IBM Professional Certification Program

Study Guide Series

Exam C1000-156

IBM Security QRadar SIEM V7.5 Administration

Purpose of Exam Objectives

When an exam is being developed, a team of Subject Matter Experts work together to define the job role the individual will fill. They define all the tasks and knowledge that an individual would need to have to successfully perform that role. This creates the foundation for the objectives and measurement criteria, the foundation of the exam. The item writers used these objectives to write the questions that appear on the exam.

It is recommended that you review these objectives carefully. Do you know how to complete the tasks in the objective? Do you know why that task needs to be done? Do you know what will happen if you do it incorrectly? If you are not familiar with a task, then work through the objective and perform that task in your own environment. Read more information about the task. If there is an objective on a task, it is almost certain that you WILL see questions about it on the actual exam.

After you have reviewed the objectives and completed your own research, don't forget to review the free sample questions for this exam on the IBM Certification website. These sample question come complete with an answer key and will give you a feel for the type and style of question on the actual exam.

After that, take the assessment exam. The questions on the assessment exam were developed at the same time and by the same people who wrote the question on the actual exam. The assessment exam is weighted to be equally difficult to the actual test so your results should be predictive of your expected results on the actual test. While the assessment exam will not tell which questions are answered incorrectly, it will tell you how you did on a section-by-section basis so you will know where to focus your further studies.

Contents

Role Definition 5

Key Areas of Competency 5

Prerequisite Knowledge 5

Section 1: System Configuration 6

TASK: 1.1 Perform license management 6

TASK: 1.2 Administer managed hosts 6

TASK: 1.3 Understand distributed architecture 7

TASK: 1.4 Manage configuration and data backups 7

TASK: 1.5 Configure custom SNMP and email templates 8

TASK: 1.6 Manage network hierarchy 8

TASK: 1.7 Use and manage reference data 8

TASK: 1.8 Manage automatic update 9

TASK: 1.9 Demonstrate the use of the asset database 9

TASK: 1.10 Install and configure apps 10

Section 2: Performance Optimization 11

TASK: 2.1 Construct identity exclusions 11

TASK: 2.2 Deal with resource restrictions 11

TASK: 2.3 Rule configuration and tuning 12

TASK: 2.4 Index management 12

TASK: 2.5 Search management 13

TASK: 2.6 Manage routing rules and event forwarding 13

Section 3: Data Source Configuration 14

TASK: 3.1 Manage flow sources 14

TASK: 3.2 Manage log sources 14

TASK: 3.3 Export event and flow data 15

TASK: 3.4 Vulnerability information source configuration 15

TASK: 3.5 Manage custom event and flow properties 16

TASK: 3.6 Manage custom log source types 16

TASK: 3.7 Manage data obfuscation 16

Section 4: Accuracy Tuning 18

TASK: 4.1 Understand and implement ADE rules 18

TASK: 4.2 Manage and use building blocks........18
TASK: 4.3 Manage content packs........18
TASK: 4.4 Distinguish native information sources........19
TASK: 4.5 Configure integrations........19
Section 5: User Management........20
TASK: 5.1 Manage users........20
TASK: 5.2 Create and update security profiles........20
TASK: 5.3 Create and update user roles........21
TASK: 5.4 Manage user authentication and authorization........21
Section 6: Reporting, Searching, and Offense Management........23
TASK: 6.1 Manage reports........23
TASK: 6.2 Utilize different search types........23
TASK: 6.3 Manage offenses........23
TASK: 6.4 Sharing content among users........24
Section 7: Tenants and Domains........25
TASK: 7.1 Differentiate network hierarchy and domain definition........25
TASK: 7.2 Manage domains and tenants........25
TASK: 7.3 Allocate licenses for multi-tenant........26
TASK: 7.4 Assign users to tenants........26
Section 8: Troubleshooting........27
TASK: 8.1 Review and respond to system notifications........27
TASK: 8.2 Troubleshoot common documented issues........27
TASK: 8.3 Configure, manage and troubleshoot applications........27
TASK: 8.4 Perform healthchecks........28
TASK: 8.5 Basic GUI REST-API usage........28

Role Definition

This intermediate level certification is intended for professionals who wish to validate their comprehensive knowledge of IBM Security QRadar SIEM V7.5 Administration.

These administrators will have knowledge and experience in the configuration, performance optimization, tuning, troubleshooting, and ongoing system administration for an IBM Security QRadar SIEM V7.5 on premise deployment. This includes the apps installed with the product: Use Case Manager, QRadar Assistant, Log Source Manager, and Pulse, plus a knowledge of the basic functions of these key IBM-supported apps: User Behavior Analytics, QRadar Deployment Intelligence, Reference Data Management. This does not include the SaaS offering of QRadar on Cloud (QRoC).

Key Areas of Competency

- QRadar troubleshooting
- Searching and reporting
- Rules and building blocks
- Understanding reference data
- Basic QRadar tuning and network hierarchy
- QRadar deployment and component architecture
- Understanding QRadar Event and Flow pipelines
- QRadar user management and data access control
- Basic concepts of multi-domain QRadar instances

Prerequisite Knowledge

Knowledge and foundational skills one must possess before acquiring skills measured on the certification test. These foundational skills are NOT measured on the test.

- Enterprise logging
- Offense and log analysis
- Network monitoring using flows
- QRadar Network Insights, QRadar Incident Forensics
- Basic security technologies, SIEM concepts, TCP/IP networking, IT security concepts, and IT skills

Section 1: System Configuration

This section accounts for 20% of the exam (12 out of 62 questions).

