C1000-026^{Q&As}

IBM Security QRadar SIEM V7.3.2 Fundamental Administration

Pass IBM C1000-026 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/c1000-026.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official
Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Due to regulatory constraints, an administrator must increase the minimum password length and complexity.

In which QRadar section can the administrator change this setting?

A. Admin / System settings

B. Admin / Password policy

C. Admin / Security profiles

D. Admin / Authentication

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/en/SSHLHV_5.4.0/com.ibm.alps.doc/tasks/alps_configuring_admin_settings.htm

---

QUESTION 2

An administrator needs to save a search to use it in the dashboards.

To do so, which search feature does the administrator need to select in the "Include in my Dashboard" checkbox?

A. Filter events of the last 7 days

B. Filter events of the last month

C. Filter events of the last 5 minutes

D. Group by some property

Correct Answer: D

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_users_guide.pdf (42)

QUESTION 3

A QRadar user reported the following notification:

38750099 – The accumulator was unable to aggregate all events/flows for this interval

When does this message appear?

A. When the aggregate data view configuration that is in memory is unable to write data to the database

B. When the system is unable to accumulate data aggregations within 60 seconds

C. When aggregated data views are disabled

D. When search results is unable to return over 200 unique objects

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/38750099.html

---

QUESTION 4

Which event routing rule is required to add QRadar Data Store (QDS) capability to a deployment?

A. Log Only (exclude Analytics)

B. Delete data When storage space is required

C. Bypass Correlation

D. Delete data immediately after the retention period has expired

Correct Answer: A

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

QUESTION 5

An administrator would like to add a new managed host which uses an existing Network Address Translation (NAT).

Which parameters have to be provided if "Host is NATed" is chosen while adding a managed host?

A. Select Network Attached Telemetric, Enter MAC address of the server or appliance to add

B. Select NATed network, Enter public IP of the server or appliance to add

C. Select NATed network, Enter MAC address of the server or appliance to add

D. Select Network Attached Telemetric, Enter public IP of the server or appliance to add

Correct Answer: B

Reference: https://www.google.com/url?
sa=tandrct=jandq=andesrc=sandsource=webandcd=1andved=2ahUKEwihsu3Li5XmAhVYwAIHHeCLDtoQFjAAegQIBh
ACandurl=https%3A%2F%2Fwww.ibm.com%2Fdeveloperworks%2Fcommunity%2Fforums% 2Fajax%
2Fdownload%2Fd5b20a5b-11bd-4a1d-b294-08ec138eb0e1%2F9d086dd8-eee9-4cbd-912d-26059ffdd0ca
%2FQRadar_721_AdminGuide.pdfandusg=AOvVaw1GO4OmOjWV7uiyCLrdE0FV