1.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 maching “policy ID” of the IDS.

Which type of property must the administrator create?

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

2. An administrator has to changed the system hardware check of the QRadar server. The administrator has already restarted the main services (hostservices, tomcat, hostcontext) and needs to synchronize the QRadar Console time with the QRadar managed hosts.

Which command can the administrator use to accomplish this?

A./opt/qradar/support/all_servers.sh service ntpd restart
B./opt/qradar/support/all_servers.sh /opt/qradar/bin/time_sync.sh
C./sbin/hwclock –systohc /opt/qradar/bin/time_sync.sh
D./opt/qradar/support/all_servers.sh systemctl restart systemd-timedated.service

3. An administrator logs in to the Offenese 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. Source IPs
B. Magnitude
C. Last Event/Flow
D. Offense Type

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

Which configuration item should the administrator select?

A. Installed Applications Configuration
B. Installed Applications Backup Configuration
C. Backup Installed Aplications
D. Installed Programs Configuration

5. 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 port 5000 is opened on the console.
B. If the completion of the /opt/qradar/check_app_host.sh script was successful
C. If IP tables are disabled on the console
D. If an IP tables entry was already created to allow traffic from the App Host IP

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

How can the administrator do this?

A. Build an AQL query using the QRadar Scratchpad
B. Use the IBM DataStudio to create the query
C. Combine GROUP BY and ORDER BY clauses in a single query
D. Build an AQL query using the QRadar GUI using Assets > Search Filter

7. 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 public IP of the server or appliance to add
B. Select Network Attached Telemetric, Enter MAC address of the server or appliance to add
C. Select NATed network, Enter MAC address of the server or appliance to add
D. Select NATed network, Enter public IP of the server or appliance to add

8. How many default dashboards does QRadar have?

A. 5
B. 7
C. 4
D. 8

9. What is a reason for restarting hostcontext in QRadar?

A. A new app was installed
B. A new network hierarchy was uploaded
C. The host is not responding to deploy requests
D. A new user was created and it needs to be replicated

10. 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. .tgz
B. .exe
C. .zip
D. .sh

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

12. An administrator needs to collect logs from the Command Line Interface (CLI).

Which command should the administrator use?

A. /opt/support/qradar/get_logs.sh
B. /opt/qradar/support/get_logs.sh
C. /opt/support/get_logs.sh
D. /opt/bin/qradar/support/get_logs.sh

13. An administrator logs into the QRadar Console to review the stored backup files. There is an exclamation mark beside some files.

What is the cause of this?

A. Incomplete backup files
B. Canceled backup files
C. Corrupted backup files
D. Missing backup files

14. 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_server.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 -g
C. /opt/qradar/support/all_servers.sh -C
D. /opt/qradar/support/all_servers.sh -k

15. 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 map of sets
B. Reference map of maps
C. Reference map
D. Reference set

16. To comply with specific regulations, an administrator has been requested to increase asset retention to 365 days.

In which QRadar section can the administrator find the asset retention settings?

A. Assets Tab / Retention settings
B. Admin Tab / System settings
C. AdminTab / Asset Retention
D. Assets Tab / Asset Retention

17. 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 45 day period
B. 5000 EPS for a 45 day period
C. 10000 EPS for a 35 day period
D. 5000 EPS for a 35 day period

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

In which QRadar section can the administrator change this settings?

A. Admin / System settings
B. Admin / Password policy
C. Admin / Security profiles
D. Admin / Authentication

19. An administrator enabled the base license of QRadar Vulnerability Manager.

How many assets can be scanned using this license?

A. up to 100
B. up to 512
C. up to 128
D. up to 256

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

A. The events will not be parsed
B. The events will be dropped immediately
C. The source system will be asked to resend the events later
D. The events will be put into queues

21. Which event QID test is used to send an email as a rule response when disk usage reachesa threshold?

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

22. 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. Run the ./cleanAssets.sh –list command
B. On the Asset tab, run the “Clean Assets” action
C. On the Admin Tab, select System Configuration --> Asset Profiler Configuration
D. On the “Log Activity” tab, run the “Deviating Asset Growth: Asset Report event search”

23. An administrator has been tasked to create a saved search that shows a list of multiple login failures for a single user by username. The administrator has done the following:

1. Selected Last Hour in the view option
2. In the Add filter window, selected the search parameter Custom Rule [indexed]
3. Selected Equals for Operator.
4. Selected Authentication for Rule Group

What is the next step the administrator needs to perform for the Rule option?