TASK: 1.1 Perform license management

SUBTASKS:

1.1.1. Implement and manage shared license pool

1.1.2. Deploy incremental licenses

1.1.3. Explain burst handling

1.1.4. Upload and allocate a license key to a host

1.1.5. View license details for all QRadar components

REFERENCES:

Burst handling	https://www.ibm.com/docs/en/qsip/7.5?topic=management-burst-handling
Internal events	https://www.ibm.com/docs/en/qsip/7.5?topic=capacity-internal-events
Shared license pool	https://www.ibm.com/docs/en/qsip/7.5?topic=capacity-shared-license-pool
License management	https://www.ibm.com/docs/en/qsip/7.5?topic=administration-license-management
Incremental licensing	https://www.ibm.com/docs/en/qsip/7.5?topic=capacity-incremental-licensing

TASK: 1.2 Administer managed hosts

SUBTASKS:

1.2.1. Add/remove managed hosts

1.2.2. Edit managed host connections

1.2.3. Update managed hosts

1.2.4. Enable/disable encryption

1.2.5. Change managed host high availability (HA) configuration

REFERENCES:

HA Management	https://www.ibm.com/docs/en/qsip/7.5?topic=deployments-ha-management
Upgrading QRadar SIEM	https://www.ibm.com/docs/en/qsip/7.5?topic=upgrading-qradar-siem
Changing where apps are run	https://www.ibm.com/docs/en/qsip/7.5?topic=hosts-changing-where-apps-are-run
QRadar Network Insights overview	https://www.ibm.com/docs/en/qradar-on-cloud?topic=monitoring-qradar-network-insights-overview
What is a QRadar Data Node Appliance?	https://www.ibm.com/support/pages/what-qradar-data-node-appliance
QRadar: Finding files that use the most disk space	https://www.ibm.com/support/pages/qradar-finding-files-use-most-disk-space
Changing the network settings of a QRadar Console in a multi-system deployment	https://www.ibm.com/docs/en/qsip/7.5?topic=nsm-changing-network-settings-qradar-console-in-multi-system-deployment

Encryption	https://www.ibm.com/docs/en/qsip/7.5?topic=hosts-encryption
Managed Hosts	https://www.ibm.com/docs/en/qsip/7.5?topic=management-managed-hosts

TASK: 1.3 Understand distributed architecture

SUBTASKS:

1.3.1. Explain network requirements for distributed architecture

1.3.2. Understand and identify components

- Identify Console
- Identify EP/FP
- Identify EC/FC
- Identify AppHost
- Identify Data Node

REFERENCES:

App Host	https://www.ibm.com/docs/en/qsip/7.5?topic=deployment-app-host
Data Nodes and data storage	https://www.ibm.com/docs/en/qsip/7.5?topic=deployment-data-nodes-data-storage
QRadar architecture overview	https://www.ibm.com/docs/en/qsip/7.5?topic=deployment-qradar-architecture-overview
IBM QRadar: High Availability Guide	https://www.ibm.com/docs/en/SS42VS_7.5/pdf/b_qradar_ha_guide.pdf
Forensics and full packet collection	https://www.ibm.com/docs/en/qsip/7.5?topic=overview-forensics-full-packet-collection
Geographically distributed deployments	https://www.ibm.com/docs/en/qsip/7.5?topic=overview-geographically-distributed-deployments
Expanding deployments to add more capacity	https://www.ibm.com/docs/en/qsip/7.5?topic=overview-expanding-deployments-add-more-capacity
IBM QRadar Network Insights: Installation Guide	https://www.ibm.com/docs/en/SS42VS_7.5/pdf/b_qni_ig.pdf
Common ports and servers used by QRadar	https://www.ibm.com/docs/en/qsip/7.5?topic=problems-common-ports-servers-used-by-qradar

TASK: 1.4 Manage configuration and data backups

SUBTASKS:

1.4.1. Understand and configure data retention

1.4.2. Import config backup

- through the GUI
- through file system

1.4.3. Restore config backup options

1.4.4. Schedule config backup

1.4.5. Restore data backup

REFERENCES:

Administration backup and recovery	https://www.ibm.com/docs/en/qsip/7.5?topic=administration-backup-recovery
Backup and recovery	https://www.ibm.com/docs/en/qsip/7.5?topic=console-backup-recovery
Data back up and restore	https://www.ibm.com/docs/en/qsip/7.5?topic=installations-data-back-up-restore
Scheduling nightly backup	https://www.ibm.com/docs/en/qsip/7.5?topic=data-scheduling-nightly-backup
Backup QRadar configurations and data	https://www.ibm.com/docs/en/qsip/7.5?topic=recovery-backup-qradar-configurations-data

Restore QRadar configurations and data	https://www.ibm.com/docs/en/qsip/7.5?topic=recovery-restore-qradar-configurations-data
Creating an email notification for a failed backup	https://www.ibm.com/docs/en/qsip/7.5?topic=data-creating-email-notification-failed-backup
Restoring data	https://www.ibm.com/docs/en/qsip/7.5?topic=data-restoring
Data retention	https://www.ibm.com/docs/en/qsip/7.5?topic=tasks-data-retention

TASK: 1.5 Configure custom SNMP and email templates

SUBTASKS:

1.5.1. Understand and configure SNMP templates

1.5.2. Understand and configure email templates

REFERENCES:

Customizing the SNMP trap output	https://www.ibm.com/docs/en/qsip/7.5?topic=configuration-customizing-snmp-trap-output
Configuring custom offense email notifications	https://www.ibm.com/docs/en/qsip/7.5?topic=notifications-configuring-custom-offense-email
Configuring event and flow custom email notifications	https://www.ibm.com/docs/en/qradar-on-cloud?topic=notifications-configuring-event-flow-custom-email

TASK: 1.6 Manage network hierarchy

SUBTASKS:

1.6.1. Update network hierarchy using the GUI

1.6.2. Import network hierarchy using the REST-API, CLI or app

REFERENCES:

Defining your network hierarchy	https://www.ibm.com/docs/en/qsip/7.5?topic=nh-defining-your-network-hierarchy

TASK: 1.7 Use and manage reference data

SUBTASKS:

1.7.1. Differentiate types of reference data collections

1.7.2. Add, edit, and delete reference sets using the GUI

1.7.3. View and update the contents of a reference set using the GUI

1.7.4. Create and manage reference data collections using the CLI

1.7.5. Create and manage reference data collections using REST-API

1.7.6. Use AQL to access reference data content

REFERENCES:

Types of reference data collections	https://www.ibm.com/docs/en/qsip/7.5?topic=qradar-types-reference-data-collections
Viewing the contents of a reference set	https://www.ibm.com/docs/en/qsip/7.5?topic=overview-viewing-contents-reference-set
Adding, editing, and deleting reference sets	https://www.ibm.com/docs/en/qsip/7.5?topic=overview-adding-editing-deleting-reference-sets

