Redbooks
ibm.com/redbooks

IBM QRadar Version 7.3
Planning and Installation Guide

Elias Carabaguiaz
Fabian Alfaro
Francisco Villalobos
Jeffry Arias
Kenneth Gonzalez
Warren Perez

IBM

Redbooks

International Technical Support Organization

IBM QRadar Version 7.3: Planning and Installation Guide

January 2018

SG24-8412-00

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (January 2018)

This edition applies to IBM QRadar V7.3.0.

Contents

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

AppScan®	IBM®	Redbooks®
BigFix®	IBM Watson®	Redbooks (logo)  ®
Guardium®	QRadar®	Watson™

The following terms are trademarks of other companies:

ITIL is a Registered Trade Mark of AXELOS Limited.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Preface

With the advances of technology and the reoccurrence of data leaks, cyber security is a bigger challenge than ever before. Cyber attacks evolve as quickly as the technology itself, and hackers are finding more innovative ways to break security controls to access confidential data and to interrupt services. Hackers reinvent themselves using new technology features as a tool to expose companies and individuals. Therefore, cyber security cannot be reactive but must go a step further by implementing proactive security controls that protect one of the most important assets of every organization: the company's information.

This IBM® Redbooks® publication provides information about implementing IBM QRadar® for Security Intelligence and Event Monitoring (SIEM) and protecting an organization's networks through a sophisticated technology, which permits a proactive security posture. It is divided in to the following major sections to facilitate the integration of QRadar with any network architecture:

- Chapter 2, "Before the installation" on page 3 provides a review of important requirements before the installation of the product.
- Chapter 3, "Installing IBM QRadar V7.3" on page 57 provides step-by-step procedures to guide you through the installation process.
- Chapter 4, "After the installation" on page 77 helps you to configure additional features and perform checks after the product is installed.

QRadar is an IBM Security prime product that is designed to be integrated with corporate network devices to keep a real-time monitoring of security events through a centralized console. Through this book, any network or security administrator can understand the product's features and benefits.

Authors

This book was produced by group of specialists with previous experience working on different cybersecurity areas. These six engineers work for IBM Security in the XForce Command Center located in Heredia, Costa Rica.

Elias Carabaguiaz is a Security Intelligence Analyst at IBM Security in Costa Rica. He is a graduated computer engineer with more than 4 years of experience working as a Security Specialist. His technical skills include QRadar, Proventia IPS/IDS, Snort, FireEye, and SourceFire, and he also holds a Project Management Diploma. His previous experience includes Datacenter and Virtualization Engineer, Computer Engineer Teacher, and Security Consultant. Elias is an active contributor in Tecnología Vital Magazine.

Fabian Alfaro has been working with IBM Security for almost 3 years as a QRadar Administrator for the Managed SIEM team in Heredia, Costa Rica. He has more than 6 years of experience in IT and 4 of them working in security technologies. He has broad experience in Juniper firewalling solutions and holds certifications like JNCSP-SEC, JNCIP-SEC, and JNCIS-ENT. He is also certified Associate Analyst in QRadar. His skills include providing technical support of routing, switching, and security solutions. Fabian used to work as a Program Ready Trainer for new engineers while he worked at Juniper Technical Assistance Center in Costa Rica.

Francisco Villalobos is part of the Managed SIEM Security Analysts team located in Heredia, Costa Rica. He has been working for this team since 2015, and holds 6 years of experience working with IT technologies. His areas of expertise include customer services and problem solving. Francisco is a certified Associate Analyst in QRadar.

Jeffry Arias is an information systems engineer with more than 8 years of experience in IT. His background includes activities such as Windows and Linux servers administration, VMware and vCenter management, software development (C++, Java, CSS, HTML, and so on), database administration (Oracle and MySQL), and network administration focused on Cisco and Dell devices. Jeffry is certified as Associate Administrator on QRadar V7.2.8 and an Associate Analyst on QRadar v7.2.6.

Kenneth Gonzalez has more than 10 years of experience on IT services. He used to work as Project Manager and Consultant for telecommunication and security projects to implement Business Continuity and Disaster Recovery plans, improve process controls, and monitor systems, such as IPS, Firewalls, UTMs, Management Servers, and so forth. Kenneth's qualifications include Certified Ethical Hacking V9, Certified Information Security Manager QRadar V7.2.6, CISA, CISSP, ITILv3, SSCP, among others.

Warren Perez has been working as a SIEM Administrator for the last 2 years in IBM Security. His skills on QRadar include user access management, verifying availability, monitoring database loads, installing and monitoring system patches and upgrades, and so on. Warren has previous experience working as an administrator of Active Directory systems, Linux, and Windows servers and load balancing applications.

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

Introduction

This chapter provides general information about SIEM technologies and its use to fight against cyber crime. It includes the following topics:

- Overview of SIEM
- Why IBM QRadar for SIEM

1.1 Overview of SIEM

In cyber security, Security Information and Event Management (SIEM) is considered a series of technologies in charge of providing analysis, threat mitigation, and logging of security events across a determined network. SIEM provides a general view of all technical infrastructure, with specific data of security events, and the mitigation of those infrastructures.

SIEM includes functions, such as Security Information Management (SIM) and Security Event Management (SEM), into a single solution. To better understand SIEM, think of a solution that gathers data from security sources for analysis correlation and action upon possible threats. SIEM management offers a variety of functions in the following areas:

- Event and log collection
- Rule correlation
- Log source management
- Adaptability
- Data normalization and registry

This solution tries to solve scenarios where people cannot analyze advanced threats using the normal monitoring tools, on a general level, by using a business technical infrastructure and by unifying all the elements, which are typically agents in a hierarchical model, to gather events from endpoints, servers, and network equipment. It provides third-party interoperability so that many solutions can be integrated, which makes this product scalable and more robust. Piggeé describes the SIEM solution as "...a group of complex technologies that together provide a bird's-eye view into an infrastructure." (Piggeé, 2016)

1.2 Why IBM QRadar for SIEM

QRadar is one of the most popular SIEM solutions in the market today. It is a network management platform that provides situational awareness, event management, and data recollection into a central console. This console normalizes the data, correlates signatures, events, and flows, and analyzes traffic for any potential threat within a technical environment. QRadar uses a combination of flow-based network knowledge, event correlation, and asset-based vulnerability assessment.

2

Before the installation

This chapter provides information about the requirements that you need to check before you install IBM QRadar V7.3.0. The QRadar V7.3.0 release notes are covered in detail to provide information that is related to features that are supported and configuration options. This chapter also discusses the infrastructure requirements that can provide the best performance of QRadar when monitoring flows and events with a corporate network. It includes the following topics:

- Release notes, V7.3.0
- QRadar capabilities
- QRadar architecture
- Components
- Preferred practices
- Requirements

2.1 Release notes, V7.3.0

With any new version of QRadar, the developers try to add features requested by clients and users of the platforms. Those features introduce characteristics into the environment that can facilitate the detection of threats and improve the operative task of the console and other components of the QRadar platform.

QRadar V7.3.0 includes the following new features:

- Events Per Second (EPS) and Flows Per Minute (FPM) are combined into a shared license data. So, you can “split” the license between different devices.
- Updates the core of the console operative system Red Hat Enterprise Linux 7.3 with security enhancements and file system and storage improvements.
- Any new installation can use Logical Volume Management (LVM) on disks, so that you can now create, resize, or delete partitions.
- You can now install QRadar without an activation key. You can define the license later.
- The log source limits are removed, so that you can have a unlimited number of devices reporting into QRadar (as long as the device performance is allowed).
- QRadar V7.3.0 uses TLS v1.2 to secure the communications.
- Tenants create their on-reference data collections and their own custom properties.
- HA performance is improved for the Event Collector Appliances (15xx), which can reduce the downtime during a failover. Also, HA provides a new set of sensors to detect failover scenarios.
- The following new appliance types are now available:
  - An M5 xx29 for use as an All-in-One 3129, Flow Processor 1729, or an Event Processor 1629. 2.
  - An M5 xx48 high performance appliance for large systems or high throughput processing with 28 cores and 18TB of SSD storage.
- Updates for the use of the API to create new integrations and execute advanced task.
- Ariel Query Language (AQL) improvements are included, especially on queries and operators.
- QRadar V7.3.0 is updated to the app framework and app nodes.
- The user interfaces are improved (such as remote networks and services).
- QRadar V7.3.0 removes the Deployment Editor.

2.2 QRadar capabilities

QRadar provides the following capabilities, with specific functions, each of which are described briefly in the sections that follow:

- Log Activity
- Network Activity
- Assets
- Offenses
- Reports
- Data collection
- QRadar SIEM rules

2.2.1 Log Activity

QRadar can monitor and display normalized data of events in real time to perform advanced searches. It can also investigate event data, search for events, monitor the log activity, and identify false positives.

2.2.2 Network Activity

The Network Activity feature provides help to investigate the communication between two hosts. If the content capture motion is enabled, information displays about how network traffic is communicated and what information was transferred. This feature provides information in real time and monitors the network using configurable time charts.

2.2.3 Assets

QRadar automatically creates asset profiles by using passive flow data and vulnerability data to discover network servers and hosts. These profiles, provide information about each known asset in your network, including the services that they are running. This feature is mainly used for rule and event correlation processes to mitigate the possibility of a false-positive.

2.2.4 Offenses

An *offense* is the product of the rules that are created to trigger an action where several conditions are met. Each rule can be configured to capture and respond to a specific event, sequence of events, flow sequence or offense. The offense is triggered after all the conditions created by the rule and the customer rule engine are met.

2.2.5 Reports

You can create custom reports or use default reports with templates provided by QRadar itself. You can customize and rebrand these presets to be distributed to all users within the console.

2.2.6 Data collection

QRadar accepts the information in various formats from a wide range of devices, including security events, network traffic, and scan results. All collected data is categorized in three sections:

- Event data collection
- Flow data collection
- Vulnerability assessment information

The event collection is generated from the log sources, such as firewalls, routers, servers, IDS, or IPS. The flow data collection provides information about the network traffic and can be sent to QRadar in the following formats:

- Flowlog files
- NetFlow
- J-Flow
- SFlow
- Packeteer

The vulnerability assessment information comes from different types of scanners.

2.2.7 QRadar SIEM rules

Rules are created to perform tests on events, flows, or offenses. If all conditions are met the rule will be triggered and generate a response or counter-action. These actions can contain a wide range of activities, including excessive firewall denies, multiple login failures, or potential botnet activity. You can use an anomaly detection rule to perform tests. You can then use the results of the saved flow information or event searches to detect unusual traffic patterns that might occur in a network and address possible threats before an attack or malicious process compromises the integrity of the technological infrastructure.

2.3 QRadar architecture

When you are planning to integrate or implement an IBM Security QRadar deployment on your network and security infrastructure, it's always good to have an awareness of the QRadar architecture to see how the different components of the system affect your network. Having those concepts clear can facilitate the planning process for you to be able to integrate the IBM Security QRadar system and take advantage of the benefits the product offer to your organization.

The IBM Security QRadar system collects, processes, aggregates, and stores network data in real time. It uses that data to contribute to your network security by providing real-time information and correlation; the system correlates all network security events and flows and generates alerts and offenses that can be analyzed by your network security team.

To have a good understanding of how QRadar process the data it receives from the network devices, it is good to segment the operation of IBM Security QRadar system into three layers:

- Data collection
- Data processing
- Data searches

This segmentation applies to any QRadar deployment structure, regardless of the size, complexity, number or log sources, or modules it has installed or attached to it.

Figure 2-1 shows the layers that make up the QRadar architecture.

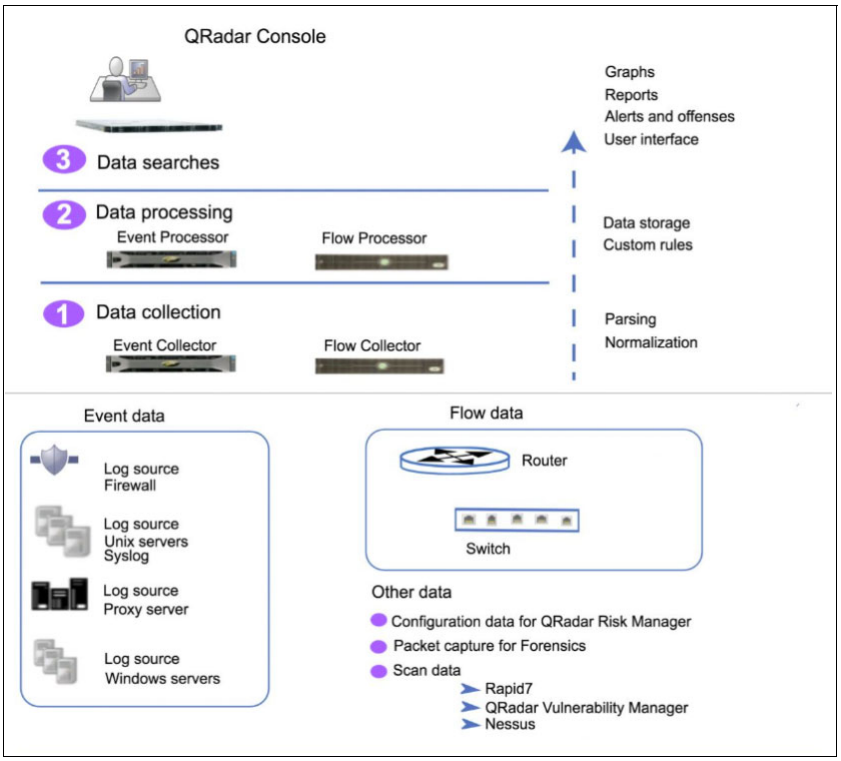


Figure 2-1 QRadar architecture

The layers represented in Figure 2-1 constitute the core functionality of any QRadar system. Understanding these layers can provider a clearer understanding of how each of them contribute to data processing.

