C1000-026

Number: C1000-026
Passing Score: 800
Time Limit: 120 min
File Version: 1

C1000-026

Exam A

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.

https://vceplus.com/ 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: C
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 4
An administrator is seeing the following system notification:

38750057 – A protocol source configuration may be stopping events from being collected.

What is a valid user action to this issue?

A. Re-install the QRadar Console
B. Review the /var/log/qradar.log file for more information
C. Restart the QRadar Console
D. Review the /var/log/error.log file for more information

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/38750057.html **QUESTION 5**
An administrator is about to integrate logs from a custom firewall in a QRadar deployment using syslog. The SIEM has two domains, namely Domain A and Domain B. While reviewing the following sample logs, the administrator notices a "context" keyword:

May 14 11:05:01 192.168.1.23 20190514 11:05:00 **context=contextA** permit 192.168.1.24 source: 10.10.1.15; source_port: 64094; destination: 10.10.13.34; service: 53; protocol: udp;

May 13 12:07:01 192.168.1.23 20190513 11:07:00 **context=contextB** permit 192.168.1.25 source: 10.10.1.15; source_port: 64094; destination: 10.10.13.34; service: 53; protocol: udp;

Which options assign the "contextA" logs to DomainA and the "contextB" logs to domain B? (Choose two.)

A. Create a single log source, create a "Context" custom event property, and assign the log to both domains using a custom rule.
B. Create two individual log sources by configuring a separated logging instance for each context on the firewall and assign each log source to the correct domain.
C. Create a single log source, create a "Context" custom event property, and assign the log to the correct domain using custom event property value.
D. Create two individual log sources using the context value as log source identifier and assign each log source to the correct domain.
E. Create a single log source, create a "Context" custom event property, and assign the log to the correct domain using a custom rule.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
How many default dashboards does QRadar have?

A. 4
B. 5
C. 7
D. 6

Correct Answer: B

Section: (none)
Explanation

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

QUESTION 7
An administrator needs to upgrade their QRadar environment. The administrator has downloaded the Patchupdate File from Fixcentral and transferred this Image to the Appliance.

Which commands does the administrator need to run to start the upgrade process?

A. 1. cd/medial/updates
   2. systemctl stop Qradar
   3. Qradar.sh upgrade all
   4. systemctl reboot
B. 1. mount –o loop –t squashfs XX_patchupdate.sfs /media/updates
   2. cd /media/updates
   3. /installer
C. 1. cd /media/updates
   2. yum update XX_patchupdate.sfs
D. 1. patch XX_patchupdate.sfs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
An administrator needs to extract a property from an intrusion detection system (IDS) log. Using a regular expression, the administrator wants to extract a specific part of the log showing the matching “policy ID” of the IDS.

Which type of property must the administrator create?

A. Custom event property
B. Custom flow property
C. Custom asset property
D. Normalized event property

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 9
A company has two different domains in their IBM QRadar system: Domain_A and Domain_B. An administrator has been tasked to create a rule to look only at events that are tagged with Domain_A and ignore rules that are tagged with the other domains.

What **domain text** should the administrator use to create this rule?

A. is from domain: Domain_A
B. from domain: Domain_A
C. domain is: Domain_A
D. domain is one of: Domain_A

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 10
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
Section: (none)
Explanation

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

QUESTION 11

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
Section: (none)
Explanation

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

QUESTION 12
Which event QID test is used to send an email as a rule response when disk usage reaches a threshold?

A. (38750076) Disk Sentry Reached Warn threshold
B. (38750076) Disk Sentry Disk Usage Exceeded Warning threshold levels
C. (38750076) Disk Usage Exceeded Warn threshold
D. (38750076) Disk Sentry Disk Usage Exceeded Warn threshold

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/pages/qradar-configuring-qradar-remote-alerts-about-disk-usage

QUESTION 13
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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
Section: (none)
Explanation

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

QUESTION 15
After fixing the assets that contributed to the asset growth deviation, an administrator needs to find the asset artifacts that have to be cleaned up.

What action should the administrator take to find the artifacts?

A. On the “Log Activity” tab, run the “Deviating Asset Growth: Asset Report event search”
B. On the Admin Tab, select System Configuration --> Asset Profiler Configuration
C. Run the **./cleanAssets.sh --list** command
D. On the Asset tab, run the “Clean Assets” action
Correct Answer: A
Section: (none)
Explanation

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

QUESTION 16
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
Section: (none)
Explanation

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

QUESTION 17
An administrator needs to complete the upgrade process from V7.3.1 to V7.3.2.

What is the correct procedure?

A. Copy the ISO file extension to the recommended directories and use this file
B. Use the ISO file to execute the upgrade process
C. Do a clean installation using the ISO file on a bootable USB device
D. Copy the SFS file extension to the recommended directories and use this file

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 18
An administrator wants to upload a file with information related to network hierarchy instead of using the GUI wizard.

How can the administrator do this?

A. Install application “Network Hierarchy Management for QRadar”
B. Upload file using REST API
C. Modify /opt/qradar/conf/remotenet.conf
D. Use upload button in Network Hierarchy wizard

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/pages/qradar-restoring-network-hierarchy-using-network-hierarchy-management-qradar-app-updated

QUESTION 19
A company has several appliances and the administrator needs to copy a file to all appliances to run some tests to verify the integrity of the processes. The /opt/qradar/support/all_servers.sh script can be used to issue commands to all QRadar appliances within the deployment.

What option must be used with the script to copy the file to all appliances in the deployment?

A. /opt/qradar/support/all_servers.sh -p
B. /opt/qradar/support/all_servers.sh -k
C. /opt/qradar/support/all_servers.sh -C
D. /opt/qradar/support/all_servers.sh -g

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www-01.ibm.com/support/docview.wss?uid=swg21998517

QUESTION 20
An administrator needs to develop advanced filters to retrieve information from the QRadar System pertaining to the top abnormal events of the most bandwidthintensive 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
Section: (none)
Explanation

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

QUESTION 21
An administrator logs in to the Offenses tab and finds a large number of new Offenses that need action.

What column in the list of Offenses should the administrator use to prioritize them?

A. Magnitude
B. Offense Type
C. Source IPs
D. Last Event/Flow

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_users_guide.pdf (43)

QUESTION 22

An administrator receives an expensive custom rule notification.

Which tool can now be enabled via the Advanced 'System Settings' – Custom Rule Settings to help troubleshoot this?

A. Offense Analysis
B. Rule Analysis
C. Custom Rule Analysis
D. Performance Analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
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
Section: (none)
Explanation

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

QUESTION 24
An administrator would like to extend the functionality of QRadar using an external application.

Which file format is supported to successfully upload an application from the QRadar Console?

A. .zip
B. .tgz

C. .sh
D. .exe

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.appfw.doc/b_qradar_appframework_devguide.pdf **QUESTION 25**
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
Section: (none)
Explanation

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

QUESTION 26
A QRadar upgrade is planned and a maintenance window is scheduled. The administrator must stage the FIXPACK from IBM Fix Central.

Which QRadar FIXPACK file type must the administrator download?

A. RPM
B. IMG
C. SFSD. XFS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Reference: https://www-945.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+QRadar+Network+Insights&release=7.3.0&platform=Linux&function=all

QUESTION 27
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/24f91a23-846b-483c-ba22-d78b95eed91e/page/d504c946-a9b0-42778e4f-bc554ac30e4e/versions