PassQueen
a.k.a dumpsqueen.com

# IBM Security QRadar SIEM V7.5 Administration

## IBM C1000-156

**Version Demo**

**Total Demo Questions: 8**

**Total Premium Questions: 82**

**Buy Premium PDF**

https://passqueen.com

support@passqueen.com

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, QRadar Architecture | 12 |
| Topic 2, QRadar Administration | 45 |
| Topic 3, Log Source Management | 8 |
| Topic 4, Network Hierarchy | 2 |
| Topic 5, Rules | 9 |
| Topic 6, Offense Management | 3 |
| Topic 7, Reports | 3 |
| Total | 82 |

QUESTION NO: 1

An organization is preparing a replacement appliance to act as the secondary host in a QRadar high-availability pair.

Which two (2) requirements must be satisfied before the appliances can be configured as an HA pair?

**A.** The appliances must be the same appliance type

**B.** The appliances must run the same QRadar software version and fix pack level

**C.** The appliances must use the same management IP address

**D.** The appliances must use the same host name

**E.** The appliances must be assigned to different QRadar domains

**ANSWER: A B**

**Explanation:**

The primary and secondary appliances must be compatible for an HA configuration. In particular, they must be the same appliance type and must run the same QRadar software version, including the applicable fix pack level. These requirements ensure that the secondary can synchronize and assume the functions of the primary appliance during a failover.

The secondary appliance does not need to be configured with the same management IP address as the primary. Each HA host has its own management address, while the HA configuration provides a separate virtual IP address for services that must remain available after failover.

**QUESTION NO: 2**

Which profile database does the Server Discovery function use to discover several types of servers on a network?

**A.** Flow profile database

**B.** Network profile database

**C.** Domain profile database

**D.** Asset profile database

**ANSWER: D**

**Explanation:**

The correct answer is **Asset profile database**. In QRadar, the Asset Profiler maintains an asset-profile database containing the information QRadar learns about hosts in the environment, such as IP and MAC addresses, host names, operating-system details, services, ports, and observed network activity. Server Discovery uses this asset information to identify and classify systems that provide particular server functions on the network. This association is important because QRadar does not treat server identification as a separate, isolated inventory; it builds server discovery on the collected and correlated asset knowledge already maintained by the Asset Profiler.

As events, flows, vulnerability data, and other asset updates are processed, QRadar enriches the relevant asset records. The Server Discovery capability can use those records to recognize the characteristics associated with server types and present discovered servers for administration and security-monitoring purposes. Maintaining accurate asset profiles therefore supports reliable server identification and improves the context available during investigations. IBM's QRadar documentation describes the Asset Profiler as the component that discovers and maintains asset information, including the use of server discovery with asset-profile data. See the IBM QRadar Asset Profiler documentation and IBM documentation on Server Discovery.

**QUESTION NO: 3**

Which is the default port for the first NetFlow flow source that is configured in QRadar?

**A.** 8413

**B.** 21

**C.** 2055

**D.** 514

**ANSWER: C**

**Explanation:**

**2055** is the default listening port assigned when the first NetFlow flow source is configured in IBM QRadar. NetFlow exporters, such as routers, switches, and firewalls, send flow records to a Flow Collector or Flow Processor so QRadar can create network-flow data for searches, dashboards, offenses, and network-activity analysis. During the initial NetFlow flow-source setup, QRadar presents UDP port 2055 as the default receiver port. This aligns with the commonly used NetFlow collector port and allows an administrator to use the standard setting when configuring the exporting network device.

The listening port must match the destination UDP port configured on the NetFlow-exporting device. Administrators can choose a different unused port when operational requirements, existing listener assignments, firewall policy, or device configuration require it; however, that does not change the default presented for the first configured NetFlow flow source. IBM's QRadar documentation for flow-source administration identifies the NetFlow configuration workflow and its default port behavior. For additional context on QRadar flow collection and supported flow sources, see IBM QRadar: Adding a NetFlow flow source and IBM QRadar: Flow sources.

**QUESTION NO: 4**

When will events or flows stop contributing to an offense?

**A.** When the offense becomes dormant

**B.** When the offense becomes inactive

**C.** After the offense is assigned to an analyst

**D.** When you protect the offense

**ANSWER: A**

**Explanation:**

Events and flows stop contributing to an offense when the offense becomes dormant. In QRadar, an offense is initially active while it is receiving contributing events or flows from the rules, anomaly detection, or other offense-generating mechanisms. After the configured period without further contributing activity, QRadar changes the offense to the dormant state. Dormancy indicates that the offense is no longer being updated with newly matching events or flows, preserving the offense as a record of the activity already correlated while preventing additional unrelated or later activity from extending it indefinitely.