2.3.1 Data collection

Data collection is the first layer of the architecture. This layer is where the QRadar system retrieves the data, such as events and flows that it receives from network devices.

You can use the QRadar All-In-One appliance to collect the data directly from the network, or the administrator can use collectors, such as QRadar Event Collectors or QRadar Flow Collectors, to collect event or flow data. The data is then processed (parsed and normalized) before it goes up to the processing layer.

Note: Event data represents events that occur at a point in time somewhere in the network such as user logins, VPN connections, firewall denies, proxy connections, and any other event that might be logged in the network devices.

Alternately, flow data is network activity information or session information between two hosts on a network that the IBM Security QRadar system translates into flow records. In other words, QRadar translates or normalizes raw data into IP addresses, ports, byte packet counts, and other information into flow records that effectively represent a session between two hosts.

In addition to collecting flow information with a QRadar Flow Collector, full packet capture is available with the QRadar Incident Forensics component.

2.3.2 Data processing

After data collection, the second layer of data processing is where QRadar system processes that data against the Custom Rule Engine (CRE) component. After having the CRE component processing the data, the system can generate offenses and alerts to then write or save the data into storage.

Events and flows can be processed by an All-In-One appliance without the need of having QRadar Event Processors or Flow Processors; however, if the processing capacity is exceeded, you might need to add Event Processors or Flow Processors to be able to handle the load. You might also need to deploy QRadar Data Nodes in case you need more storage capacity.

Other features, such as QRM, QVM, or QRadar Incident Forensics, allow processing of different type of data. You can find more information about these features in 4.3, “Features check” on page 80.

2.3.3 Data searches

In this layer, the data that was collected and processed by the system is stored, and it is available to be used on searches, reports, alerts, and offenses investigation. As the name implies, in an All-In-One system, all data is collected, processed, and stored on a single appliance.

In a distributed environment, the QRadar console does not perform event and flow collecting, processing, or storage. In this case, it is primarily used for the users to be able to run searches, reports, alerts, and investigation of offenses.

2.3.4 QRadar high availability

As with other information technology and security systems, it is important to make sure the systems are always available. In the case of a security system as important as the IBM Security QRadar system, it is always a good practice to include a high availability (HA) setup or solution to make sure the system is always available to reinforce the security on the network infrastructure.

Having a QRadar HA solution, the system can continue to collect, store, and process event and flow data even if there is a hardware or software failure.

To get the system working on a HA environment, QRadar connects a primary HA host with a secondary HA host and configure a virtual IP (VIP) to create an HA cluster.

Figure 2-2 shows a basic HA setup.

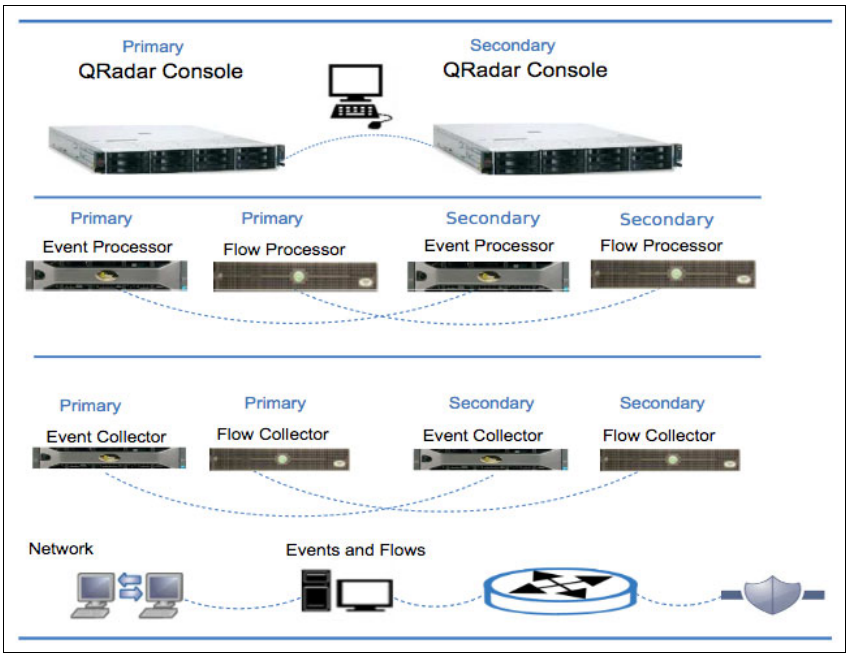


Figure 2-2 Basic HA setup

The concept around HA is similar to other HA deployments that can be found with other vendors. You install and configure a second appliance that takes over the role of primary in case a failure on the primary occurs. The secondary HA host maintains access to the same data as the primary host by using data synchronization or shared external storage. It also inherits the license from the primary HA host so that there is no need to purchase and apply a separate license for the secondary host.

Some of the failures that can potentially affect the operation of the primary systems are failures on a power supply, a network failure detected by the network connectivity tests, an operating system failure that delays or stops the heartbeat ping tests, a complete RAID failure, and a failure on the management interface. It might also be possible to trigger a manual failover for the secondary system to become the primary one.

Primary HA host

The primary HA host might be any device (console or managed host) on the deployment that need protection from data loss in the event of a failure (either hardware or software failure).

When an HA cluster is created, the IP address assigned to the primary system is automatically reassigned to a cluster virtual IP address. That being said, you must assign an unused IP address to the primary HA host when configuring the HA host.

Secondary HA host

The secondary HA host is the standby system for the primary HA host. If the primary HA system fails, the secondary system automatically detects this failure and takes ownership of all the responsibilities of the primary HA host.

Virtual IP address

When you create an HA cluster, the cluster virtual IP address takes the IP address of the primary HA host. To increase the HA system performance in large environments or deployments, it is strongly suggested to use 10 GB crossover cables between the primary

and secondary HA hosts. Using a 10 GB crossover interface reduces the time required for the systems to be synchronized and ensures optimal performance of the pair.

Specifically, in QRadar version 7.3.0, IBM introduces a technology that minimizes downtime during failover activities for Event Collectors. This is accomplished by the introduction of a technology called *Gluster File System*. The Gluster File System technology makes the synchronization time shorter for failovers between primary and secondary HA hosts, so it is a more efficient technology.

For more information about HA, refer to the *IBM Security QRadar SIEM High Availability* guide.

2.4 Components

Before starting, to go further on the different QRadar components that you find on a distributed environment, it is important to keep in mind that all appliances must be running the same software version for the system to operate correctly.

Figure 2-3 shows the devices that can be found on a distributed environment.

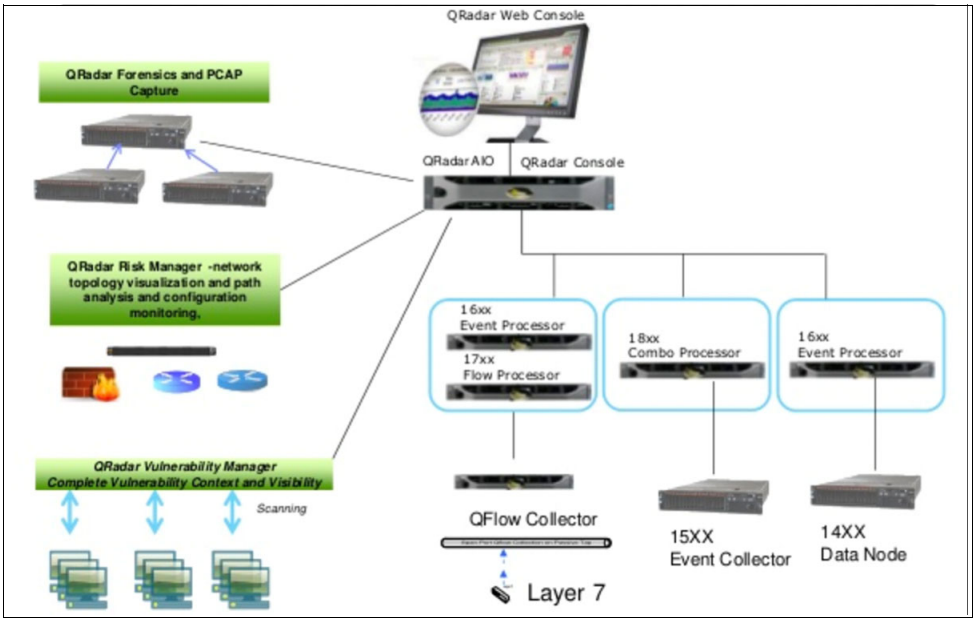


Figure 2-3 QRadar distributed environment

2.4.1 QRadar console

The QRadar console provides the user interface where the user can review reports, offenses, asset information, and administrative functions. It can also be used to configure the different system settings, create and configure rules for the system to be able to generate offenses, and create reports to meet the different requirements that your company might have.

2.4.2 QRadar event collector

The Event Collector system collects events from the different log sources that might be found on the network. It also normalizes that raw events it receives to a format that can be used by the IBM Security QRadar system to further process the data.

It bundles or coalesces identical events to conserve or save system usage. It also sends the data (raw and normalized) to the QRadar Event Processor for it to process the data further.

Note: The Event Collectors do not store the data locally; instead, they simply collect and parse events before they send those events to an Event Processor appliance for them to be stored there.

The Event Collector inherits the EPS license of the Event Processor it is connected to.

2.4.3 QRadar event processor

Events that are collected by one or more IBM Security QRadar event collector component, or directly received from log sources in the network, are processed by QRadar Event Processor using the Custom Rules Engine (CRE). If events are matched to the CRE custom rules that are predefined on the Console, the Event Processor executes the actions defined for the rule response configuration.

Data storage happens on each Event Processor or it can also be done by the QRadar Data Nodes (if deployed and configured).

The processing rate is determined by the EPS license. If the EPS rate defined on the license is exceeded, events are buffered and remain in the Event Collector source queues until the rate drops. If you continue to exceed the EPS license rate, and the queue is filled up, the IBM Security QRadar system drops events and issues a notification or warning to report this.

Note: When a QRadar Event Processor is added to an All-In-One system, the event processing function is moved from the All-In-One appliance to the new Event Processor that was added.

2.4.4 QRadar QFlow collector

The Flow collector collects flows by connecting to a SPAN port or a network TAP. It also supports the collection of external flow-based data sources such as Cisco NetFlow or Juniper J-Flow.

The QRadar QFlow Collectors are not designed to be full packet capture systems. If it is required to have a full packet capture system, you might want to consider the QRadar Incident Forensics option.

2.4.5 QRadar Flow Processor

The Flow Processor processes flows from one or more QFlow Collector systems. It can also collect external flows such as NetFlow, J-Flow, and sFlow directly from the network devices.

Note: When a Flow Processor is added to an All-In-One appliance, the processing of flows is moved from the All-In-One device to the Flow Processor.

2.4.6 QRadar Data Node

Data Nodes are primarily used for storage purposes; they add storage and process capacity on demand as required. Data nodes will help to increase the search speed in the deployment by providing more hardware resources to run queries on.

2.4.7 QRadar events and flows

The main difference between event and flow data is that the event occurs at a specific time and it is logged at that time. Alternatively, a flow is a record of network communications that can last for seconds, minutes, hours, or days, depending on the activity within the session or communication. For example, when you do a web request, the web client might download multiple files such as images, text, and video, and it can last for 5 to 10 seconds. Another example can be when a user watches a movie or video. In this case, the network session might lasts up to a few hours. Thus, a *flow* is a record of network activity between two hosts.

Events

The IBM Security QRadar accepts logs or events from the different log sources found on the network. A log source is a data source such as a firewall or an IPS device.

The system accepts logs by using several protocols such as Syslog and SNMP. It can also get the logs by establishing outbound connections to get events through protocols such as SCP, SFTP, JDBC, and Checkpoint OPSEC.

As mentioned earlier, before you can view and use event data on the QRadar Console, events are collected from log sources and then processed by the Event Processor system. Remember than in the case of an All-In-One Appliance, the system works as an Event Collector, Event Processor, and Console at the same time.

Event pipeline

Figure 2-4 shows the layers of the event pipeline.