Creating reference data collections by using the command line	https://www.ibm.com/docs/en/qsip/7.5?topic=rdiq-creating-reference-data-collections-by-using-command-line
Reference data query examples	https://www.ibm.com/docs/en/qsip/7.5?topic=language-reference-data-query-examples
Creating reference data collections with the APIs	https://www.ibm.com/docs/en/qsip/7.5?topic=qradar-creating-reference-data-collections-apis

TASK: 1.8 Manage automatic update

SUBTASKS:

1.8.1. Choose appropriate update types for deployment

1.8.2. Understand what security content can be modified by auto updates

1.8.3. Configure auto updates

1.8.4. Configure auto updates in a non-standard connectivity environment

- behind a proxy server
- air-gapped

REFERENCES:

Automatic updates	https://www.ibm.com/docs/en/qsip/7.5?topic=configuration-automatic-updates
Configuring automatic update settings	https://www.ibm.com/docs/en/qsip/7.5?topic=updates-configuring-automatic-update-settings
QRadar: Important auto update server changes for administrators	https://www.ibm.com/support/pages/node/6244622

TASK: 1.9 Demonstrate the use of the asset database

SUBTASKS:

1.9.1. Identify sources of asset data

1.9.2. Manually update to asset data

- API
- CSV

1.9.3. Identify asset growth deviations

1.9.4. Tune asset profiler retention

1.9.5. Clean/Purge assets

REFERENCES:

QRadar Data Sources	https://ibm.biz/Technical_Sales_Foundations_for_IBM_QRadar_for_Cloud
QRadar Linux services	https://www.ibm.com/mysupport/s/forumsquestion?language=en_US&id=0D50z00006PFbXJCA1
Sources of asset data	https://www.ibm.com/docs/en/qsip/7.5?topic=management-sources-asset-data
Incoming asset data workflow	https://www.ibm.com/docs/en/qsip/7.5?topic=management-incoming-asset-data-workflow
Asset profile data in CSV format	https://www.ibm.com/docs/en/qsip/7.5?topic=configuration-asset-profile-data-in-csv-format
Tuning the number of IP addresses allowed for a single asset	https://www.ibm.com/docs/en/qsip/7.5?topic=deviations-tuning-number-ip-addresses-allowed-single-asset

Updates to asset data	https://www.ibm.com/docs/en/qsip/7.5?topic=management-updates-asset-data
Identification of asset growth deviations	https://www.ibm.com/docs/en/qsip/7.5?topic=management-identification-asset-growth-deviations
Clean up asset data after growth deviations	https://www.ibm.com/docs/en/qsip/7.5?topic=management-clean-up-asset-data-after-growth-deviations
Tuning the Asset Profiler retention settings	https://www.ibm.com/docs/en/qsip/7.5?topic=deviations-tuning-asset-profiler-retention-settings

TASK: 1.10 Install and configure apps

SUBTASKS:

1.10.1. Install apps

1.10.2. Manage authorized services

1.10.3. Backup and restore applications

1.10.4. Configure out-of-the-box installed Apps

REFERENCES:

Apps overview	https://www.ibm.com/docs/en/qsip/7.5?topic=overview-apps
IBM Security App Exchange	https://exchange.xforce.ibmcloud.com/hub
Backup and restore applications	https://www.ibm.com/docs/en/qsip/7.5?topic=recovery-backup-restore-applications
Configuring the QRadar Assistant app	https://www.ibm.com/docs/en/qradar-common?topic=app-configuring-qradar-assistant
QRadar apps overview	https://www.ibm.com/docs/en/qsip/7.5?topic=apps-qradar-overview
Managing authorized services	https://www.ibm.com/docs/en/qsip/7.5?topic=administration-managing-authorized-services

Section 2: Performance Optimization

This section accounts for 13% of the exam (8 out of 62 questions).

TASK: 2.1 Construct identity exclusions

SUBTASKS:

2.1.1. Display understanding of identity exclusions

- Identity exclusion searches
- Differences between identity exclusions searches and blocklists

2.1.2. Create identity exclusion searches

REFERENCES:

Identity exclusion search deviations	https://www.ibm.com/docs/en/qsip/7.5?topic=deviations-identity-exclusion-searches
Identity exclusion searches	https://www.ibm.com/docs/en/qsip/7.5?topic=searches-creating-identity-exclusion

TASK: 2.2 Deal with resource restrictions

SUBTASKS:

2.2.1. Document the function of resource restrictions in distributed and non-distributed environments

- Access wise
- Resource limitation wise
- Canceled searches
- Empty search results
- Inconsistent search results
- Limited search results

2.2.2. Configure resource restrictions

- Set resource restrictions to apply time or data limitations to event and flow searches
- Execution time, time span, record limit

2.2.3. Explain different types of resource restrictions

- User-based
- Role-based
- Tenant-based

REFERENCES:

Types of resource restrictions	https://www.ibm.com/docs/en/qsip/7.5?topic=searches-types-resource-restrictions
Configuring resource restrictions	https://www.ibm.com/docs/en/qsip/7.5?topic=searches-configuring-resource-restrictions
Restrictions to prevent resource-intensive searches	https://www.ibm.com/docs/en/qsip/7.5?topic=tasks-restrictions-prevent-resource-intensive-searches

TASK: 2.3 Rule configuration and tuning

SUBTASKS:

2.3.1. Explain different types of correlation rules

- Event rules
- Flow rules
- Common rules
- Offense rules

2.3.2. Create different types of correlation rules

- Rule creation wizard
- Test groups
- Response parameters

2.3.3. Tune rules

- Tuning wizard
- Basic rule tests familiarity

2.3.4. Identify expensive rules with QRadar support tools

REFERENCES:

QRadar tuning	https://www.ibm.com/docs/en/qsip/7.5?topic=deployment-qradar-tuning
Creating a custom rule	https://www.ibm.com/docs/en/qsip/7.5?topic=rules-creating-custom-rule
IBM QRadar building blocks	https://www.ibm.com/docs/en/qsip/7.5?topic=phase-qradar-building-blocks
Creating an OR condition within the CRE	https://www.ibm.com/docs/en/qsip/7.5?topic=phase-creating-condition-within-cre
Guidelines for tuning system performance	https://www.ibm.com/docs/en/qsip/7.5?topic=phase-guidelines-tuning-system-performance
Troubleshooting Custom Rule performance with findExpensiveCustomRules.sh	https://www.ibm.com/support/pages/qradar-troubleshooting-custom-rule-performance-findexpensivecustomrulessh
Custom rules	https://www.ibm.com/docs/en/qsip/7.5?topic=rules-custom

TASK: 2.4 Index management

SUBTASKS:

2.4.1. Enable indexes

2.4.2. Enable payload indexing

2.4.3. Describe the use of index management

- What is an index
- Reading the index management interface

2.4.4. Configure retention period for payload indexes

REFERENCES:

Enabling indexes	https://www.ibm.com/docs/en/qsip/7.5?topic=management-enabling-indexes
Index management	https://www.ibm.com/docs/en/qsip/7.5?topic=tasks-index-management
Configuring the retention period for payload indexes	https://www.ibm.com/docs/en/qsip/7.5?topic=management-configuring-retention-period-payload-indexes
Enabling payload indexing to optimize search times	https://www.ibm.com/docs/en/qsip/7.5?topic=management-enabling-payload-indexing-optimize-search-times

TASK: 2.5 Search management

SUBTASKS:

2.5.1. Manage saved searches

2.5.2. Manage search results

- Explain different types of parameters (new search, save results, cancel, delete, notify, view)

REFERENCES:

Scheduled search	https://www.ibm.com/docs/en/qsip/7.5?topic=searches-scheduled-search
Advanced search options	https://www.ibm.com/docs/en/qsip/7.5?topic=searches-advanced-search-options
Saving search criteria	https://www.ibm.com/docs/en/qsip/7.5?topic=searches-saving-search-criteria
Quick filter search options	https://www.ibm.com/docs/en/qsip/7.5?topic=searches-quick-filter-search-options
Finding IOCs quickly with lazy search	https://www.ibm.com/docs/en/qsip/7.5?topic=searches-finding-iocs-quickly-lazy-search
Using a subsearch to refine search results	https://www.ibm.com/docs/en/qsip/7.5?topic=searches-using-subsearch-refine-search-results
Adding filters to improve search performance	https://www.ibm.com/docs/en/qsip/7.5?topic=phase-adding-filters-improve-search-performance
Searching for offenses that are indexed on a custom property	https://www.ibm.com/docs/en/qsip/7.5?topic=searches-searching-offenses-that-are-indexed-custom-property
Manage search results	https://www.ibm.com/docs/en/qsip/7.4?topic=SS42VS_7.4/com.ibm.qradar.doc/t_qrm_ug_man_srch_rslts.html

TASK: 2.6 Manage routing rules and event forwarding

SUBTASKS:

2.6.1. Explain routing rules configuration and usage

- Different routing options for rules
- Create a routing rule

REFERENCES:

Routing options for rules	https://www.ibm.com/docs/en/qsip/7.5?topic=data-routing-options-rules
Configuring routing rules to forward data	https://www.ibm.com/docs/en/qsip/7.5?topic=systems-configuring-routing-rules-forward-data

Section 3: Data Source Configuration

This section accounts for 14% of the exam (9 out of 62 questions).

TASK: 3.1 Manage flow sources

SUBTASKS:

3.1.1. Understand flow sources

- What are flow sources
- What are the types
- External versus internal

3.1.2. Add or edit a flow source

3.1.3. Enable, disable, and delete a flow source

3.1.4. Understand Flow source alias

- Add
- Delete

REFERENCES:

Types of flow sources	https://www.ibm.com/docs/en/qradar-on-cloud?topic=sources-types-flow
Adding a flow source	https://www.ibm.com/docs/en/qsip/7.5?topic=sources-adding-flow-source
Adding or editing a flow source	https://www.ibm.com/docs/en/qradar-on-cloud?topic=sources-adding-editing-flow-source
Flow sources	https://www.ibm.com/docs/en/qsip/7.5?topic=configuration-flow-sources
Flow source aliases	https://www.ibm.com/docs/en/qsip/7.5?topic=sources-flow-source-aliases
Enabling flow sources	https://www.ibm.com/docs/en/qsip/7.5?topic=sources-enabling-flow
Deleting a Flow Source	https://www.ibm.com/docs/en/qsip/7.5?topic=sources-deleting-flow-source

TASK: 3.2 Manage log sources

SUBTASKS:

3.2.1. Add log sources

3.2.2. Filter log sources

3.2.3. Test log sources

3.2.4. Bulk add/edit log sources

3.2.5. Disconnected log collector (DLC)

- Understanding
- Collecting events

REFERENCES:

Gateway log source	https://www.ibm.com/docs/en/dsm?topic=management-gateway-log-source
DSM Editor overview	https://www.ibm.com/docs/en/qradar-on-cloud?topic=qradar-dsm-editor-overview

Protocol configuration options	https://www.ibm.com/docs/en/dsm?topic=configuration-protocol-options
Adding a log source to receive events	https://www.ibm.com/docs/en/qradar-common?topic=app-adding-log-source-receive-events
QRadar: How does coalescing work in QRadar?	https://www.ibm.com/support/pages/qradar-how-does-coalescing-work-qradar
Communication between WinCollect agents and QRadar	https://www.ibm.com/docs/en/qradar-common?topic=wincollect-communication-between-agents-qradar
Testing log sources	https://www.ibm.com/docs/en/qradar-common?topic=app-testing-log-sources
Filtering log sources	https://www.ibm.com/docs/en/qradar-common?topic=app-filtering-log-sources
QRadar Log Source Management App 7.0	https://www.securitylearningacademy.com/course/view.php?id=5744
Managing Disconnected Log Collectors with the QRadar Log Source Management app	https://www.securitylearningacademy.com/course/view.php?id=5016

TASK: 3.3 Export event and flow data

SUBTASKS:

3.3.1. Export events from QRadar

3.3.2. Export flow data

REFERENCES:

Exporting events	https://www.ibm.com/docs/en/qsip/7.5?topic=investigation-exporting-events
Viewing normalized events	https://www.ibm.com/docs/en/qsip/7.5?topic=monitoring-viewing-normalized-events
Introduction to QRadar events	https://www.securitylearningacademy.com/course/view.php?id=6585
Insufficient disk space to export data	https://www.ibm.com/docs/en/qsip/7.5?topic=appliances-insufficient-disk-space-export-data
Exporting flows	https://www.ibm.com/docs/en/qsip/7.5?topic=data-exporting-flows

TASK: 3.4 Vulnerability information source configuration

SUBTASKS:

3.4.1. Understand QRadar vulnerability manager deployments

3.4.2. Add scanners to QVM deployment

3.4.3. Understand QVM

3.4.4. Configure vulnerability scans

3.4.5. Add third-party scanners to QRadar

3.4.6. Install the Java Cryptography Extension on QRadar

3.4.7. Integrate unsupported third-party vulnerability scanners using the AXIS format

REFERENCES:

Scan policies	https://www.ibm.com/docs/en/qsip/7.5?topic=configuration-scan-policies
Risk score details	https://www.ibm.com/docs/en/qsip/7.5?topic=scores-risk-score-details
Installations and deployments	https://www.ibm.com/docs/en/qsip/7.5?topic=manager-installations-deployments
Common Vulnerability Scoring System (CVSS)	https://www.ibm.com/docs/en/qsip/7.5?topic=vulnerabilities-common-vulnerability-scoring-system-cvss

Deploying a dedicated QRadar Vulnerability Manager processor appliance	https://www.ibm.com/docs/en/qsip/7.5?topic=deployment-deploying-dedicated-qradar-vulnerability-manager-processor-appliance
Options for adding scanners to your QRadar Vulnerability Manager deployment	https://www.ibm.com/docs/en/qsip/7.5?topic=id-options-adding-scanners-your-qradar-vulnerability-manager-deployment
Scan configuration	https://www.ibm.com/docs/en/qsip/7.5?topic=manager-scan-configuration
Supported vulnerability scanners	https://www.ibm.com/docs/en/SS42VS_DSM/pdf/b_vuln.pdf
Overview of QRadar Vulnerability Manager	https://www.ibm.com/docs/en/qsip/7.5?topic=manager-overview-qradar-vulnerability
QRadar Vulnerability Manager deployments	https://www.ibm.com/docs/en/qsip/7.5?topic=overview-qradar-vulnerability-manager-deployments

TASK: 3.5 Manage custom event and flow properties

SUBTASKS:

3.5.1. Understand custom event and flow properties

3.5.2. Create a custom property

3.5.3. Modify or delete a custom property

3.5.4. Define custom properties using expressions

REFERENCES**:**

Custom event and flow properties	https://www.ibm.com/docs/en/qsip/7.5?topic=siem-custom-event-flow-properties
Defining custom properties by using custom property expressions	https://www.ibm.com/docs/en/qsip/7.5?topic=cefp-defining-custom-properties-by-using-custom-property-expressions
Creating a custom property	https://www.ibm.com/docs/en/qsip/7.5?topic=properties-creating-custom-property
Modifying or deleting a custom property	https://www.ibm.com/docs/en/qsip/7.5?topic=properties-modifying-deleting-custom-property

TASK: 3.6 Manage custom log source types

SUBTASKS:

3.6.1. Understand custom log source types

3.6.2. Create a custom log source type

REFERENCES**:**

Custom log source types	https://www.ibm.com/docs/en/qsip/7.5?topic=qradar-custom-log-source-types
Identity properties for event mappings	https://www.ibm.com/docs/en/qsip/7.5?topic=mapping-identity-properties-event-mappings
Referencing capture strings by using format string fields	https://www.ibm.com/docs/en/qradar-on-cloud?topic=pcide-referencing-capture-strings-by-using-format-string-fields
Creating a custom log source type to parse events	https://www.ibm.com/docs/en/qsip/7.5?topic=types-creating-custom-log-source-type-parse-events

TASK: 3.7 Manage data obfuscation

SUBTASKS:

3.7.1. Understand data obfuscation

- profiles
- expressions

3.7.2. Create a data obfuscation profile

3.7.3. Create a data obfuscation expression

3.7.4. View deobfuscated data

3.7.5. Edit or disable obfuscation expressions created in previous releases

REFERENCES**:**

Data obfuscation expressions	https://www.ibm.com/docs/en/qsip/7.5?topic=protection-data-obfuscation-expressions
De-obfuscating data so that it can be viewed in the console	https://www.ibm.com/docs/en/qsip/7.5?topic=soun-deobfuscating-data-so-that-it-can-be-viewed-in-console
Editing or disabling obfuscation expressions created in previous releases	https://www.ibm.com/docs/en/qsip/7.5?topic=soun-editing-disabling-obfuscation-expressions-created-in-previous-releases
Sensitive data protection	https://www.ibm.com/docs/en/qsip/7.5?topic=administration-sensitive-data-protection
Creating a data obfuscation profile	https://www.ibm.com/docs/en/qsip/7.5?topic=names-creating-data-obfuscation-profile
Creating data obfuscation expressions	https://www.ibm.com/docs/en/qsip/7.5?topic=names-creating-data-obfuscation-expressions

Section 4: Accuracy Tuning

This section accounts for 10% of the exam (6 out of 62 questions).