A. Select login failures followed by success to the same username
B. Select multiple login failures to the same destination
C. Select multiple login failures for a single username
D. Select multiple login failures from the same source

24.

25. 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 System Settings window
B. Configure the new network storage using the Assets Manager
C. Change the Backup Repository Path by adding a new Network Activity Rule
D. Change the Backup Repository Path to the network storage location using the Backup Recovery Configuration window

26. An administrator is tasked to reduce data volumes in the asset database and reduce stale data contributing to asset growth deviation.

How can the administrator tune the configuration of the Asset Profiler?

A. On the navigation menu, click Admin, click the Asset Profile Configuration and reduce the retention values for the Asset Profiler Retention Configuration and Save. On the navigation menu, click Admin and from the Advanced menu, click Restart Event Collection Services. Next, deploy the changes into the environment for the updates to take effect.

B. In the System Configuration section of the Admin, accesss the Asset Profile Configuration and reduce the retention values for the Asset Profiler Retention Configuration and Save. Next, deploy the changes into the environment for the updates to take effect.

C. In the System Configuration section of the Admin, access the Asset Profile Configuration and increase the retention values for the Asset Profiler Retention Configuration and Save. Next, deploy the changes into the environment for the updates to take effect.

D. In the System Configuration section of the Admin, access the Asset Profile Configuration and increase the retention values for the Asset Profiler Retention Configuration and Save. On the navigation menu, click Admin and from the Advaned menu, click Restart Event Collection Services. Next, deploy the changes into the environment for the updates to take effect.

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

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

29. A QRadar user reported the following notification:

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

When does this message appear?

A. When search results is unable to return over 200 unique objects
B. When aggregated data views are disabled
C. When the aggregate data view configuration that is in memory is unable to write data to the database
D. When the system is unable to accumulate data aggregations within 60 seconds

30. An administrator has been asked to configure a new QRadar console high availability (HA) deployment. Both the primary and secondary consoles have been installed with the QRadar software.

What should the administrator do to complete the HA configuration?

A. Add the secondary console to the deployment, and then create the HA host
B. Select "Secondary Host" on the wizard when adding the secondary host to the deployment
C. Reinstall the QRadar software on the secondary console using an "HA Recovery Setup"
D. Create the HA host to add the secondary console to the deployment

31. 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. SFS
C. XFS
D. IMG

32. Which app should be used for monitoring QRadar performance and health?

A. QRadar Extension Management
B. QRadar Monitoring Intelligence
C. QRadar Performance Overview
D. QRadar Deployment Intelligence

33. A QRadar administrator added High Availability (HA) to the Event Processor and needs to verify the crossover link status between the primary and secondary hosts.

Which commands can be used to verify the crossover status? (Choose two)

A. /opt/qradar/ha/bin/ha_getstate.sh
B. /opt/qradar/ha/bin/ha cstate
C. /opt/qradar/ha/bin/getStatus crossover
D. /opt/qradar/ha/bin/qradar_nettune.pl linkaggr <*interface*> status
E. /opt/qradar/ha/bin/qradar_nettune.pl crossover status
F. cat /proc/drbd

34. An administrator needs to add the following networks to a QRadar network hierarchy as a single Classless Inter-Domain Routing (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 192.168.66.0 with subnet mask 255.255.255.0
D. Network 192.168.64.0 with subnet mask 255.255.255.0

35. And 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 > Move apps
B. Admin Tab > System and License Management > Click to change where apps are run
C. Admin Tab > System Settings > Move apps
D. Admin Tab > Extension Management > Click to change where apps are run

36. 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. mount -o loop -t squashfs XX_patchupdate.sfs /media/updates
2. cd /media/updates
3. ./installer

B. 1. cd /media/updates
2. yum update XX_patchupdate.sfs

C. 1. cd /media/updates
2. systemctl stop Qradar
3. Qradar.sh upgrade all
4. systemctl reboot

D. 1. patch XX_patchupdate.sfs

37. An administrator needs to know if a custom rule is being correlated correctly.

Which QRadar component is responsible for this process?