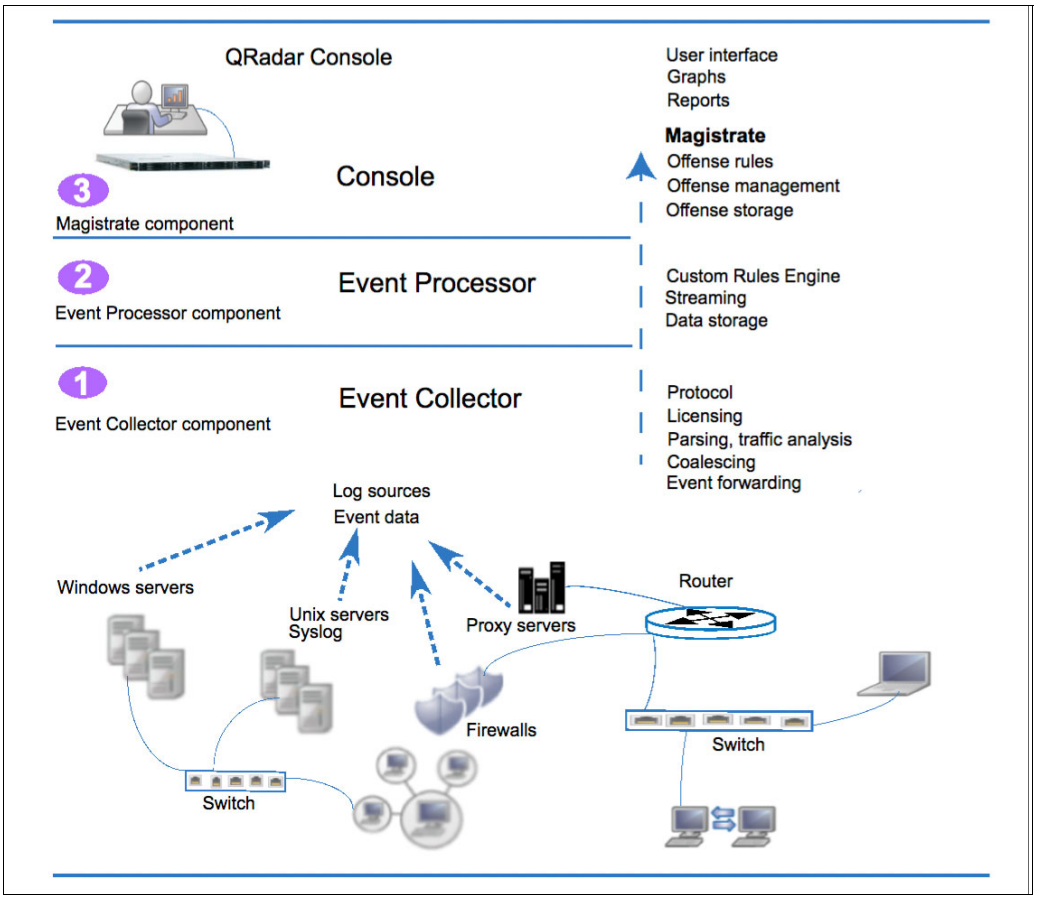


Figure 2-4 Layers of the event pipeline

Event collection

The IBM Security QRadar Event Collector collects data from log sources using the different protocols it supports. It is also in charge of monitoring the number of incoming events to manage input queues and EPS licensing, which is handled by the license throttling process. It takes the raw events received from the log sources and parses the fields into a QRadar usable format.

The IBM Security QRadar Event Collector is also in charge of log source traffic analysis and auto discover processes; it processes the parsed and normalized event data against all DSMs that support automatic discovery.

Events are parsed and then coalesced or bundled based on common attributes across events, this is done by the coalescing process.

The Event Collector is finally in charge of event forwarding. It Applies routing rules for the system to forward data to offsite targets, external syslog servers and other SIEMs (if configured to do so).

When the Event Collector receives the events from the different log sources, the events are transferred into input queues for further processing to be done. The queue size changes based on the protocol or method in use and from these queues, the events are parsed and

normalized. The normalization process is basically the transformation of the raw data into a format that has fields such as IP addresses that QRadar can use.

The IBM Security QRadar system recognizes known log sources by the source IP address or host name that is contained on the header. This is known as the log source identifier.

QRadar process (parses and coalesces) events from the log sources into records. Events from new or unknown data sources that were not detected or automatically configured in the past are passed to the traffic analysis engine or auto detection engine.

Note: When new log sources are discovered, the QRadar Console receives a configuration request message for it to add the new log source. If auto detection is disabled, or you exceeded your log source licensed limit, the new log sources are not added.

Event processing

The Event Processor component is responsible for processing events that are received by QRadar and comparing them against defined rules through the use of the Custom Rule Engine (CRE); keeping track of systems involved in incidents over time, generating notifications to users.

When events match a rule, a notification is sent from the Event Processor to the Magistrate component on the QRadar Console indicating that a specific event triggered or hit a rule. The Magistrate component is in charge of creating and managing offenses. When rules are triggered, responses or actions such as notifications, new syslog events, SNMP traps, email message and offenses are generated.

The IBM Security QRadar Event Processor also sends real-time event data to the QRadar Console when a user is viewing events from the Log Activity tab with Real time (streaming). Streamed events are not provided from the database.

The Event Collector sends normalized event data to the Event Processor where the events are processed by Custom Rules Engine (CRE). If events are matched to the CRE custom rules that are predefined on the QRadar Console, the Event Processor executes the action that is defined for the rule response.

Magistrate component

The Magistrate component is in charge of monitoring and acting on offenses; it generates actions such as sending email notifications, creating offenses, or any action specified on the rule the event matched. It is also in charge of updating active offenses, changing statuses of offenses and providing user access to offense information from the offenses tab.

Finally, it writes offense data to a Postgres database where they are stored.

The Magistrate Processing Core (MPC) is also in charge of correlating offenses with event notifications from multiple Event Processor components. Keep in mind that you will only find the magistrate component on a QRadar Console.

Flows

QRadar flows represent network activity by normalizing IP addresses, ports, byte and packet counts, and other data, into flow records, which effectively are records of network sessions between two hosts. The component in QRadar that collects and creates flow information is known as *QFlow*.

A flow starts when the Flow Collector detects the first packet that has a unique source IP address, destination IP address, source port, destination port, and other specific protocol options. Each new packet is evaluated here. Counts of bytes and packets are added to the statistical counters in the flow record. At the end of an interval, a status record of the flow is sent to a Flow Processor and statistical counters for the flow are reset.

A flow is finished when there is no activity for the flow within the configured time.

QFlow can process flows from internal or external sources. External sources are flow sources such as NetFlow, sFlow, and JFlow. They can be sent to a dedicated Flow Collector or to a Flow Processor such as the QRadar Flow Processor 1705 appliance.

External sources do not require as much CPU processing because every packet is not processed to build flows. In this configuration, you might have a dedicated Flow Collector and a Flow Processor that both receive and create flow data. In smaller environments with less than 50 Mbps, an All-in-One appliance might handle all the data processing.

The Flow Collector can also collect internal flows by using or connecting to a SPAN port, or a network TAP. Figure 2-5 shows the options for collecting flows in a network.

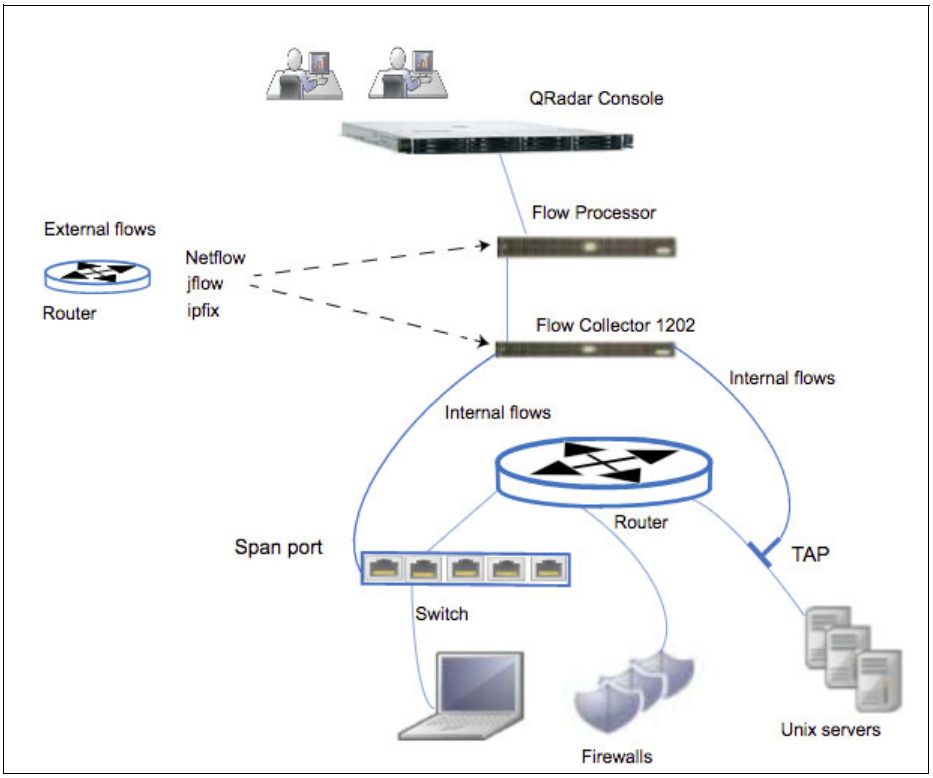


Figure 2-5 Flows collection

Flow pipeline

The *Flow Collector* generates flow data from raw packets that are collected from monitor ports such as SPANs, TAPs and monitor sessions, or from external flow sources such as NetFlow, sFlow, and JFlow. This data is transformed or packaged into a QRadar flow format and transferred down the pipeline for processing.

The *Flow Processor* is in charge of the flow de-duplication process, which removes duplicate flows when multiple Flow Collectors provide data to Flow Processors appliances. It is also combines two sides of each flow when data is provided asymmetrically. This process is done

so that the system can be capable of recognizing flows from each side and then combine them into one record. It monitors the number of incoming flows to the system to manage input queues and licensing. Finally, it applies routing rules for the system, such as sending flow data to offsite targets, external Syslog systems, JSON systems, and other SIEMs.

The flow data is processed through the Custom Rules Engine (CRE), and it is correlated and analyzed against the rules that are configured on the system so that an offense can be generated based on this correlation and processing. As mentioned before offenses can be viewed on the Offenses tab.

2.4.8 Modules and others

IBM QRadar can integrate with separate appliances, as described in the sections that following, that can perform specific actions to enhance capabilities for these appliances.

QRadar Risk Manager

IBM Security QRadar Risk Manager (QRM) is sold separately and is an appliance installed for monitoring device configurations, simulate changes to your network environment and it is also capable of prioritizing risks and vulnerabilities in the network. QRM uses data that is collected by QRadar from any network device, it can be configuration data, vulnerability feeds or third-party security sources. Data sources allows QRM to identify security, policy and compliance risks in the network and estimate the probability of a risk exploitation. When QRM discovers any risk, it will display offenses on the Offenses tab of the QRadar console. This data is then analyzed and reported as any other data that QRadar processes.

With QRM you establish a risk tolerance for the company network by managing and monitoring all the risk data flowing through the network. It can also be used to query all network connections, compare device configurations, filter the network topology and simulate the possible effects of updating device configurations.

QRM allows you to define a set of policies or questions about the network and monitor this policies for any change. One easy example is, if you want to deny traffic from any unencrypted protocol in your DMZ coming from the Internet, you can define a policy monitor rule or question to detect all traffic using these unencrypted protocols. This returns a list of all connections using this unencrypted protocol from the Internet to your DMZ, ultimately allowing you to establish which of them represent a security risks based on your criteria. After a QRM appliance is installed into the system, it can be accessed using the Risk tab on the IBM Security QRadar Console.

QRM enhances the IBM Security QRadar system by providing the QRadar administrator with tools to accomplish these tasks:

- Centralize risk management.
- Use a topology to view your network.
- Configure and monitor network devices.
- View connections between network devices.
- Search firewall rules.
- View existing rules and the event count for triggered rules.
- Search for devices and paths for your network devices.
- Monitor and audit your network to ensure compliance.
- Define, schedule, and run exploit simulations on your network.
- Search for vulnerabilities.

All these tasks allow to have a centralized risk management and compliance, for increased intelligence information, which ultimately provides visibility and efficiency that you cannot achieve by using manual processes or with other product technologies.

QRadar Vulnerability Manager

IBM Security QRadar Vulnerability Manager (QVM) is a network scanning platform that detects vulnerabilities within the applications, systems and devices on the network.

QRM uses security intelligence to help you manage and prioritize the network vulnerabilities.

Real time visibility of the vulnerabilities that are detected by the built-in QRadar Vulnerability scanner and other third-party scanners (Third-party scanners are integrated with QRadar and include IBM BigFix®, IBM Guardium®, IBM AppScan®, Nessus, nCircle, and Rapid 7) can be achieved.

You can use QVM to accomplish the following tasks:

- Continuously monitor vulnerabilities.
- Improve resource configuration.
- Identify software patches.
- Prioritize security gaps by correlating vulnerability data with network flows, log data, firewall, and intrusion prevention system (IPS) data.
- Schedule scans to run at times convenient for your network assets.
- Specify the assets that you want to exclude from scans, either globally or for each scan.
- Configure authenticated patch scans for Linux, UNIX, or Windows operating systems.
- Configure different scanning protocols or specify the port ranges that you want to scan.

