortinet.com/document/fortimanager/6.4.1/administrationguide/792943/task-monitor
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 54: View the tasks FortiAnalyzer administrators have performed, including progress and status.

QUESTION 8
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.

Correct Answer: C
Section:
Explanation:
Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMGFAZ/0800_ADOMs/0015_FortiClient%20and%20ADOMs.htm

QUESTION 9
Refer to the exhibit.



Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)
A. Report size will be optimized to conserve disk space on FortiAnalyzer.

B. Reports will be cached in the memory.
C. This feature is automatically enabled for scheduled reports.
D. Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

Correct Answer: C, D
Section:
Explanation:
"Enable auto-cache in the report settings to boost the reporting performance and reduce report generation time. Scheduled reports have auto-cache enabled already."
FortiAnalyzer_7.0_Study_Guide-Online page 306

QUESTION 10
Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)
A. FortiAnalyzer HA can function without VRRP. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
B. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
C. All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
D. FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

Correct Answer: B, C
Section:
Explanation:
Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FMGFAZ/4600_HA/0000_HA.htm?TocPath=High%20Availability%7C_____0
FortiAnalyzer HA implementation works only in networks where Virtual Router Redundancy Protocol (VRRP) is permitted. Therefore it may not be supported by some public cloud infrastructures.

QUESTION 11
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.

Correct Answer: B, D
Section:
Explanation:
Reference: https://community.fortinet.com/t5/Fortinet-Forum/FW-Migration-between-ADOMs/mp/32683?m=158008

QUESTION 12
Which two actions should an administrator take to view Compromised Hosts on FortiAnalyzer?
(Choose two.)
A. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
B. Make sure all endpoints are reachable by FortiAnalyzer.
C. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer device.
D. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up to date.

Correct Answer: A, D
Section:
Explanation:
In order to configure IOC, you require the following:
• A one-year subscription to IOC. Note that FortiAnalyzer does include an evaluation license, but it is restrictive and only meant to give you an idea of how the feature works.
• A web filter services subscription on FortiGate device(s)
• Web filter policies on FortiGate device(s) that send traffic to FortiAnalyzer Compromised Hosts or Indicators of Compromise service (IOC) is a licensed feature.

To view Compromised Hosts, you must turn on the UTM web filter of FortiGate devices and subscribe your FortiAnalyzer unit to FortiGuard to keep its local threat database synchronized with the FortiGuard threat database. See Subscribing FortiAnalyzer to FortiGuard.
Ref : https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/137635/viewingcompromised-hosts

QUESTION 13
In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results.
Similarly, which feature you can use for FortiView?
A. Export to Report Chart
B. Export to PDF
C. Export to Chart Builder
D. Export to Custom Chart

Correct Answer: A
Section:
Explanation:
Reference: https://community.fortinet.com/t5/FortiAnalyzer/Creating-a-Custom-report-from-FortiView-Export-to-Report-Chart/ta-p/190154?externalID=FD40483
Similar to the Chart Builder feature in Log View, you can export a chart from a FortiView. The chart export includes any filters you set on the FortiView. FortiAnalyzer_7.0_Study_Guide-Online pag. 292.

QUESTION 14
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.

Correct Answer: A
Section:
Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.2.0/hardening-yourfortigate/582009/system-administrator-best-practices

QUESTION 15
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.

Correct Answer: A
Section:
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

QUESTION 16
Which two statements express the advantages of grouping similar reports? (Choose two.)

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

Correct Answer: A, C
Section:
Explanation:

QUESTION 17
What are analytics logs on FortiAnalyzer?
A. Log type Traffic logs.
B. Logs that roll over when the log file reaches a specific size.
C. Logs that are indexed and stored in the SQL.
D. Raw logs that are compressed and saved to a log file.

Correct Answer: C
Section:
Explanation:

QUESTION 18
What is Log Insert Lag Time on FortiAnalyzer?
A. The number of times in the logs where end users experienced slowness while accessing resources.
B. The amount of lag time that occurs when the administrator is rebuilding the ADOM database.
C. The amount of time that passes between the time a log was received and when it was indexed on FortiAnalyzer.
D. The amount of time FortiAnalyzer takes to receive logs from a registered device

Correct Answer: C
Section:
Explanation:

QUESTION 19
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:
Explanation:

QUESTION 20
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:

Explanation:

QUESTION 21
Which statement describes a dataset in FortiAnalyzer?

Correct Answer: A
Section:
Explanation:

QUESTION 22
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:
Explanation:

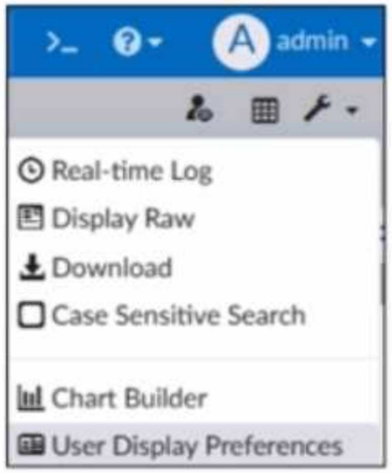
QUESTION 23
What is the purpose of trigger variables?
A. To display statistics about the playbook runtime
B. To use information from the trigger to filter the action in a task
C. To provide the trigger information to make the playbook start running
D. To store the start times of playbooks with On_Schedule triggers

Correct Answer: B
Section:
Explanation:

QUESTION 24
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:
Explanation:

QUESTION 25
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:
Explanation:

QUESTION 26

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:
Explanation:

QUESTION 27

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
task-list-size	: 2000
webservice-proto	: 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:
Explanation:

QUESTION 28
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:
Explanation:

QUESTION 29
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 30
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:
Explanation:

QUESTION 31
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 32
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.