TASK: 4.1 Understand and implement ADE rules

SUBTASKS:

4.1.1. Understand anomaly rules

4.1.2. Understand threshold rules

4.1.3. Understand behavior rules

4.1.4. Create an anomaly detection rule

REFERENCES**:**

Anomaly detection rules	https://www.ibm.com/docs/en/qsip/7.5?topic=rules-anomaly-detection
Creating an anomaly detection rule	https://www.ibm.com/docs/en/qsip/7.5?topic=rules-creating-anomaly-detection-rule

TASK: 4.2 Manage and use building blocks

SUBTASKS:

4.2.1. Tune building blocks

4.2.2. Review the building blocks in the use case manager

4.2.3. Add servers to building blocks

REFERENCES**:**

Tuning building blocks	https://www.ibm.com/docs/en/qsip/7.5?topic=blocks-tuning-building
QRadar Use Case Manager app	https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-use-case-manager-app
Servers and building blocks	https://www.ibm.com/docs/en/qsip/7.5?topic=tuning-servers-building-blocks

TASK: 4.3 Manage content packs

SUBTASKS:

4.3.1. Understand the types of security content

4.3.2. Install extensions using extensions management

4.3.3. Synchronize dashboard templates from content extensions

4.3.4. Uninstall a content extension

4.3.5. Install Threat Monitoring extension

REFERENCES**:**

QRadar Assistant app	https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-assistant-app
Types of security content	https://www.ibm.com/docs/en/qsip/7.5?topic=content-types-security
Installing extensions by using Extensions Management	https://www.ibm.com/docs/en/qsip/7.5?topic=content-installing-extensions-by-using-extensions-management
IBM QRadar Security Threat Monitoring Content Extension	https://www.ibm.com/docs/en/qsip/7.5?topic=integration-qradar-security-threat-monitoring-content-extension
Synchronizing dashboard templates from content extensions	https://www.ibm.com/docs/en/qradar-common?topic=app-synchronizing-dashboard-templates-from-content-extensions
Uninstalling a content extension	https://www.ibm.com/docs/en/qsip/7.5?topic=content-uninstalling-extension

TASK: 4.4 Distinguish native information sources

SUBTASKS:

4.4.1. Manage remote networks and remote services

4.4.2. Install and manage the QRadar Threat Intelligence app

4.4.3. Configure a threat feed to populate a reference set

4.4.4. Review network hierarchy

4.4.5. Understand building blocks role

REFERENCES**:**

Threat intelligence feeds	https://www.ibm.com/docs/en/qradar-common?topic=app-threat-intelligence-feeds
QRadar Threat Intelligence app	https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-threat-intelligence-app
Reviewing your network hierarchy	https://www.ibm.com/docs/en/qradar-common?topic=tuning-reviewing-your-network-hierarchy
Remote networks and services configuration	https://www.ibm.com/docs/en/qsip/7.5?topic=administration-remote-networks-services-configuration

TASK: 4.5 Configure integrations

SUBTASKS:

4.5.1. Configure MaxMind

4.5.2. Manage X-Force integration

4.5.3. Install and configure IBM X-Force Exchange plug-in for QRadar

4.5.4. Enable the X-Force Threat Intelligence feed

REFERENCES**:**

IBM X-Force integration	https://www.ibm.com/docs/en/qsip/7.5?topic=administration-x-force-integration
Enabling the X-Force Threat Intelligence feed	https://www.ibm.com/docs/en/qsip/7.5?topic=feed-enabling-x-force-threat-intelligence
Enabling the X-Force Threat Intelligence feed	https://www.ibm.com/docs/en/qsip/7.5?topic=feed-enabling-x-force-threat-intelligence#t_qradar_ag_xforce_enable
QRadar: Configuring a MaxMind account for geographic data updates	https://www.ibm.com/support/pages/node/1172842
IBM X-Force Exchange plug-in for QRadar	https://www.ibm.com/docs/en/qsip/7.5?topic=integration-x-force-exchange-plug-in-qradar

Section 5: User Management

This section accounts for 6% of the exam (4 out of 62 questions).

TASK: 5.1 Manage users

SUBTASKS:

5.1.1. Understand how to create a user account

- Understand different parameters:
  - User role
  - Security profile
  - Override system inactivity timeout

5.1.2. Validate user account creation requirements

- Deploy after user creation

5.1.3. Understand how to edit a user account

- User Management window
- Use of the Advanced Filter to search by user role or security profile when editing

5.1.4. Validate user account edition requirements

- Deploy after user edit

5.1.5. Disable a user account

5.1.6. Delete a user account

5.1.7. Delete saved searches of a deleted user

REFERENCES**:**

Configuring inactivity timeout for a user	https://www.ibm.com/docs/en/qsip/7.5?topic=authentication-configuring-inactivity-timeout-user
Deleting saved searches of a deleted user	https://www.ibm.com/docs/en/qsip/7.5?topic=accounts-deleting-saved-searches-deleted-user
Editing a user account	https://www.ibm.com/docs/en/qsip/7.5?topic=accounts-editing-user-account
Creating a user account	https://www.ibm.com/docs/en/qsip/7.5?topic=accounts-creating-user-account
Deleting a user account	https://www.ibm.com/docs/en/qsip/7.5?topic=accounts-deleting-user-account
Disabling a user account	https://www.ibm.com/docs/en/qsip/7.5?topic=accounts-disabling-user-account

TASK: 5.2 Create and update security profiles

SUBTASKS:

5.2.1. Understand security profiles

- Domains
- Permission precedence

5.2.2. Create a security profile

5.2.3. Edit a security profile

5.2.4. Duplicate a security profile

5.2.5. Delete a security profile

REFERENCES:

Security profiles	https://www.ibm.com/docs/en/qsip/7.5?topic=management-security-profiles
Permission precedence	https://www.ibm.com/docs/en/qsip/7.5?topic=profiles-permission-precedence
Creating a security profile	https://www.ibm.com/docs/en/qsip/7.5?topic=profiles-creating-security-profile
Deleting a security profile	https://www.ibm.com/docs/en/qsip/7.5?topic=profiles-deleting-security-profile
Editing a security profile	https://www.ibm.com/docs/en/qsip/7.5?topic=profiles-editing-security-profile
Duplicating a security profile	https://www.ibm.com/docs/en/qsip/7.5?topic=profiles-duplicating-security-profile

TASK: 5.3 Create and update user roles

SUBTASKS:

5.3.1. Understand user roles

- QRadar functions that the user can access

5.3.2. Create a user role

5.3.3. Edit a user role

5.3.4. Delete a user role

REFERENCES:

User roles	https://www.ibm.com/docs/en/qsip/7.5?topic=management-user-roles
Creating a user role	https://www.ibm.com/docs/en/qsip/7.5?topic=roles-creating-user-role
Editing a user role	https://www.ibm.com/docs/en/qsip/7.5?topic=roles-editing-user-role
Deleting a user role	https://www.ibm.com/docs/en/qsip/7.5?topic=roles-deleting-user-role