In QVM, vulnerability scanning is controlled by creating scan profiles that specify the assets that are required to be scanned and the scan schedule. A vulnerability processor is also automatically deployed on the QRadar console when a license for QVM is purchased; the processor contains a QVM scanning component.

QVM checks for multiple types of vulnerabilities in the network, these vulnerabilities are categorized into the following broad categories:

- Risky default settings: By leaving some default settings in place, you can make your network vulnerable to attacks.
- Software Features: Some software settings for systems or applications are designed to improve usability but these settings can introduce risk to the network.
- Misconfiguration: Identify misconfiguration in default settings.
- Vendor flaws: This is a broad category that includes events such as buffer overflows, string format issues, and cross-site scripting.

QVM uses a combination of active checks that involves sending packets and remote probes, and passive correlation checks. The QVM database covers around 70,000 network, operating system, and application layer vulnerabilities. You can search the complete scanning library from the research window on the Vulnerabilities tab.

QRadar Vulnerability Manager tests

The following examples are some of the categories that QRadar Vulnerability Manager tests:

- Router checks
- Firewall checks
- Database checks
- Web server checks
- Web application server checks
- Common web scripts checks

- Custom web application checks
- DNS server checks
- Mail server checks
- Application server checks
- Wireless access point checks
- Common service checks
- Obsolete software and systems

QRadar network traffic capture

IBM Security QRadar Packet Capture (PCAP) is a network traffic capture and search application, PCAP appliance has only one capture port (DNA0) and you can install either a 10G or 1G SFP transceiver. With this appliance you can capture network packets at rates up to 10 Gbps from a live network interface and write them to files without packet loss. You can also this appliance to search captured network traffic by time and packet envelope data. With the right appliance resources and well-made searches, you can make searches and record data simultaneously without any data loss.

PCAP appliances that have 10G transceiver support clusters, allowing them to expand the overall data storage and computational ability and better performance than a single stand-alone server. QRadar PCAP appliances that have 1G transceiver do not support clusters. Some features included in PCAP appliance are:

- *Standard PCAP file format*, which is used to store network traffic and which integrates with existing third-party analysis tools
- *High performance packet-to-disk recording*, which captures network packets from a live network
- *Multi-core support*, which is designed for multi-core architectures
- Direct-IO disk space, which uses direct IO access to disks to obtain maximum disk write throughput
- *Real time indexing*, which can produce an index automatically during packet capture

Capture files are saved in the standard PCAP format with time stamps in microsecond solution, these are stored in sequential order based on the file size, and stores in directories, once this directory is full the capture files are overwritten, based on preconfigured recording parameters.

For packet capture appliances, the speed of capturing network traffic depends on whether you have data nodes attached to the master node:

- For packet capture appliances that don't have data nodes attached, the maximum capture speed is up to 7 Gbps.
- For packet capture appliances that have data nodes attached to the master node, the capture speed increases up to 10 Gbps.

The QRadar Incident Forensics module

The IBM Security QRadar Incident Forensics module (QIF) makes the detection of emerging threats, the determination of the root cause and prevention recurrences possible. By using this feature, security analysts can focus on the investigations of the source that initiated the threat, how they did it and what was compromised through the threat. You can retrace the step by step actions of cyber criminals and reconstruct the raw network data related to a security incident.

QRadar Incident Forensics module can be used in specific scenarios in the different types of investigations, such as network security, insider analysis, fraud, abuse and evidence gathering.

You can search to look for any contextual element or identifier that you know about the attacker or incident. If you use the keyword in the search, suspicious content is returned. Some of the suspicious content might be relevant to the investigation. QRadar Incident Forensics allows to use data pivoting which is achieved by making the content that is returned by a search result appear as a hotlink, this hotlink can be used to investigate this object quickly.

Use Digital Impression to look through the data and to map the relationship between entities, such as IP addresses, names, and MAC addresses based on frequency. One or more results can be selected to view the frequency and direction of the relationship. Use Surveyor to see a timeline of activities so that you can retrace an attack. Surveyor reconstructs the session and sorts the documents in time order. Use content filtering to look at a subset of content categories, such as WebMail, Pornography, to help you remove the noise or irrelevant when you search.

Network security investigations

QRadar Incident Forensics can be used to detect and investigate malicious activities that target critical assets. The built-in forensics tools are there to help to remediate a network security breach and prevent it from happening again. Use QIF investigative tools to help you find out how the event occurred, minimize its impact, and do everything you can to prevent another breach.

QRadar Incident Forensics can be used on the following scenarios:

- Identify the source of an attack: In this scenario, an organization is alerted to a suspected breach. It seeks to find the initial point of an attack to isolate the source. The organization must quarantine the compromised system.
- Compromised systems: Here, an organization is alerted that one or more of their systems was compromised by an advanced cyber-attack technique.
- Data leaked to unauthorized entities: The organization is alerted that sensitive data was leaked to unauthorized entities within the organization or to external parties.
- Insider analysis investigations: Use QIF to detect collusion, sabotage, and misuse of access. Identify the perpetrator, identify collaborators, identify compromised systems, and document data losses.
- Misuse of access: The organization is alerted that one or more of their employees are misusing credentials or are used as a proxy to access sensitive systems and data for unauthorized activities.
- Collusion: Here the organization is alerted that one or more stakeholders are colluding among themselves or with external parties to engage in activities that are detrimental to the organization.
- Sabotage: An organization is alerted that one or more stakeholders are attempting to disrupt operations. The stakeholder might be being used as a proxy.
- Fraud and abuse investigations: Use QIF to locate unauthorized transactions, unsanctioned allocation of resources, protocol deviations, and evading legal controls.
- Unauthorized transactions: An organization is alerted that unauthorized transactions.
- Unsanctioned allocation of resources: The organization suspects unsanctioned allocation of resources, which is leading to a negative financial impact on business operations.

- Protocol deviations and evading legal controls: An organization is alerted that business, IT protocols, and legal controls were circumvented, which can result in a negative financial impact.
- Evidence collection investigations: Use QIF to assess the risk of vulnerabilities in the organization, quantify the confidence in identifying threats or perpetrators, and refine security practices.
- Confidence in identifying threats: The organization is alerted about a certain threat, exploit, or vulnerability. To justify remediation efforts that might otherwise preempt normal business operations, they want to quantify a confidence interval for any associated risk.
- Refining security practices: The detection of new and risky behaviors motivates an organization to assess whether existing security practices are sufficient. In this scenario, an organization seeks to qualify the effectiveness of its security rules for the risks that it faces.
- Risk assessments: A security bulletin that outlines certain vulnerabilities, exploits, or malicious behavior prompts an organization to do a risk assessment. The risk assessment determines whether the organization is susceptible or is already compromised.

Ariel Query Language

The Ariel Query Language (AQL) is a structured query language that can be used to communicate with the Ariel database. Use AQL to manage event and flow data from the Ariel database.

Use the following AQL built-in functions to do calculations on data in the Ariel database.

- Basic functions
  - `STR`: Converts any parameter to a string.
  - `STRLEN`: Returns the length of this string.
  - `SUBSTRING`: Copies a range of characters into a new string.
  - `CONCAT`: Concatenates all passed strings into one string.
  - `PARSEDATETIME`: Returns the current time, which is expressed as milliseconds since the time 00:00:00 Coordinated Universal Time (UTC) on 01 January 1970.
  - `DATEFORMAT`: Formats a time, which is expressed as milliseconds since the time 00:00:00 Coordinated Universal Time (UTC) on 01 January 1970 to a user-readable form.
  - `NOW`: Returns the current time that is expressed as milliseconds since the time 00:00:00 Coordinated Universal Time (UTC) on 01 January 1970.
  - `UTF8`: Returns the UTF8 string of a byte array.
- Aggregate functions
  - `GROUP BY`: Creates an aggregate on one or more columns.
  - `COUNT`: Returns the count of the rows.
  - `UNIQUECOUNT`: Returns the unique count of the value taken together.
  - `FIRST`: Returns the first entry of the rows taken together.
  - `SUM`: Returns the sum of the rows taken together.
  - `AVG`: Returns the average value of the rows taken together.
  - `MIN`: Returns the minimum value of the rows taken together.
  - `MAX`: Returns the maximum value of the rows taken together.
  - `HAVING`: Allows operators on the result of a grouped by column.

- External functions
  - `HostName`: Looks up a log source ID or a flow source ID.
  - `AssetHostname`: Looks up a host name of an asset at a point in time.
  - `AssetProperty`: Looks up a property for an asset at the current time.
  - `AssetUser`: Looks up a user for an asset at a point in time.
  - `MatchesAsset Search`: If the asset is contained in the results of the asset saved search it returns true.
  - `ReferenceMap`: Looks up the value for a key in a reference map.
  - `ReferenceTable`: Looks up the value for a column key in a table that is identified by a table key in a specific reference table collection.
  - `Reference MapSet Contains`: If a value is contained in, a key in a specific reference map of set it returns true identifies a reference set that.
  - `ReferenceSet Contains`: If a value is contained in a specific reference set, it returns true.
  - `CategoryName`: Looks up the name of a category by its ID.
  - `LogSource Group Name`: Looks up the name of a log source group by its log source ID.
  - `QidDescription`: Looks up the description of a QID by its QID.
  - `QidName`: Looks up the name of a QID by its QID.
  - `Application Name`: Returns the name of a flow application.
  - `LogSource Name`: Looks up the name of a log source by its log source ID.
  - `LogSource Type Name`: Looks up the name of a log source type by its log source ID.
  - `UTF-8`: Returns the UTF-8string.
  - `StrLen`: Returns the length of this string.
  - `Str`: Converts parameter to string.
  - `SubString`: Copies a range of characters into a new string.
  - `Concat`: Concatenates all passed strings into one string.
  - `ParseDate time`: Returns the current time, which is expressed as milliseconds since the time 00:00:00 Coordinated Universal Time (UTC) on 01 January 2014.
  - `Now`: Returns the current time, which is expressed as milliseconds since the time 00:00:00 Coordinated Universal Time (UTC) on 01 January 2014.
  - `ProtocolName`: Returns the name of a protocol, which is based on a protocol ID number.
  - `InOffense`: If an event or flow belongs to the specified offense, it returns true.
  - `InCIDR`: If the IP/column, specified is contained in, or equal to, the specified IP/CIDR, it returns true.
  - `NetworkName`: Looks up the network name from the network hierarchy for the Host that is passed in.
  - `RuleName`: Returns one or more rule names that are based on the rule ID or IDs that are passed in.
  - `Long`: Parses a string that represents a number into a Long (integer) data type.
  - `Double`: Parses a string that represents a number into a Double (integer) data type.

- Logical and comparative operators

  Use logical operators in AQL statements to determine any equality or difference between values. By using logical operators in the WHERE clause of an AQL statement, the results returned are restricted or filtered to those that match the conditions in the WHERE clause.

  You can use the following logical and comparative operators in AQL statements:

=	Compares two values, and returns true if they are equal.
!=	Compares two values, and returns true if they are *not* equal.
(and)	Use parenthesis to nest components of a WHERE or HAVING clause to create complex Boolean expressions.
< and <=	Compares two values, and returns true if the left value is less than (<) or less than or equal to (<=) the right value.
> and >=	Compares two values and returns true if the left value is greater than (>) or greater than or equal to (>=) the right value.
*	Multiplies two values and returns the result.
/	Divides two values and returns the result.
+	Adds two values and returns the result.
–	Subtracts one value from another and returns the result.
^	Takes a value, raises it to the specified power, and returns the result.
%	Takes the modulo of a value, and returns the result.
AND	Takes the left side of a statement and the right side of a statement, and returns true if *both* are true.
OR	Takes the left side of a statement and the right side of a statement, and returns true if *either* is true.
NOT	Takes in a statement and returns true if the statement evaluates to false.
IS NULL	Takes in a value and returns true if the value is null.
NOT NULL	Takes in a value and returns true if the value is not null.
BETWEEN (X,Y)	Takes in a left side and two values (X,Y), and returns true if the left side is between the two values.
LIMIT	Limits the number of results to the provided number.
ORDER BY (ASC,DESC)	Orders the result set by the provided columns.
COLLATE	Parameter to order by that allows a BCP47 language tag to collate.
INTO	Creates a named cursor that contains results that can be queried at a different time.
START	Passes a time interval to start selecting data from in the format yyyy-MM-dd HH:mm.
STOP	Passes a time interval to stop selecting data from in the format yyyy-MM-dd HH:mm.
LAST	Passes a time interval to select data from. Valid intervals are MINUTES, HOURS, and DAYS.
LIKE	Matches if the string passed, is LIKE the passed value. % is a wildcard.

ILIKE	Matches if the string passed, is LIKE the passed value in a case-insensitive manner. % is a wildcard.
MATCHES	Matches if the string matches the provided regular expression.
IMATCHES	Matches if the string matches the provided regular expression in a case-insensitive manner.
TEXT SEARCH	Searches the Lucene full text index for the passed value. TEXT SEARCH is valid only with AND operators and cannot be used with OR with other tests. Attempts to do so results in a syntax error.

- SELECT statement

  Use the SELECT statement to retrieve specific data from the events or flows table in the Ariel database. A SELECT operation is called a *query*.

