Question: 1

An administrator needs to import data into QRadar for a specific use case.
The data that has been provided to the administrator is stored in records that map a key to a value.
Which type of data collection must the administrator create?

A. Reference set
B. Reference map of sets
C. Reference map
D. Reference map of maps

Answer: B

Reference:
https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/t_qradar_conifig_rul_resp_reference_set.html

Question: 2

An administrator needs to know if a custom rule is being correlated correctly.
Which QRadar component is responsible for this process?

A. QRadar Event Collector
B. QRadar Console
C. Magistrate
D. QRadar Event Processor

Answer: D

Reference:
https://www.ibm.com/support/pages/qradar-global-correlation

Question: 3

An administrator needs to collect logs from the Command Line Interface (CLI).
Which command should the administrator use?

A. /opt/bin/qradar/support/get_logs.sh
B. /opt/support/get_logs.sh
C. /opt/support/qradar/get_logs.sh

D. /opt/qradar/support/get_logs.sh

Answer: D

Reference:
https://www.ibm.com/support/pages/getting-help-what-information-should-be-submittedqradarservice-request

Question: 4

To comply with specific regulations, an administrator has been requested to increase asset retention to 365 days.
In which QRadar section can the administrator find the asset retention settings?

A. Admin Tab / Asset Retention
B. Assets Tab / Retention settings
C. Admin Tab / System settings
D. Assets Tab / Asset Retention

Answer: C

Reference:
https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/t_qradar_adm_asset_tuning_ip_retention.html

Question: 5

A QRadar administrator added High Availability (HA) to the Event Processor and needs to verify the crossover link status between the primary and secondary hosts.
Which commands can be used to verify the crossover status? (Choose two.)

A. /opt/qradar/ha/bin/ha_getstate.sh
B. /opt/qradar/ha/bin/getStatus crossover
C. /opt/qradar/ha/bin/qradar_nettune.pl crossover status
D. /opt/qradar/ha/bin/qradar_nettune.pl linkaggr <interface> status
E. /opt/qradar/ha/bin/ha cstate
F. cat /proc/drbd

Answer: CF

Reference:
https://www.ibm.com/developerworks/community/forums/html/topic?id=5c01c198-016d-

461ba648-
a87cdc445768