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.leads4pass.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

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 2

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

Correct Answer: D

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

QUESTION 3

An administrator modified a configuration setting in the Global System Notifications using the QRadar Console Admin tab.

What is the last step to apply changes?

A. Reload Web Server

B. Restart Services

C. Re-login to QRadar console

D. Deploy Changes

Correct Answer: D

QUESTION 4

An administrator has been tasked to run all health checks at once using the DrQ command before a major event happens, such as an upgrade.

What does the DrQ command do?

A. It runs all available checks in /opt/ibm/si/diagnostiq with the checkup mode and with the summary output mode.

B. It shows all the available drives on the QRadar managed host.

C. It runs all available checks in /opt/ibm/si/diagnostiq and writes the results in a txt file.

D. It checks all the available drives on the QRadar managed host and writes the results on a txt file.

Correct Answer: A

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

QUESTION 5

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 6

An administrator needs to restore from backup the applications in QRadar.

Which configuration item should the administrator select?

A. Installed Applications Configuration

B. Backup Installed Applications

C. Installed Applications Backup Configuration

D. Installed Programs Configuration

Correct Answer: A

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

QUESTION 7

An administrator may be asked to collect diagnostic information on one of our main services. For example, ecs-ec.

Commands such as: /opt/qradar/support/thredtop.sh /opt/qradar/support/jmx.sh

These commands collect thread and statistical information on the Services pipeline, queues and filters.

How would an administrator identify a list of jmx ports for each service?

A. grep JMXPORT /opt/qradar/init/*

B. grep JMXPORT /opt/qradar/systemd/env/*

C. grep JMXPORT /opt/qradar/system/bin/*

D. grep JMXPORT /opt/qradar/system/mem/*

Correct Answer: B

QUESTION 8

An administrator installed a new App Host and would like to move the existing applications from the Console to the App Host.

What steps should be performed?

A. Admin Tab > Extension Management > Click to change where apps are run

B. Admin Tab > System Settings > Move apps

C. Admin Tab > Extension Management > Move apps

D. Admin Tab > System and License Management > Click to change where apps are run

Correct Answer: D

QUESTION 9

An administrator has added a new Event Processor to a QRadar deployment.

How many events per second (EPS) are granted from the temporary license and how many days will those EPS last?

A. 10000 EPS for a 35 day period

B. 5000 EPS for a 45 day period

C. 10000 EPS for a 45 day period

D. 5000 EPS for a 35 day period

Correct Answer: D

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

QUESTION 10

An administrator needs to import a list of HR staff logins into a reference set.

Which file type can be used with the import function in the reference set editor window?

A. xml

B. csv

C. xls

D. json

Correct Answer: B

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