  – Syntax:

  ```
  SELECT selectList FROM joinClauses
  ```

  – Usage:

  A SELECT statement can include one or more fields from the flow or event tables. Use an asterisk (*) to denote all columns. All field names are case-sensitive. SELECT and FROM statements are not case-sensitive.

- WHERE clause

  Restrict your AQL queries by using WHERE clauses. The WHERE clause describes the filter criteria to apply to the query and filters the resulting view to accept only those events or flows that meet the specified condition.

  – Syntax:

  ```
  WHERE searchCondition
  ```

  A searchCondition is a combination of logical and comparison operators that together make a test. Only those input rows that pass the test are included in the result.

- GROUP BY clause

  Use the GROUP BY clause to aggregate your data. To provide meaningful results of the aggregation, usually, data aggregation is combined with arithmetic functions on remaining columns.

  – Syntax:

  ```
  GROUP BY groupClause
  ```

  You can use aggregate functions in AQL queries to summarize information from multiple rows. The following aggregate functions are supported:

  - GROUP BY: Creates an aggregate on one or more columns.
  - COUNT: Returns the count of the rows in the aggregate.
  - UNIQUECOUNT: Returns the unique count of the value in the aggregate.
  - FIRST: Returns the first entry of the rows in the aggregate.
  - SUM: When used with numeric data, returns the sum of the values. When used with categorical data, it returns the union of the categorical values.
  - AVG: Returns the average value of the rows in the aggregate.
  - MIN(arg): Returns the lowest value of the rows in the aggregate.
  - MAX(arg): Returns the highest value of the rows in the aggregate.
  - HAVING: Allows operators on the result of a grouped by column.

- `ORDER BY` clause

  Use the `ORDER BY` clause to sort the resulting view that is based on expression results. The order is sorted by ascending or descending sequence.

  - Syntax:

    ```
    ORDER BY orderClause
    ```

    Only one field can be used in the `ORDER BY` clause. You can switch sorting between ascending or descending by appending the `ASC` or `DESC` keyword to the order by clause.

- `LIKE` clause

  Use the `LIKE` clause to search partial string matches in the Ariel database.

  - Syntax:

    ```
    ORDER BY orderClause
    ```

  You can search fields by using the `LIKE` clause.

- `COUNT` function

  The `COUNT` function returns the number of rows that satisfy the `WHERE` clause of a `SELECT` statement.

  If the `SELECT` statement does not have a `WHERE` clause, the `COUNT` function returns the total number of rows in the table.

  - Syntax:

    ```
    COUNT
    ```

For more information about AQL, check the IBM official documentation.

2.5 Preferred practices

As part of any holistic process in the management of the monitoring tools, it is important to have in mind a set of preferred practices and recommendations to follow to take full advantage of QRadar. This section provides guides on some of the known preferred practices.

2.5.1 Regulations and compliance

Although QRadar or SIEM technologies are generally tools that can improve the early detection of security threats, you can also use these tools to help technical and non-technical staff to obtain data that is needed to comply with various regulations or laws or basically any internal improvement process driven by a known framework or methodology. You can then determine that an implementation of QRadar can support the organization to achieve the following types of objectives (among others):

- Internal control (business policies and procedures)
- Compliance with regulations or regulators
- Maintain or obtain process certifications
- Retention of logs and events (according to legal or internal stipulations)
- Monitoring and control of security incidents
- Early detection of critical events associated with commitment indicators (IoCs)

QRadar is not a technology that is designed to focus solely on compliance, but you can take advantage of its features to correlate data, centralize asset information, standardize logs, and validate detailed information about specific events of critical assets.

Many regulations, both in specialized sectors whose compliance is mandatory (SOX and HIPPA among others), and control frameworks (COBIT, ITIL, and PCI-DSS) are implemented by companies that require the delivery, monitoring, and control of massive amounts of information. These regulations must be added to the fact that the current operating environments of most medium and large enterprises use significant amounts of devices, whether critical or not, which must be controlled by security, IT, and internal control departments.

Under these criteria, the following types of regulatory frameworks are typically necessary:

- Internal control frameworks (internal regulations)

  It is normal for companies to require management frameworks or governance or to simply not want to “reinvent the wheel” so that they can dedicate themselves to implementing improvement processes for the strategic planning, operation, and control of their information assets. For this, there are many frameworks, certifications, preferred practices, or processes that can allow organizations to work in a more efficient, orderly, and in most cases more secure.

  To achieve the correct implementation of these programs, a vast majority of companies create internal control departments, audit departments or use external consultants, which in most cases are not subject to technology departments and therefore do not have direct access to the information they require to demonstrate the correct implementation (or not) of the roadmap of these best practices.

  Therefore, it is normal that reports, evidence of events, lists or simply visibility of technology assets are required that the guidelines stipulated by these control bodies are being complied with. QRadar can support this management since it’s an information centralization platform, but before looking at the details of how QRadar can help us, we could list some control frameworks that, even though they are not specific to SIEM technologies, having QRadar would greatly facilitate obtaining evidence to guarantee their correct implementation:

  - Implementation of preferred practices internally:
    - ISO 2700x (requires the aggregation of event data from multiple systems and the security management for sensitive assets within an organization)
    - The ITIL (QRadar can be used on almost all the 5 parts of the service life cycle, especially on the service operations and continual improvement)
    - COBIT (QRadar will have a great impact on the Monitor and Evaluation stages of COBIT 4.1 and 5)
    - NIST norms (for companies without any regulatory obligation and with the necessity of new standards and guidelines for their technological infrastructure)
    - IT Balanced Scorecards (In most of the cases you need numbers to deliver part of the scorecards in your organization, specially things related to active monitoring, security incidents, metrics about detected threats and attacks, obviously QRadar can give that kind of information)
  - Internal audits
  - External audits
  - Departments of information technology
  - Department of risk management
- External control frameworks (External regulations)

  However, we mentioned the possible frameworks of governance and control that a company can use to improve its operational or monitoring processes, which QRadar can use to obtain information in a more efficient and simple way. Don’t forget that many

organizations are regulated by government bodies or international legislations, which need to ensure that technological environments comply with guidelines of certain laws.

In some scenarios, using a SIEM platform is mandatory, specially in industries where certain regulations require delivery of reports and information for external or internal audits. Qradar can be used to deliver information, such as the number of user login failures or the records of data backups. In addition, personable identifiable information (PII) file transfers can be generated with accuracy and timely using QRadar with the following frameworks:

- ISOs
- SOX
- HIPPA
- NIST
- PCI-DSS
- FISMA
- PII Regulations
- NERC

QRadar, as state-of-the-art correlation and early warning technology, can help you address the challenges of handling and controlling events, devices, and security threats, and complying with both control domains mentioned previously. You can then define several stages where QRadar can support this work.

2.5.2 QRadar features for regulations purposes

You can use QRadar with its factory characteristics to be able to carry out processes of searching, monitoring and obtaining information. This section describes QRadar features that you can use immediately without configuration.

Asset Management

The Asset Management module allows you to complete the following tasks:

- List assets within our network (almost as a Configuration Management Database - CMDB or Asset Management Database), as shown in Figure 2-6.

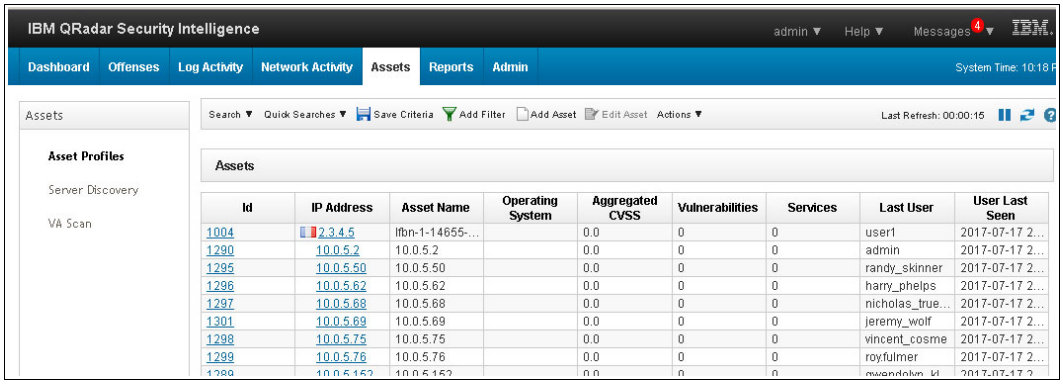
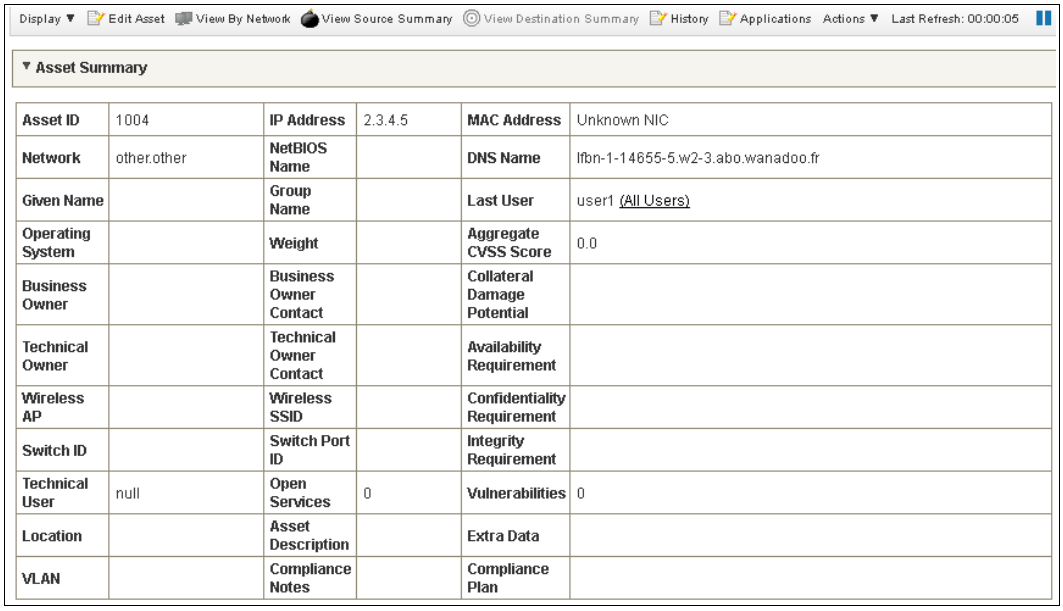


Figure 2-6 QRadar Assets tab

- Assign levels of criticality and other characteristics of high value to perform searches that require to deliver data according to the regulation that we are attending, as shown in Figure 2-7.



Asset ID	1004	**IP Address**	2.3.4.5	**MAC Address**	Unknown NIC
Network	other.other	**NetBIOS Name**		**DNS Name**	lfbn-1-14655-5.w2-3.abo.wanadoo.fr
Given Name		**Group Name**		**Last User**	user1 (All Users)
Operating System		**Weight**		**Aggregate CVSS Score**	0.0
Business Owner		**Business Owner Contact**		**Collateral Damage Potential**	
Technical Owner		**Technical Owner Contact**		**Availability Requirement**	
Wireless AP		**Wireless SSID**		**Confidentiality Requirement**	
Switch ID		**Switch Port ID**		**Integrity Requirement**	
Technical User	null	**Open Services**	0	**Vulnerabilities**	0
Location		**Asset Description**		**Extra Data**	
VLAN		**Compliance Notes**		**Compliance Plan**	

Figure 2-7 Assets summary

- Perform dynamic searches based on some predefined criteria of several that can provide data required by various regulations, as shown in Figure 2-8.

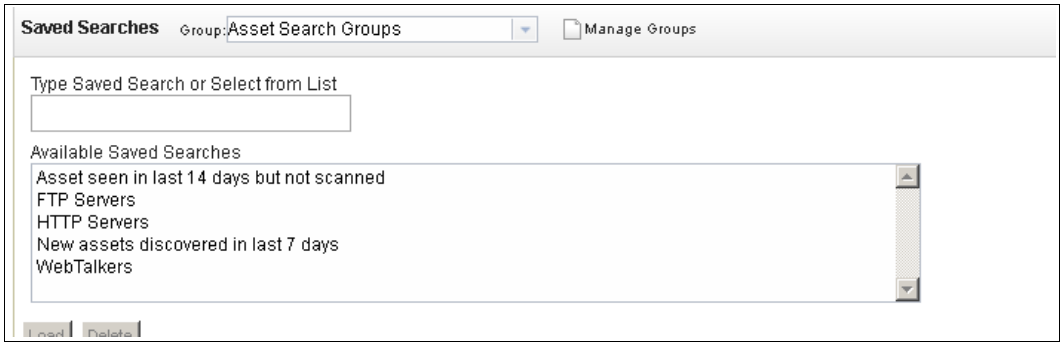


Figure 2-8 Assets Saved Searches

- Conduct searches with the criteria that we want to define, in addition to using fields already defined in QRadar to associate the asset with a compliance rule, as shown in Figure 2-9.

