C1000-026$^{Q\&As}$

IBM Security QRadar SIEM V7.3.2 Fundamental Administration

QUESTION 1

An administrator would like to categorize discovered assets by port definitions and add this information to a server type building block for further use.

Which QRadar Console functionality should the administrator use?

A. Assets Tab – Actions - Scan

B. Assets Tab – Server Discovery

C. Admin Tab – Auto Update

D. Admin – Scheduled Scans

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/b_qradar_tuning_guide.pdf

QUESTION 2

What is the minimum memory in gigabyte (GB) required for a QRadar All-in-One Virtual 3199 appliance?

A. 128

B. 32

C. 24

D. 16

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_ha_vrt_ap_reqs.html

QUESTION 3

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 4

An administrator needs data backup.

What information is contained in the data backup?

A. Audit log information, Event data, Flow data, Report data, Indexes, Log sources

B. Audit log information, Event data, Indexes, Index management information, Flow data, Report data

C. Audit log information, Event data, Flow data, Report data, Indexes

D. Audit log information, Event data, Indexes, Index management information, Flow data, Report data, Groups

Correct Answer: C

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/
c_qradar_adm_man_back_recovery.html

QUESTION 5

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 6

An administrator wants to have all QRadar apps running on a new App Host that was configured to have dedicated CPU, storage and memory resources for the Apps. Several issues were presented during the installation of the App Host.

To troubleshoot, what should the administrator check?

A. If the completion of the /opt/qradar/check_app_host.sh script was successful

B. If port 5000 is opened on the console

C. If an IP table entry was already created to allow traffic from the App Host IP

D. If IP tables are disabled on the console

Correct Answer: B

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

QUESTION 7

An administrator needs to add, delete and modify user accounts.

When deleting a user, what dependency checks are carried out?

A. Custom Rules, Historical Correlation Profiles, Security Profiles

B. Custom Rules, Report and Search Criteria, Security Roles

C. Custom Rules, Security Profiles, Report and Search Criteria

D. Custom Rules, Report and Search Criteria, Historical Correlation Profiles

Correct Answer: D

QUESTION 8

An administrator needs to develop advanced filters to retrieve information from the QRadar System pertaining to the top abnormal events of the most bandwidth-intensive IP addresses.

How can the administrator do this?

A. Build an AQL query using the QRadar Scratchpad

B. Combine GROUP BY and ORDER BY clauses in a single query

C. Use the IBM DataStudio to create the query

D. Build an AQL query using the QRadar GUI using Assets > Search Filter

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/ b_qradar_aql.pdf (21)

QUESTION 9

How many default dashboards does QRadar have?

A. 4

B. 5

C. 7

D. 6

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_customize_dboard.html

QUESTION 10

When troubleshooting issues with QRadar applications, which application Docker container log file can be used to get more information about the apps?

A. /var/log/qradar.error

B. /var/log/qradar.log

C. /var/log/app.log

D. /store/log/app.log

Correct Answer: D

Reference: https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/24f91a23-846b483c-ba22-d78b95eed91e/page/d504c946-a9b0-4277-8e4f-bc554ac30e4e/versions