TASK: 5.4 Manage user authentication and authorization

SUBTASKS:

5.4.1. User authentication

5.4.2. System authentication

5.4.3. RADIUS authentication

5.4.4. TACACS authentication

5.4.5. LDAP

5.4.6. SAML single sign-on authentication

REFERENCES:

User authentication	https://www.ibm.com/docs/en/qsip/7.5?topic=management-user-authentication
Configuring LDAP authentication	https://www.ibm.com/docs/en/qsip/7.5?topic=authentication-configuring-ldap
SAML single sign-on authentication	https://www.ibm.com/docs/en/qsip/7.5?topic=authentication-saml-single-sign
LDAP authentication	https://www.ibm.com/docs/en/qsip/7.5?topic=authentication-ldap
Configuring RADIUS authentication	https://www.ibm.com/docs/en/qsip/7.5?topic=authentication-configuring-radius
Configuring system authentication	https://www.ibm.com/docs/en/qsip/7.5?topic=authentication-configuring-system
Configuring TACACS authentication	https://www.ibm.com/docs/en/qsip/7.5?topic=authentication-configuring-tacacs

Section 6: Reporting, Searching, and Offense Management

This section accounts for 13% of the exam (8 out of 62 questions).

TASK: 6.1 Manage reports

SUBTASKS:

6.1.1. Create reports with different chart types

- Chart types - data types

6.1.2. Create custom reports

- Selecting frequency of report generation
- Options for different distribution channels

6.1.3. Explain difference between scheduled reports and reports run on raw data

REFERENCES**:**

Chart types	https://www.ibm.com/docs/en/qsip/7.5?topic=management-chart-types
Report tab toolbar	https://www.ibm.com/docs/en/qsip/7.5?topic=management-report-tab-toolbar
Creating custom reports	https://www.ibm.com/docs/en/qsip/7.5?topic=management-creating-custom-reports
Deleting generated content	https://www.ibm.com/docs/en/qsip/7.5?topic=management-deleting-generated-content
Manually generating a report	https://www.ibm.com/docs/en/qsip/7.5?topic=management-manually-generating-report

TASK: 6.2 Utilize different search types

SUBTASKS:

6.2.1. Save search criteria for further use

6.2.2. Use AQL for searches

6.2.3. When to use quick search

6.2.4. Query with dynamic search

REFERENCES**:**

Querying with dynamic search	https://www.ibm.com/docs/en/qsip/7.5?topic=searches-querying-dynamic-search
Converting a saved search to an AQL string	https://www.ibm.com/docs/en/qsip/7.5?topic=options-converting-saved-search-aql-string
AQL search string examples	https://www.ibm.com/docs/en/qsip/7.5?topic=options-aql-search-string-examples

TASK: 6.3 Manage offenses

SUBTASKS:

6.3.1. Understand how offense renaming works

- Hot and Cold rules

6.3.2. Demonstrate how offense indexing works

6.3.3. Demonstrate how offense indexing is related to offense chaining

6.3.4. Set offense prioritization with rule action options

6.3.5. Implement Soft Clean SIM data clean

6.3.6. Understand how and why to protect offenses

REFERENCES:

Offense chaining	https://www.ibm.com/docs/en/qsip/7.5?topic=management-offense-chaining
Offense indexing	https://www.ibm.com/docs/en/qsip/7.5?topic=management-offense-indexing
Protecting offenses	https://www.ibm.com/docs/en/qsip/7.5?topic=retention-protecting-offenses
Offense prioritization	https://www.ibm.com/docs/en/qsip/7.5?topic=management-offense-prioritization
Cleaning the SIM data model	https://www.ibm.com/docs/en/qsip/7.5?topic=phase-cleaning-sim-data-model
How QRadar Offense Renaming works	https://community.ibm.com/community/user/security/blogs/ashish-kothekar/2021/07/07/how-qradar-offense-renaming-works

TASK: 6.4 Sharing content among users

SUBTASKS:

6.4.1. Share reports with other users

- Understand the available sharing options

6.4.2. Sharing dashboard items with other users

- Requirement to share a dashboard
- Available Parameters

6.4.3. How to share a search criteria

REFERENCES:

Sharing report groups	https://www.ibm.com/docs/en/qsip/7.5?topic=groups-sharing-report
QRadar: Sharing Dashboard Items	https://www.ibm.com/support/pages/qradar-sharing-dashboard-items

Section 7: Tenants and Domains

This section accounts for 8% of the exam (5 out of 62 questions).

TASK: 7.1 Differentiate network hierarchy and domain definition

SUBTASKS:

7.1.1. Assign parts of the network hierarchy to specific domains

7.1.2. Show that an event is assigned to a domain

- A single log source may provide events to multiple domains

7.1.3. Understand constraints for defining the network hierarchy

REFERENCES**:**

Domain segmentation	https://www.ibm.com/docs/en/qsip/7.5?topic=sources-domain-segmentation
Guidelines for defining your network hierarchy	https://www.ibm.com/docs/en/qsip/7.5?topic=hierarchy-guidelines-defining-your-network
Domains and log sources in multitenant environments	https://www.ibm.com/docs/en/qsip/7.5?topic=management-domains-log-sources
Domain segmentation	https://www.ibm.com/docs/en/qsip/7.5?topic=administration-domain-segmentation
Network hierarchy updates in a multitenant deployment	https://www.ibm.com/docs/en/qsip/7.5?topic=management-network-hierarchy-updates-in-multitenant-deployment
QRadar Multi-tenancy, Domains and Log Source Groups - Jose Bravo video	https://www.youtube.com/watch?v=Xrn7q9v3vAk

TASK: 7.2 Manage domains and tenants

SUBTASKS:

7.2.1. Understand domains and log sources in multi-tenant environments

- Domain segmentation
- Automatic log source detection

7.2.2. Create domains

7.2.3. Configure Apps in a multi-tenant environment

7.2.4. Manage retention policies in a multi-tenant environment

REFERENCES**:**

Creating domains	https://www.ibm.com/docs/en/qradar-on-cloud?topic=segmentation-creating-domains
Provisioning a new tenant	https://www.ibm.com/docs/en/qradar-on-cloud?topic=management-provisioning-new-tenant
Domain definition and tagging	https://www.ibm.com/docs/en/qradar-on-cloud?topic=segmentation-domain-definition-tagging
Retention policies for tenants	https://www.ibm.com/docs/en/qsip/7.5?topic=management-retention-policies-tenants
Using Domain Management window to create domains	https://www.ibm.com/docs/en/qsip/7.5?topic=segmentation-creating-domains
Installing apps in a multi-tenant environment	https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-overview
Domains and log sources in multitenant environments	https://www.ibm.com/docs/en/qsip/7.5?topic=management-domains-log-sources

TASK: 7.3 Allocate licenses for multi-tenant

SUBTASKS:

7.3.1. Monitor license usage in multi-tenant deployments

- How to view EPS rates per log source
- How to view EPS rates per domain
- How to view the EPS rate for an individual log source
- How to view the EPS rate for an individual domain
- Show that there is no spillover handling for per-tenant EPS limits

REFERENCES**:**

New features in QRadar 7.2.6	https://www.ibm.com/support/pages/qradar-open-mic-11-new-features-qradar-726-15-dec-2015-replay-available
Monitoring license usage in multitenant deployments	https://www.ibm.com/docs/en/qsip/7.5?topic=management-monitoring-license-usage
Open Mic: Page 22	https://ibm.biz/BdPqC9

TASK: 7.4 Assign users to tenants

SUBTASKS:

7.4.1. Understand user roles in a multi-tenant environment

- Service provider
- Tenants

7.4.2. Partition data by use of security profiles

REFERENCES**:**

User roles in a multitenant environment	https://www.ibm.com/docs/en/qsip/7.5?topic=management-user-roles
Security profiles	https://www.ibm.com/docs/en/qsip/7.5?topic=management-security-profiles

Section 8: Troubleshooting

This section accounts for 16% of the exam (10 out of 62 questions).

TASK: 8.1 Review and respond to system notifications

SUBTASKS:

8.1.1. Create system notifications

- System Notification Rule (or any rule with 'Notification' Response)

8.1.2. Locate system notifications

- Under the bell icon on GUI
- Custom Rule is System: Notification events in Log Activity

8.1.3. React to system notifications

REFERENCES**:**

License expired	https://www.ibm.com/docs/en/qsip/7.5?topic=appliances-license-expired
Accumulator is falling behind	https://www.ibm.com/docs/en/qsip/7.5?topic=appliances-accumulator-is-falling-behind
Maximum active offenses reached	https://www.ibm.com/docs/en/qsip/7.5?topic=appliances-maximum-active-offenses-reached
Disk usage system notifications	https://www.ibm.com/docs/en/qsip/7.5?topic=notifications-disk-usage-system
Backup unable to complete a request	https://www.ibm.com/docs/en/qsip/7.5?topic=appliances-backup-unable-complete-request
How to deal with unwanted notifications	https://www.ibm.com/support/pages/qradar-how-deal-unwanted-notifications
QRadar system notifications	https://www.ibm.com/docs/en/qsip/7.5?topic=support-qradar-system-notifications

TASK: 8.2 Troubleshoot common documented issues

SUBTASKS:

8.2.1. Scenarios from the "Technical Notes 101" page

REFERENCES**:**

Technical Notes 101	https://www.ibm.com/community/qradar/home/knowledge
Cleaning the SIM data model	https://www.ibm.com/docs/en/qsip/7.5?topic=phase-cleaning-sim-data-model
QRadar Troubleshooting and System Notifications Guide	https://www.ibm.com/docs/en/SS42VS_7.5/pdf/b_qradar_system_notifications.pdf
What information should be submitted with a QRadar service request?	https://www.ibm.com/support/pages/getting-help-what-information-should-be-submitted-qradar-service-request

TASK: 8.3 Configure, manage and troubleshoot applications

SUBTASKS:

8.3.1. Use "recon" to troubleshoot apps

8.3.2. Configure Use Case Manager

8.3.3. Configure QDI

REFERENCES**:**

QRadar Deployment Intelligence app	https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-deployment-intelligence-app
Installing QRadar Deployment Intelligence	https://www.ibm.com/docs/en/qradar-common?topic=app-installing-qradar-deployment-intelligence
How to use Recon to troubleshoot QRadar applications	https://www.ibm.com/support/pages/qradar-how-use-recon-troubleshoot-qradar-applications
Configuring QRadar Use Case Manager	https://www.ibm.com/docs/en/qradar-common?topic=icc-creating-authorized-service-token#c_Qapps_LDAP_authTokens

TASK: 8.4 Perform healthchecks

SUBTASKS:

8.4.1. Perform Daily Tasks

8.4.2. Perform Weekly Tasks

REFERENCES**:**

Maintaining QRadar 101	https://www.ibm.com/support/pages/system/files/inline-files/$FILE/OpenMic_MaintainingQRadar101_updated2.pdf
Maintaining QRadar 101 - Open Mic	https://www.securitylearningacademy.com/enrol/index.php?id=4159
Perform healthchecks using ThreadTop	https://www.ibm.com/support/pages/qradar-using-threadtop-determine-qradar-process-load
Perform healthchecks defect inspector	https://www.ibm.com/support/pages/qradar-how-use-defect-inspector-identify-reported-issues
Perform healthchecks Wincollect Agent	https://www.ibm.com/support/pages/wincollect-agent-error-message-configuration-file-fingerprints-dont-match
Perform healthchecks Test Tomcat connection	https://www.ibm.com/support/pages/node/6590417
Perform healthchecks Collecting system information	https://www.ibm.com/support/pages/qradar-collecting-system-information-using-optqradarbinmyver-v

TASK: 8.5 Basic GUI REST-API usage

SUBTASKS:

8.5.1. Use the REST-API via the GUI on the console

- Pick an endpoint and show how to access it

REFERENCES**:**

API error messages	https://www.ibm.com/docs/en/qradar-common?topic=versions-api-error-messages
Accessing the interactive API documentation page	https://www.ibm.com/docs/en/qradar-common?topic=versions-accessing-interactive-api-documentation-page
QRadar API 101 - Jose Bravo video	https://www.youtube.com/watch?v=swGI5QWB29g