A. QRarad Event Collector
B. Magistrate
C. QRadar Event Processor
D. QRadar Console

38. 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. magistrate
B. consoled
C. tomcat
D. guid

39. 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.

Which 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

40. When administrator attempts to edit a log source after upgrading QRadar, a Device Support Module (DSM), a protocol, or Vulnerability Information Service (VIS) components, the following error messages appears.

An error has occurred. Refresh your browser (press F5) and attempt the action again. If the problem persists, please contact customer support for assistance.

What action should the administrator take to troubleshoot this issue? (Choose two)

A. Cleare browser cache
B. systemctl restart httpd
C. systemctl restart ecs-ep
D. systemctl restart tomcat
E. systemctl restart iptables
F. systemctl restart snmpd

41. Which IBM monitoring application can be used to see detailed health and status information at the application, middleware, and system level?

A. QRadar Operations App
B. QRadar Advisor With Watson App
C. QRadar Assistant App
D. QRadar Deployment Intelligence App

42. 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. csv
B. xml
C. json
D. xls

43. 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. Group by some property
C. Filter events of the last month
D. Filter events of the last 5 minutes

44. 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. Re-login to QRadar console
B. Deploy Changes
C. Reload Web Server

D. Restart Services

45. 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 – Server Discovery
B. Admin Tab – Auto Update
C. Admin – Scheduled Scans
D. Assets Tab – Action – Scan

46. Which log should be reviewed to determine the reasons a patch installer did not proceed during a QRadar upgrade?

A. /var/log/setup-*/patches.log
B. /var/log/qradar.log
C. /var/log/upgrade.log
D. /var/log/qradar.audit

47. An administrator need to combine multiple extraction and calculation-based properties into a single property.

Which Ariel Query Language (AQL) statement can be used?

A. AQL functions and AQL-based custom properties
B. AQL-based custom properties
C. AQL functions
D. AQL functions and SELECT, FROM, or database names

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

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

A. Custom Rules, Security Profiles, Report and Search Criteria
B. Custom Rules, Report and Search Criteria, Security Roles
C. Custom Rules, Historical Correlation Profiles, Security Profiles
D. Custom Rules, Report and Search Criteria, Historical Correlation Profiles

49. Which of the following dashboards is a QRadar default Dashboard?

A. Vulnerability Overview
B. Monitoring Overview
C. Compliance and Reporting Monitoring
D. Threat and Security Monitoring

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

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

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

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

51. 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 Threshold Detection Rule
B. an Anomaly Detection Rule
C. a Behavioral Detection Rule
D. a standard Custom Rule

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

A. 32
B. 16
C. 128
D. 24

53. 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/systemd/mem/*

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

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

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

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

A. Review the release notes and review the architecture
B. Review the software, hardware and high availability requirements, and consider to update the firmware on IBM Security QRadar appliances
C. Verify the upgrade path and update the QRadar apps
D. Verify the upgrade path, and review the software, hardware and high availability requirements

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

56. An administrator plans to deploy multiple log sources that share a common configuration.

How many log sources can be added at one time?

A. 750
B. 1000
C. 250
D. 500

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

A. Delete data Immediately after the retention period has expired
B. Delete data When storage space is required
C. Bypass Correlation
D. Log Only (Exclude Analytics)

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

A. /storage/log/app.log

B. /var/log/app.log

C. /var/log/qradar.log

D. /var/log/qradar.error

59. An administrator has reviewed the list of new features in the QRadar V7.3.2 release notes, and decides to upgrade their system to this version.

What is the minimum supported version that the administrator can upgrade from?

A. 7.3.1
B. 7.3.0
C. 7.2.8
D 7.2.6

60. An administrator needs data backup.

What information is contained in the data backup?

A. Audit log information, Event data, Flow data, Report data, Indexes
B. Audit log information, Event data, Flow data, Report data, Indexes, Log sources
C. Audit log information, Event data, Indexes, Index management information, Flow data, Report data
D. Audit log information, Event data, Indexes, Index management information, Flow data, Report data, Groups