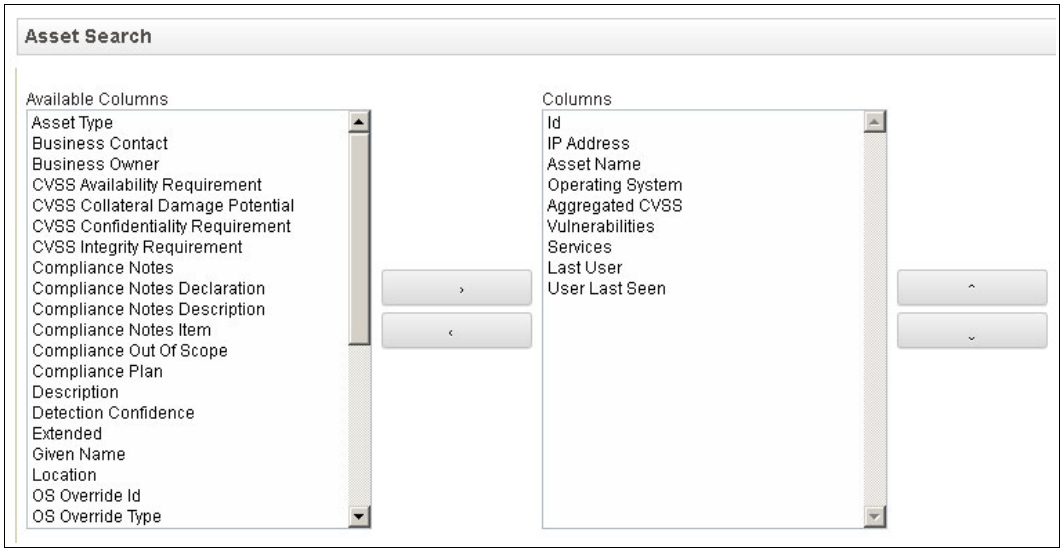


Figure 2-9 Asset Search, column definition

Centralization of events (Log Activity)

This feature is one of the most used modules of QRadar. You can use this feature for the following searches:

- Initially you can find the preloaded searches in QRadar in **Activity** → **Search** → **New Search log**. In the Log Activity tab, under “Saved Searches” the name of the group (Compliance) displays, as shown in Figure 2-10.

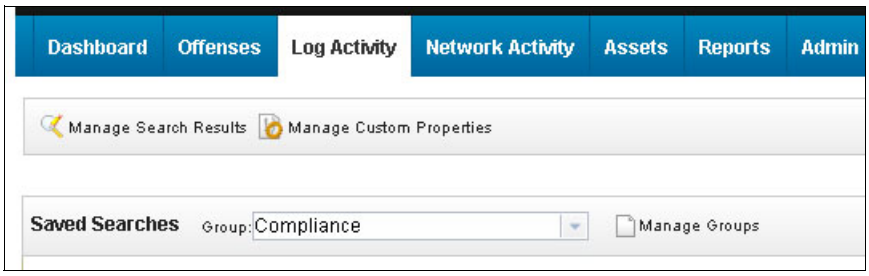


Figure 2-10 QRadar Log Activity tab

- If you select **Compliance** in the Log Activity tab, you can search within several pre-defined searches, from which you can retrieve the following information:
  - *Admin Login Failure by User*: Use these search filters to first verify that all events are properly parsed in QRadar, and then list all the events whose category is Admin Login Failure. See Figure 2-11.

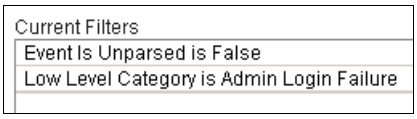


Figure 2-11 Admin Login Failure by User

– *Username Involved in Compliance Rules*: Use these search filters to verify whether there is an event that matches the logic of any of those rules.
– *Daily policy violation activity*: Use these filters to initially verify that the events are parsed. Then the filter shows everything that is within the category of the policy, such as Windows GPOs. See Figure 2-12.

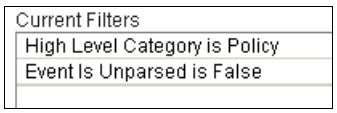


Figure 2-12 Daily policy violation activity

– *PCI 10.6 SIEM Audit Overview*: Use this filter (Figure 2-13) to list all audit events that pertain to SIEM.

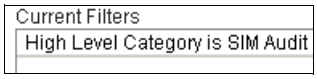


Figure 2-13 SIEM Audit Overview

– *System, Registry, application or other messages of interest*: This search filter shows initially only those events that come from the System category. See Figure 2-14.

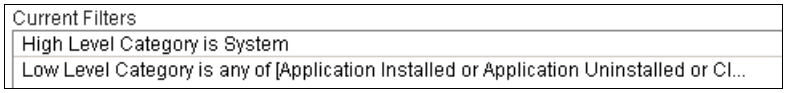


Figure 2-14 System category events

It then lists events that also coincide with one of the low-level categories, as shown in Figure 2-15.

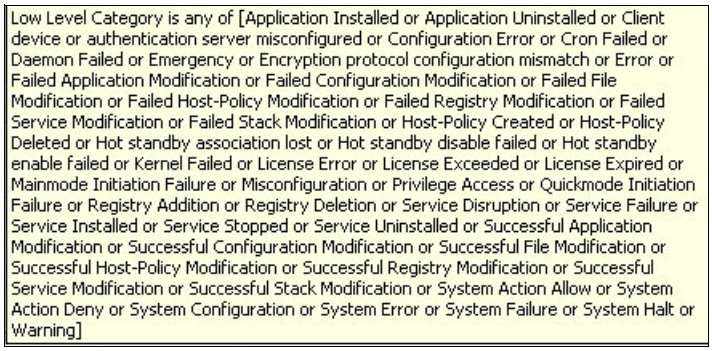


Figure 2-15 Other messages of interest

Rules and Alerts (Offenses)

The rules in QRadar are responsible for generating the logic of offenses or security alerts. In turn, they oversee correlating the data of different types of events. QRadar has several predefined rules regarding compliance issues, within which we can list the predefined rules shown in Figure 2-16 on page 30.

Rule Name ▲	Group
Compliance: Auditing Services Changed on Compliance Host	Compliance
Compliance: Compliance Events Become Offenses	Compliance
Compliance: Configuration Change Made to Device in Compliance network	Compliance
Compliance: Excessive Failed Logins to Compliance IS	Compliance
Compliance: Multiple Failed Logins to a Compliance Asset	Compliance
Compliance: Traffic from DMZ to Internal Network	Compliance
Compliance: Traffic from Untrusted Network to Trusted Network	Compliance
Vulnerabilities: Vulnerability Reported by Scanner	Compliance

Figure 2-16 QRadar predefined rules

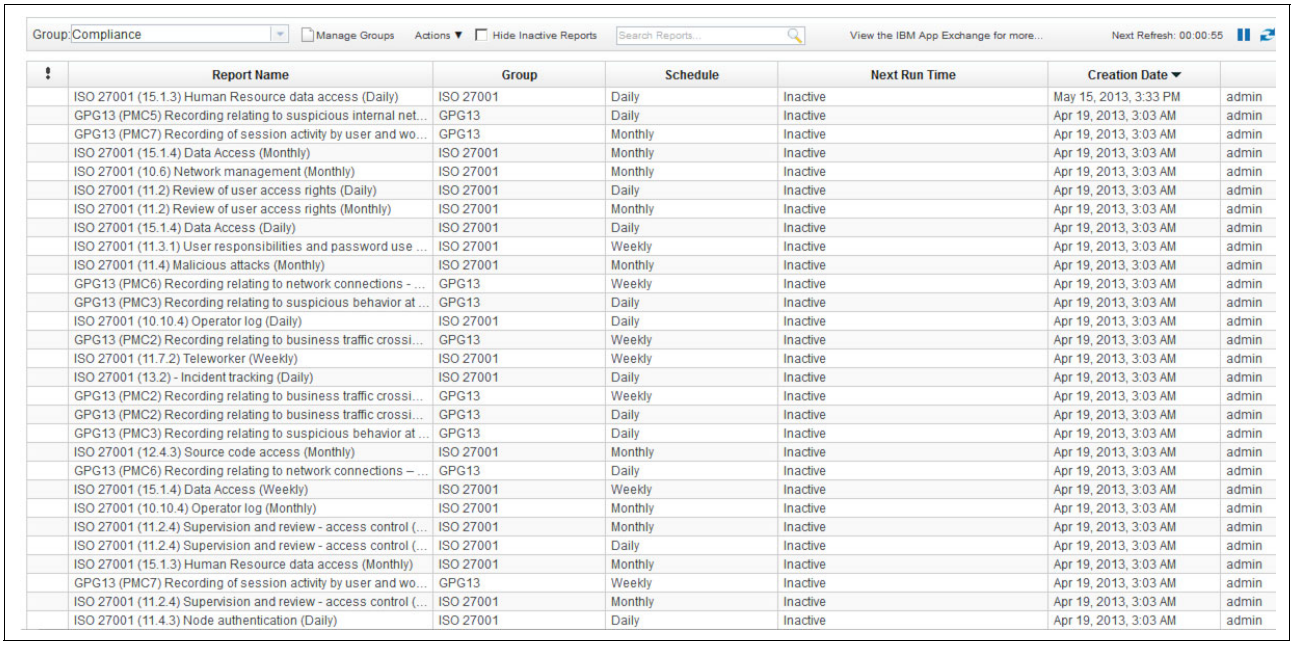
The logic behind these rules is diverse. For example, the *Compliance Rule: Excessive Failed Logins to Compliance IS* rule consists of the parameters shown in Figure 2-17.

Figure 2-17 Compliance rule

Validation parameters that the rule generates security alerts only when one of the hosts or servers associated with the activity is in the GLBA building blocks HIPAA or SOX Compliance host. It validates that the event is categorized within the category of Authentication Failures and that it comes from the same destination IP in an average of 10 minutes in duration.

Scheduled reports

You can also use reporting schemes. In fact, it is the most common method to use in matters related to compliance. Several predefined reports are available, such as those shown in Figure 2-18.



!	Report Name	Group	Schedule	Next Run Time	Creation Date ▼	
	ISO 27001 (15.1.3) Human Resource data access (Daily)	ISO 27001	Daily	Inactive	May 15, 2013, 3:33 PM	admin
	GPG13 (PMC5) Recording relating to suspicious internal net...	GPG13	Daily	Inactive	Apr 19, 2013, 3:03 AM	admin
	GPG13 (PMC7) Recording of session activity by user and wo...	GPG13	Monthly	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (15.1.4) Data Access (Monthly)	ISO 27001	Monthly	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (10.6) Network management (Monthly)	ISO 27001	Monthly	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (11.2) Review of user access rights (Daily)	ISO 27001	Daily	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (11.2) Review of user access rights (Monthly)	ISO 27001	Monthly	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (15.1.4) Data Access (Daily)	ISO 27001	Daily	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (11.3.1) User responsibilities and password use ...	ISO 27001	Weekly	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (11.4) Malicious attacks (Monthly)	ISO 27001	Monthly	Inactive	Apr 19, 2013, 3:03 AM	admin
	GPG13 (PMC6) Recording relating to network connections - ...	GPG13	Weekly	Inactive	Apr 19, 2013, 3:03 AM	admin
	GPG13 (PMC3) Recording relating to suspicious behavior at ...	GPG13	Daily	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (10.10.4) Operator log (Daily)	ISO 27001	Daily	Inactive	Apr 19, 2013, 3:03 AM	admin
	GPG13 (PMC2) Recording relating to business traffic crossi...	GPG13	Weekly	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (11.7.2) Teleworker (Weekly)	ISO 27001	Weekly	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (13.2) - Incident tracking (Daily)	ISO 27001	Daily	Inactive	Apr 19, 2013, 3:03 AM	admin
	GPG13 (PMC2) Recording relating to business traffic crossi...	GPG13	Weekly	Inactive	Apr 19, 2013, 3:03 AM	admin
	GPG13 (PMC2) Recording relating to business traffic crossi...	GPG13	Daily	Inactive	Apr 19, 2013, 3:03 AM	admin
	GPG13 (PMC3) Recording relating to suspicious behavior at ...	GPG13	Daily	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (12.4.3) Source code access (Monthly)	ISO 27001	Monthly	Inactive	Apr 19, 2013, 3:03 AM	admin
	GPG13 (PMC6) Recording relating to network connections – ...	GPG13	Daily	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (15.1.4) Data Access (Weekly)	ISO 27001	Weekly	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (10.10.4) Operator log (Monthly)	ISO 27001	Monthly	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (11.2.4) Supervision and review - access control (...	ISO 27001	Monthly	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (11.2.4) Supervision and review - access control (...	ISO 27001	Daily	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (15.1.3) Human Resource data access (Monthly)	ISO 27001	Monthly	Inactive	Apr 19, 2013, 3:03 AM	admin
	GPG13 (PMC7) Recording of session activity by user and wo...	GPG13	Weekly	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (11.2.4) Supervision and review - access control (...	ISO 27001	Monthly	Inactive	Apr 19, 2013, 3:03 AM	admin
	ISO 27001 (11.4.3) Node authentication (Daily)	ISO 27001	Daily	Inactive	Apr 19, 2013, 3:03 AM	admin

Figure 2-18 Predefined reports

Most of these reports are disabled because not all organizations require these, but at any time they can be activated. In addition, it is advisable to validate that they have the necessary log sources and specific events before activating the desired reports.

