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.pass2lead.com/c1000-026.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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 2

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

QUESTION 3

A custom rule is generating events reporting that a specific user is failing to login too many times in the last 5 minutes. The administrator opens the event details to investigate the anomaly associated with the events but finds that no Anomaly details pane is shown.

What is the reason?

The events were generated by:

A. a Behavioral Detection Rule

B. an Anomaly Detection Rule

C. a Threshold Detection Rule

D. a standard Custom Rule

Correct Answer: B

Reference: http://www.siem.su/docs/ibm/Administration_and_introduction/User_Guide.pdf

QUESTION 4

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

Correct 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 5

An administrator needs to save the nightly QRadar backups on a network storage.

The administrator has established the connection to the network storage.

What should the administrator do next?

A. Change the Backup Repository Path to the network storage location using the Backup Recovery Configuration window.

B. Change the Backup Repository Path by adding a new Network Activity Rule.

C. Change the Backup Repository Path to the network storage location using the System Settings window.

D. Configure the new network storage using the Assets Manager

Correct Answer: A

Reference: http://ftpmirror.your.org/pub/misc/ftp.software.ibm.com/software/security/products/qradar/

documents/7.2.8/en/b_qradar_admin_guide.pdf (146)

QUESTION 6

An administrator enters the QRadar web console into a web browser but does not get a response. Which process is responsible for the QRadar GUI?

A. tomcat

B. consoled

C. magistrated

D. guid

Correct Answer: A

Reference: https://www.ibm.com/support/pages/qradar-core-services-and-impact-when-restarted

QUESTION 7

An administrator needs to add the following networks to a QRadar network hierarchy as a single Classless Inter-Domain Routin (CIDR) range:

192.168.64.0/24 192.168.65.0/24 192.168.66.0/24 192.168.67.0/24

What is the correct supernet for these subnets?

A. Network 192.168.66.0 with subnet mask 255.255.252.0

B. Network 192.168.64.0 with subnet mask 255.255.252.0

C. Network 192.168.64.0 with subnet mask 255.255.255.0

D. Network 192.168.66.0 with subnet mask 255.255.252.0

Correct Answer: C

QUESTION 8

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

Correct Answer: D

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

QUESTION 9

What should an administrator do to successfully upgrade an IBM Security QRadar system from an older version?

A. Verify the upgrade path, and review the software, hardware and high availability requirements.

B. Verify the upgrade path and update the QRadar apps.

C. Review the release notes and review the architecture.

D. Review the software, hardware and high availability requirements, and consider to update the firmware on IBM Security QRadar appliances.

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/ b_qradar_upgrade.pdf (9)

QUESTION 10

What happens if QRadar receives events at a higher rate than the license allows?

A. The events will be put into queues

B. The source system will be asked to resend the events later

C. The events will not be parsed

D. The events will be dropped immediately

Correct Answer: A

Reference: https://www.ibm.com/support/pages/qradar-event-and-flow-burst-handling-buffer