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.

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
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
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. Admin Tab / Asset Retention
B. Assets Tab / Retention settings

C. Admin Tab / System settings
D. Assets Tab / Asset Retention

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_adm_asset_tuning_ip_retention.html

QUESTION 3
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 4
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
Section: (none)
Explanation
Explanation/Reference:
Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/c_qradar_adm_refdata_ui.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
An administrator plans to deploy multiple log sources that share a common configuration.

How many log sources can be added at one time?

A. 1000

B. 750
C. 250
D. 500

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/com.ibm.dsm.doc/t_logsource_bulkadd.html

QUESTION 7
Which log should be reviewed to determine the reasons a patch installer did not proceed during a QRadar upgrade?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/pages/qradar-unable-run-patch-installer-and-update-exits-screen-terminating-message

QUESTION 8
An administrator has to change the system hardware clock 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 systemctl restart systemd-timedated.service
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 service ntpd restart

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/pages/qradar-configuring-ntp-settings-qradar-appliance

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
What is a reason for restarting hostcontext service in QRadar?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/pages/qradar-restarting-hostcontext-q-switch

QUESTION 11
Which of the following dashboards is a QRadar default Dashboard?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 12
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
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 14
Which app should be used for monitoring QRadar performance and health?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/knowledgecenter/en/SSKMKU/com.ibm.QDIapp.doc/c_qapps_QDI_intro.html

QUESTION 15
An administrator needs to combine multiple extraction and calculation-based properties into a single property.

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

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

D. AQL functions

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/c_aql_whatsnew_731.html

QUESTION 16
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 17
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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 19
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
Section: (none)
Explanation

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

QUESTION 20
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 21
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

Section: (none)
Explanation

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

QUESTION 22
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. 7.2.6
B. 7.3.0
C. 7.3.1
D. 7.2.8

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/pages/release-qradar-v732-sfs-7322019020120112

QUESTION 23
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 24
An administrator enabled the base license of QRadar Vulnerability Manager.

How many assets can be scanned using this license?

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

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_qvm_deploy.html

QUESTION 25
When an administrator attempts to edit a log source after upgrading QRadar, a Device Support Module (DSM), a protocol, or Vulnerability Information Services (VIS) components, the following error message 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. systemctl restart snmpd
B. systemctl restart iptables
C. systemctl restart ecs-ep
D. systemctl start tomcat
E. systemctl restart httpd
F. Clear browser cache

Correct Answer: DF

Section: (none)
Explanation

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

QUESTION 26
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
Section: (none)
Explanation

Explanation/Reference:
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 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. Offense Analysis
B. Rule Analysis
C. Custom Rule Analysis
D. Performance Analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28

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
Section: (none)
Explanation
Explanation/Reference:
Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwihsu3Li5XmAhVYwAIHHeCLDtoQFjAAegQIBhAC&url=https%3A%2F%2Fwww.ibm.com%2Fdeveloperworks%2Fcommunity%2Fforums%2Fajax%2Fdownload%2Fd5b20a5b-11bd-4a1d-b294-08ec138eb0e1%2F9d086dd8eee9-4cbd-912d-26059ffdd0ca%2FQRadar_721_AdminGuide.pdf&usg=AOvVaw1GO4OmOjWV7uiyCLrdE0FV

QUESTION 29

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 30
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. Canceled backup files
B. Missing backup files
C. Corrupted backup files
D. Incomplete backup files

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
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 32
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