QRadar Vulnerability Management and Control

QRadar Vulnerability Manager (QVM), proactively senses and discovers network device and application security vulnerabilities, adds context and supports the prioritization of remediation and mitigation activities. Uses advanced analytics to enrich the results of both scheduled and dynamic vulnerability scans with network asset information, security configurations, flow data, logs and threat intelligence to manage vulnerabilities and achieve compliance.

This feature can help you with the development of an optimized plan for addressing security exposures. Unlike stand-alone tools, the solution integrates vulnerability information to help security teams gain the visibility they need to work more efficiently and reduce costs.

QRadar Vulnerability Manager correlates vulnerability data with network topology and connection data to prioritize application vulnerabilities and intelligently manage and reduce risk. A policy engine automates compliance checks, enabling risk dashboards, and historical compliance reports.

Forensic operations (QFM)

QRadar Incident Forensics allows you to retrace the step-by-step actions of a potential attacker, and quickly and easily conduct an in-depth forensics investigation of suspected malicious network security incidents. It reduces the time it takes security teams to investigate QRadar offense records, in many cases from days to hours—or even minutes. It can also help you remediate a network security breach and prevent it from happening again.

IBM QRadar Incident Forensics offers an optional IBM QRadar Packet Capture appliance to store and manage data used by IBM QRadar Incident Forensics if no other network packet capture (PCAP) device is deployed. Any number of these appliances can be installed as a tap on a network or sub-network to collect the raw packet data.

IBM QRadar Incident Forensics:

- Retraces the step-by-step actions of cyber criminals to provide deep insights into the impact of intrusions and help prevent their reoccurrence.
- Reconstructs raw network data related to a security incident back into its original form for a greater understanding of the event.

Event-related QRadar Risk Management

You can use QRadar Risk Manager (QRM) to identify security, policy, and compliance risks in your network and calculate the probability of risk exploitation. QRadar Vulnerability Manager and QRadar Risk Manager are combined into one offering and both are enabled through a single base license. Add a QRadar Risk Manager 700 appliance to get the following capabilities:

- Compliance assessment
- Risk policies that are based on vulnerability data and risk scores that help you quickly identify high-risk vulnerabilities
- Visibility into potential exploit paths from potential threats and untrusted networks through the network topology view
- Risk policy-based filtering
- Topology visualization

- False positives reduction in vulnerability assessments
- Visibility into what vulnerabilities are blocked by firewalls and Intrusion Prevention Systems (IPS)

Use of plug-ins to improve searches and results

Not only you can use the default mechanisms that come in QRadar to facilitate compliance with regulations and control frameworks, but you can use plug-ins or apps that are installed through the XForce App Exchange. One of them is the Compliance App.

The Compliance theme adds the following compliance to new installations of QRadar 7.2.6:

- 4 custom event properties that look for variations in Account Name payloads.
- 42 event searches related to monitoring compliance.
- 7 flow searches related to monitoring compliance.
- 153 reports related to monitoring compliance.
- 140 rules and building blocks related to monitoring compliance.
- 10 reference data sets related to monitoring server types for compliance purposes.

Figure 2-19 shows an example of the rules available after you install the App Extension.

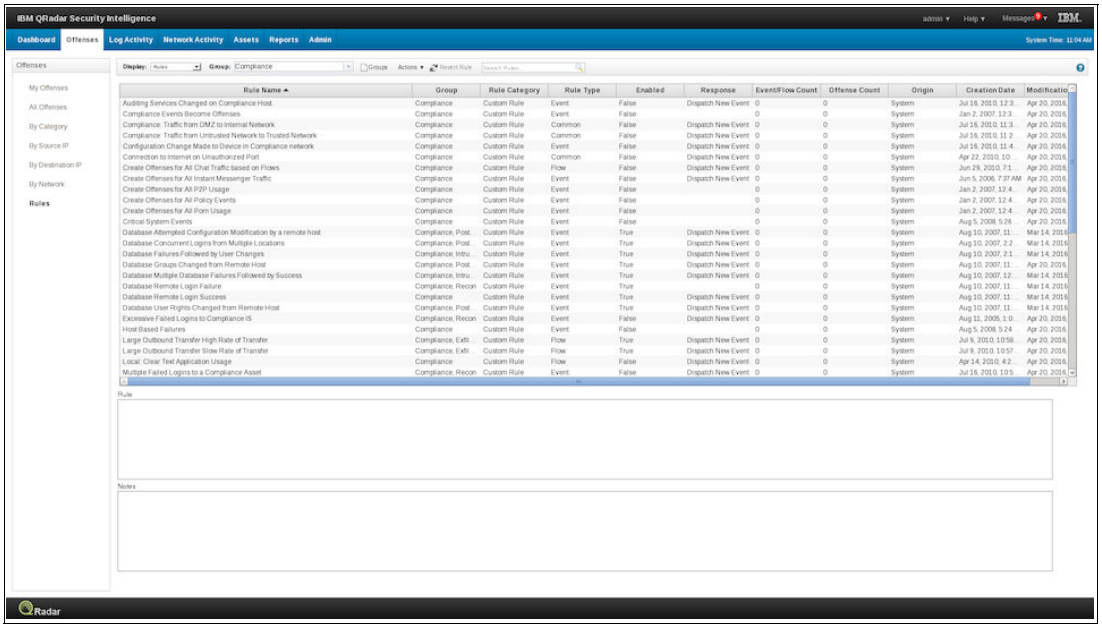


Figure 2-19 Offenses rules

To install the app:

1. First, download the app from:

   `https://exchange.xforce.ibmcloud.com/hub/extension/IBMQRadar:IBMContentPackageInternalCompliance`

2. Then, go to the Admin tab, and go to the Extension Manager.
3. Click **Add** and then select the file that you downloaded previously.
4. Click **Install**. A preview of the application content displays.

2.5.3 EPS calculation

EPS is a known term used across multiple IT Systems, that is mainly used as a metric for how many events or processes are logged within any given time on an appliance. Techopedia mentions that with the EPS Calculation you could "…review and evaluate the usability statistics of a hardware device, software application, network medium or hardware, Internet application, and/or a security device/appliance." (Techopedia INC., 2017).

Most of the SIEM Tools and offering in the market count with this metric to determine the size of the solution, amount of log sources, policies and scalability. With this metric, you can make budget decisions on how many appliances will be added into the solution and which IBM solution will be best for the customer's needs. This will also impact the service level and licensing provided to the customer to add more devices and optimize the solution which in this case, will be IBM QRadar. EPS calculation is crucial also for storage management of the events logged, this is due to the number of events that will be logged and stored for analysis. The metric will calculate the daily storage and compression ratio for optimal used space.

IBM uses a licensed formula to determine several aspects to calculate the EPS for each solution. It involves an inventory of the appliances, Devices Support Modules and the actual size of the solution. This will provide the guidelines and the scope on how many devices and how much throughput could generate. An important disclaimer to take into consideration is that this metric will only provide and approximate ideal number that is used as reference for service level, entitlement and licensing for the solution.

Calculation

The best way to deal with spikes of data is to ensure you have enough Events Per Second and Flows Per Minute (FPM). The main purpose is to allocate an efficient amount of resources so that the host has enough capacity to process a possible spike, and at the same time to avoid a large number of idle devices not processing EPS or FPM.

When the EPS that is allocated from the license pool is very to the average of the EPS Calculation metric, the system is likely to accumulate data in a temporary queue to be processed later. The more data is accumulated in the temporary queue, the longer it takes QRadar to process the backlog. The offenses will not be generated until the data is processed by the appliance, that is why it is important to minimize how frequently QRadar adds data to the temporary queue, known as the Burst Handling Queue. By ensuring that each managed host has enough capacity to process shot burst of data, you are minimizing the time QRadar process the information and ensuring offenses are created at the same time an event occurs.

A common mistake would be increasing the queue size when the system continuously exceeds the allocated processing capacity. The excess data is added to the end of the burst handling queue where it waits to be processed. The larger the queue, the longer it takes to processed by the appliance.

Deployment

The Event Collector gathers events from local and remote log sources and normalizes the raw information. The Event Collector is assigned to an EPS license that matches the Event Processor that it is connected to.

On the other hand, the Event Processor gathers all the data collected by the Event Collector and processes it by correlating the information from QRadar products and distributes the information to the appropriate area, depending on the type of the event. If the event rate exceeds the average EPS metric, you must add another event processor or recalculate the solution.

2.5.4 Optimization

Although QRadar provides default configurations that are ready to be used immediately and that take advantage of security alerts based on the internal behavior of the network and connected devices, you can optimize the process and your management practices to take full advantage of several QRadar features.

Monitoring and configuring

Although there are many manual processes that you can complete to optimize the use of QRadar from an administration and configuration perspective, the following apps are also available to facilitate implementation processes:

- QRadar Deployment Intelligence (Early Access at this time), which requires QRadar V7.2.8+ to be installed

  This monitoring tool allows the admin of the platform to get a basic and easy overview of the of the health of their QRadar system. The app uses historical data, such as status, up-time, notifications, event and flow rates, system performance metrics, QRadar specific metrics and more, to deliver statistics, dashboards, and other useful information. See Figure 2-20.

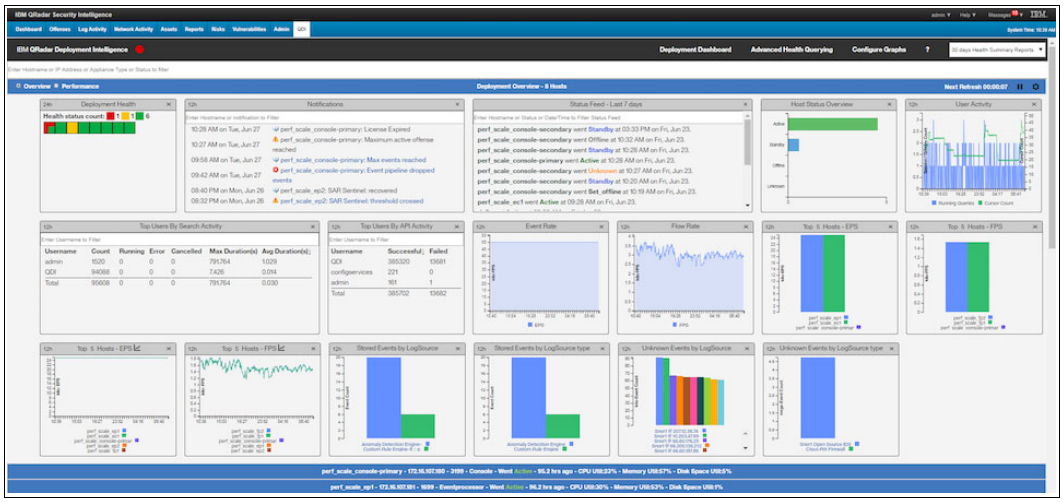


Figure 2-20 QRadar Deployment Intelligence Dashboard

- QRadar Master Console

  The QRadar Master Console, shown in Figure 2-21 on page 35, allows the admin to get a graphical representation, referred to as a *deployment card*, of the health and operational data for each IBM Security QRadar deployment that is connected and controlled to Master Console.

  The dashboard on the app can shows the following information, which is useful for any administrator who wants to understand the status of the platforms:

  – The number of managed hosts in the deployment
  – The status of the deployment
  – The number of critical, warning, and informational system notifications within the last 15 minutes
  – The event and flow rates, which are measured as an average over the last 15 minutes

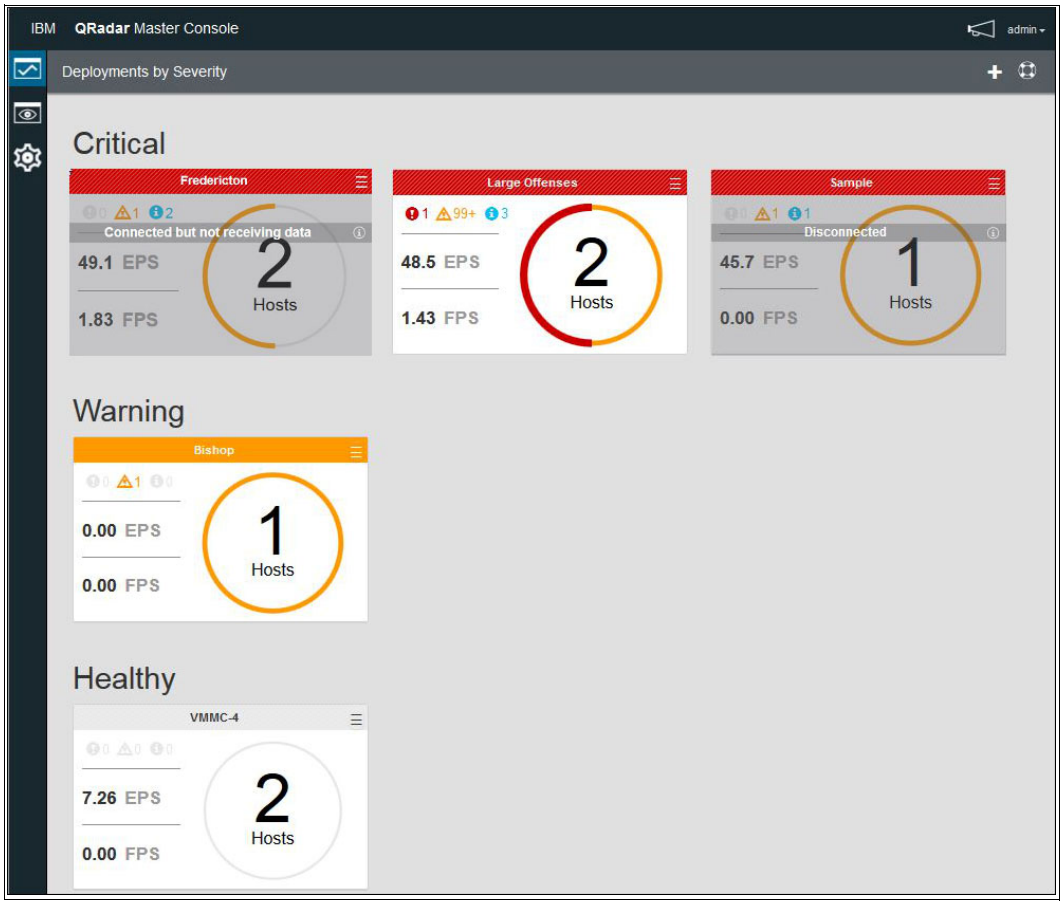


Figure 2-21 Deployments by Severity

- Health checks

  They are scripts, apps, and other useful frameworks that you can use to create health checks for the QRadar console. Some of these tools are developed by third-party companies (IBM Partners in most of the cases).