This lifecycle behavior helps analysts distinguish offenses that still have ongoing contributing evidence from those whose correlation activity has ceased. If subsequent activity meets the relevant offense-creation criteria, QRadar processes it according to its correlation and offense rules rather than treating assignment or protection status as a control on event and flow contribution. The dormant state is therefore the relevant threshold for determining when contribution to that offense ends. IBM describes offense status and lifecycle management in its QRadar documentation: IBM QRadar offense management and IBM QRadar SIEM 7.5 offense management.

**QUESTION NO: 5**

An administrator is reviewing the QRadar network hierarchy after adding a new cloud environment that uses publicly routable address space.

Which two (2) statements describe valid uses of the network hierarchy?

**A.** Define IP address ranges that QRadar considers local

**B.** Organize address ranges into network objects and groups

**C.** Automatically classify every RFC 1918 address as local

**D.** Assign normalized QIDs to incoming events

**E.** Create log source configurations for network devices

**ANSWER: A B**

**Explanation:**

The network hierarchy defines which IP address ranges QRadar considers local. Therefore, publicly routable cloud address ranges can be defined as local when they belong to the organization. The hierarchy also organizes address ranges into network objects and groups, which makes it possible to represent the organization's network structure in QRadar.

RFC 1918 address space is not automatically local unless it is included in the configured network hierarchy. The hierarchy does not assign a QID to events and does not replace the need to configure log sources.

## QUESTION NO: 6

An administrator receives a file with all the vital assets in the company and wants to import this file into QRadar. How must this import file be formatted?

**A.** CSV file in the format: IP address, Name, Weight, Description

**B.** JSON file in the format: IP address. Name, Weight, Domain

**C.** XML file in the format: IP address. Name, Weight, Domain

**D.** XLS file in the format: IP address, Name. Weight, Description

**ANSWER: A**

**Explanation:**

**CSV file in the format: IP address, Name, Weight, Description** is correct because QRadar's vital-asset import process uses a comma-separated values file to map each listed system to its associated vital-asset metadata. The IP address identifies the asset record that QRadar must update. Name provides a readable identifier for the vital asset, while Weight supplies the asset's relative business importance for QRadar risk evaluation and prioritization. Description stores supporting context about the system or why it is considered vital. Each asset is represented as a row in the CSV file, with the values arranged in the required field order so that QRadar can parse and apply the information consistently during import. Assigning appropriate asset weights is especially important because QRadar incorporates asset criticality into offense prioritization and risk-related analysis. Administrators should ensure that the IP addresses correspond to assets known to QRadar and that the CSV data is clean and consistently delimited before importing it through the asset-management workflow. IBM documents asset and vital-asset administration in the QRadar SIEM documentation: Importing vital asset information and Asset profiles.

## QUESTION NO: 7

An administrator wants QRadar asset profiles to contain both observed network information and known vulnerability information for managed systems.

Which two (2) sources can contribute information to QRadar asset profiles?

**A.** Network flow data

**B.** Vulnerability scan data

**C.** Rule-response email messages

**D.** Generated report output

**E.** Saved search results

**ANSWER: A B**

**Explanation:**

Network flow data can contribute observed information about assets, such as network activity and services associated with an IP address. Vulnerability scan data can contribute vulnerability and operating-system information obtained from supported vulnerability scanners. QRadar uses these sources to build and update asset profiles that provide context during investigations and offense analysis.

Rule-response email messages and report output are not asset-discovery sources. A saved search can retrieve information that is already stored, but it does not itself populate asset profiles.

## QUESTION NO: 8

An administrator enables event coalescing for a high-volume log source that repeatedly sends identical events. The administrator wants to reduce the number of stored event records while preserving the frequency of the repeated activity.

Which two (2) statements describe event coalescing?

**A.** It can reduce the number of stored records for repeated events

**B.** It preserves the frequency of repeated events in Event Count

**C.** It permanently discards all repeated-event information

**D.** It coalesces network flow records instead of events

**E.** It prevents repeated events from being evaluated by rules

**ANSWER: A B**

**Explanation:**

Event coalescing combines qualifying repeated events into a single event record and preserves the number of represented events in the Event Count field. This reduces the number of stored event records for repetitive activity while allowing analysts to determine how frequently the event occurred.

Event coalescing does not discard all evidence of repeated events, and it does not apply to network flow records. It also does not prevent the Custom Rules Engine from evaluating events that are received from the log source.