Fortinet

Exam Questions NSE5_FAZ-7.0

Fortinet NSE 5 - FortiAnalyzer 7.0

NEW QUESTION 1
Which item must you configure on FortiAnalyzer to email generated reports automatically?

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

Answer: A

NEW QUESTION 2
For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

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

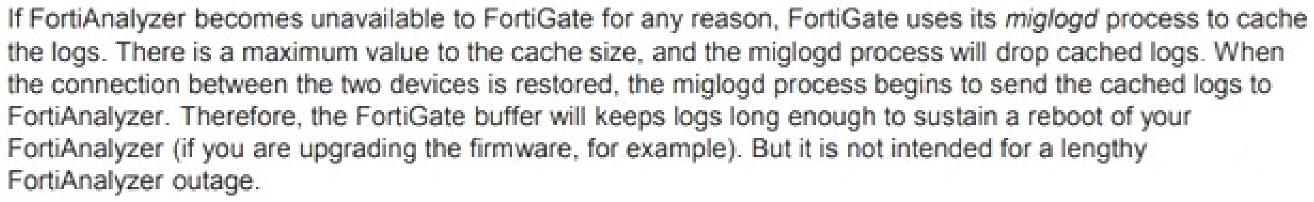
Answer: BD

NEW QUESTION 3
You need to upgrade your FortiAnalyzer firmware.
What happens to the logs being sent to FortiAnalyzer from FortiGate during the time FortiAnalyzer is temporarily unavailable?

A. FortiAnalyzer uses log fetching to retrieve the logs when back online
B. FortiGate uses the miglogd process to cache the logs
C. The logfiled process stores logs in offline mode
D. Logs are dropped

Answer: B

Explanation:



If FortiAnalyzer becomes unavailable to FortiGate for any reason, FortiGate uses its *miglogd* process to cache the logs. There is a maximum value to the cache size, and the miglogd process will drop cached logs. When the connection between the two devices is restored, the miglogd process begins to send the cached logs to FortiAnalyzer. Therefore, the FortiGate buffer will keeps logs long enough to sustain a reboot of your FortiAnalyzer (if you are upgrading the firmware, for example). But it is not intended for a lengthy FortiAnalyzer outage.

NEW QUESTION 4
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

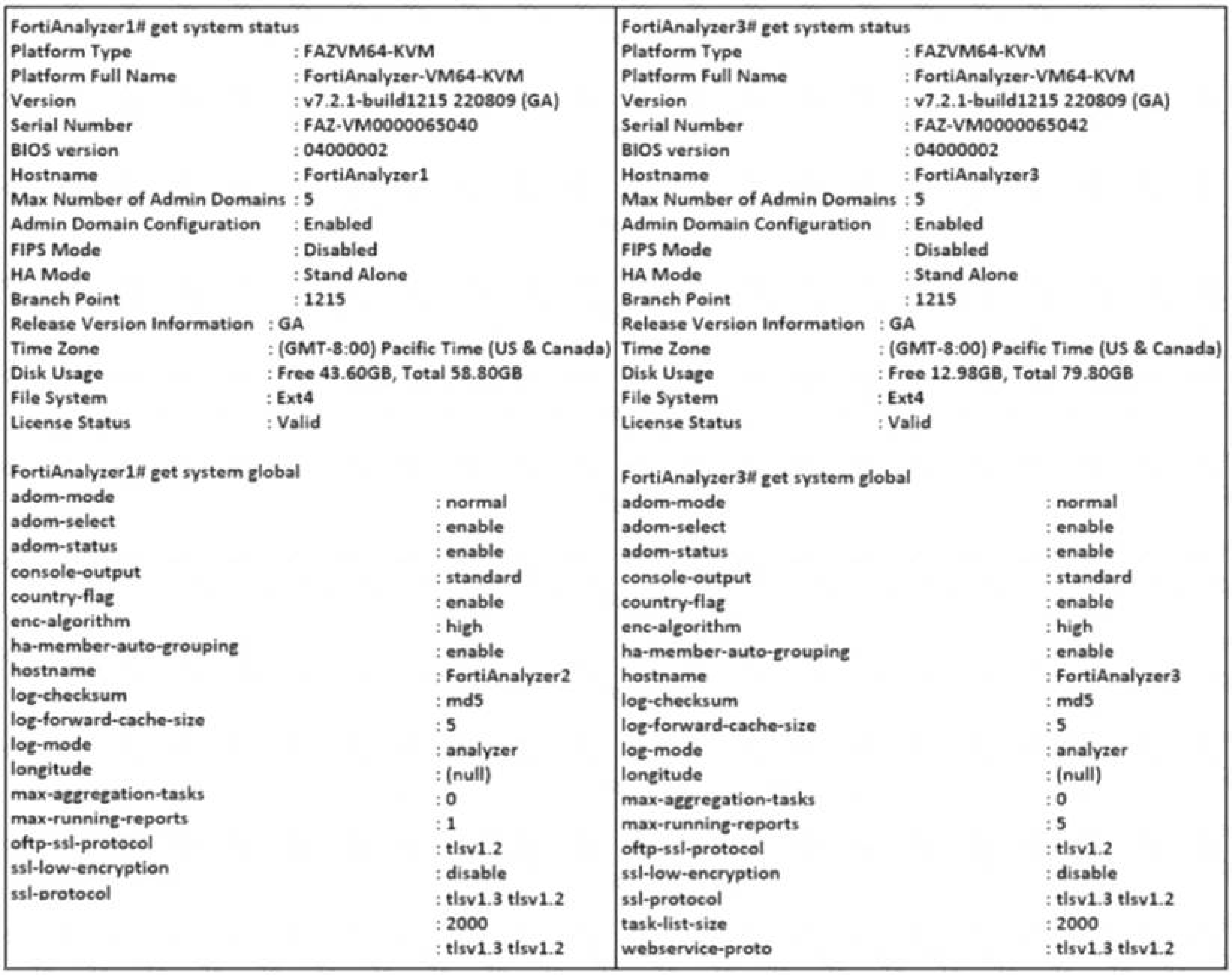
Answer: B

NEW QUESTION 5
Which statement about the FortiSIEM management extension is correct?

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

Answer: A

NEW QUESTION 6
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 7
Which two methods can you use to send event notifications when an event occurs that matches a configured event handler? (Choose two.)

A. SMS
B. Email
C. SNMP
D. IM

Answer: BC

NEW QUESTION 8
You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used.
What does the disk quota refer to?

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

Answer: D

NEW QUESTION 9
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 10
What purposes does the auto-cache setting on reports serve? (Choose two.)

A. To reduce report generation time
B. To automatically update the hcache when new logs arrive
C. To reduce the log insert lag rate
D. To provide diagnostics on report generation time

Answer: AB

NEW QUESTION 11
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

Answer: D

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetcher-management

NEW QUESTION 12
Which two statements are correct regarding the export and import of playbooks? (Choose two.)

A. You can export only one playbook at a time.
B. You can import a playbook even if there is another one with the same name in the destination.
C. Playbooks can be exported and imported only within the same FortiAnaryzer.
D. A playbook that was disabled when it was exported, will be disabled when it is imported.

Answer: BD

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.

NEW QUESTION 13
Which two statements express the advantages of grouping similar reports? (Choose two.)

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

Answer: AC

NEW QUESTION 14
Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

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

Answer: B

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

NEW QUESTION 15
......