  The example included here is a health check app that is developed by ScienceSoft, called *Health Check Framework for IBM QRadar SIEM* (Figure 2-22 on page 36). You can more information about the ScienceSoft health check app online.

  > "Because QRadar's health and performance depend heavily on how properly the system is fine-tuned, Health Check Framework (HCF) provides a clear vision of QRadar health for timely detection of abnormalities. With automated QRadar health assessment based on performance and behavioral metrics and health markers, the tool allows to continuously sustain the platform's operability. HCF ensures a comprehensive 360-degree view of your system by letting detect operational deviations along with data losses, and helping to troubleshoot them promptly. HCF Manager, installed as a QRadar tab, is a user-side tool for HCF administrating, which provides HCF updating, report execution and scheduling, mailing list management, and reports download"[1]

[1] Taken from https://www.scnsoft.com/services/security/siem/qlean

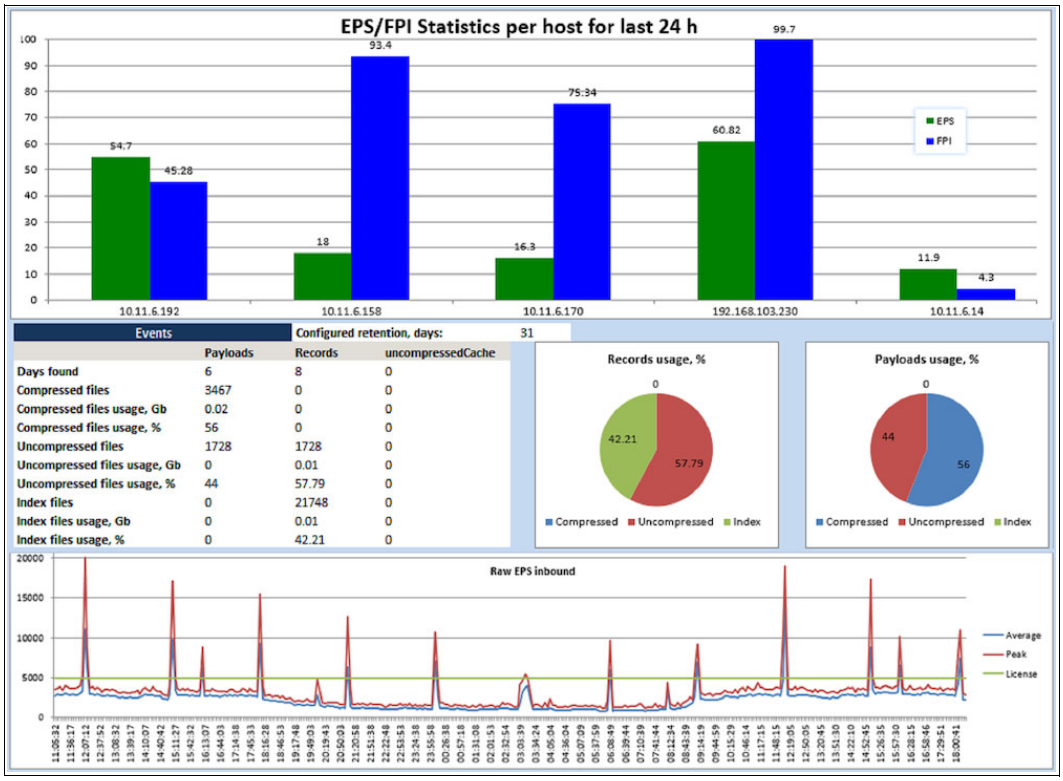


Figure 2-22 EPS/FPI Statistics per host

Usage

As part of an optimization process in the use of the QRadar platform, consider that you can use one of the following apps, which were created to improve the performance and information that can be obtained directly from the platform:

- QRadar Advisor with IBM Watson®

  This app has the cognitive capabilities of IBM Watson to the IBM QRadar platform to discover new threats and security alerts and to correlate external data from Internet sources. See Figure 2-23 on page 37. To install this app requires the following components:

  - IBM QRadar version 7.2.8 or higher
  - Local and Remote security monitoring
  - QRadar Console Internet access

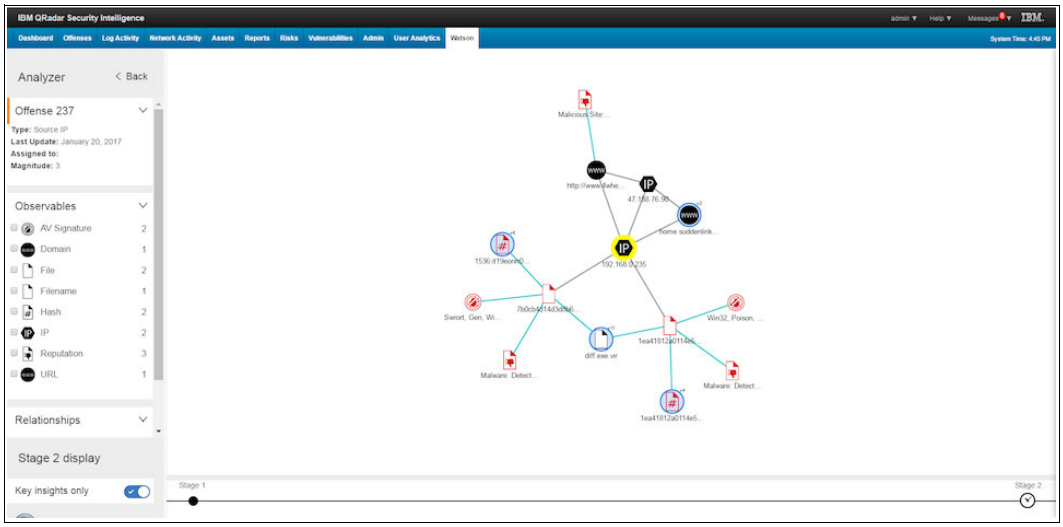


Figure 2-23 QRadar Watson integration

- IBM QRadar Operations

Use the QRadar Operations app to quickly view user activities and assess their impact on the overall system (Figure 2-24). The Operations app collects information from all relevant sources within the system and provides a single view of user configuration changes to help administrators easily troubleshoot and investigate the cause of certain behaviors in the system. The user interface is fully interactive. Throughout the app, you can click multiple data points to view the changes that users make on the system or click any of the graphs to view the data that exists during a specific time frame.

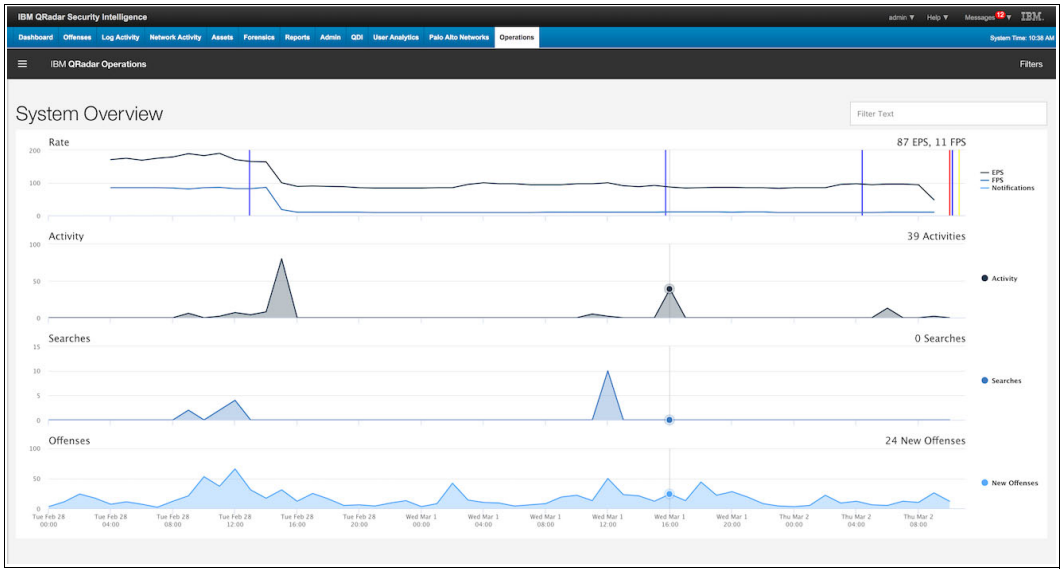


Figure 2-24 QRadar Operations

Rules, reports, and log activity

QRadar uses a set of tools to create alerts and to report and validate useful information. This section explores the following tools that you can use to create security alerts, to create automated reports of data, and to search for particular events, flows and information collected on QRadar:

- Elimination of false positives

  As part of QRadar's optimization efforts, it is extremely important to be aware that at times, the offenses generated by the platform are false positives. Thus, although the tool reports a security alert, this alert is not correct or does not represent critical information for the organization.

  Under these criteria, you can enhance the following processes:

  – Perform a process to improve the offense or rule (manual process)

    For this we would have to analyze the events that are associated in the offense and validate why those captured events generated such a security alert. For example: we could validate 100 deny firewall events, which alert a possible DoS, but we could see that these events are first of all denies, in addition to being correct denies, in other words they are expected. If this case applies, the DoS rule should have an exclusion on the hosts or IPs on which many Firewall denies exist.

  – Perform a more automated process (more risk in this process)

    Although this process is simpler it is a bit riskier because the false positive makes a pseudo automatic exclusion of the event in terms of alerts and offenses.

    Figure 2-25 shows the options for false positive tuning.

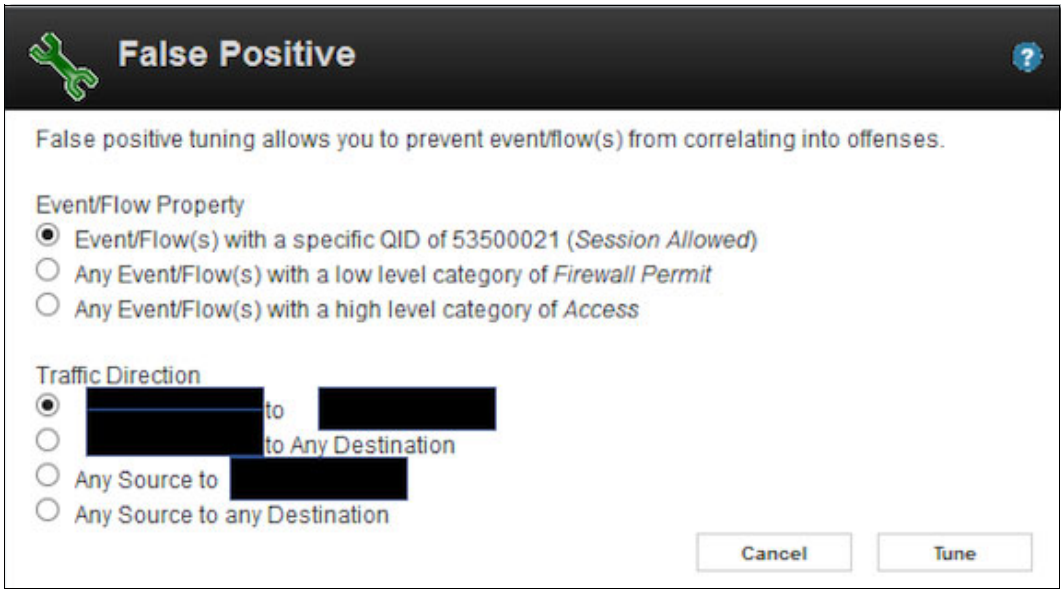


Figure 2-25 False positive tuning

– Updating of severity of events and offenses

It is also valid to review the severity of the events created in a personalized way, in addition to the data of severity, credibility, relevance. See Figure 2-26.

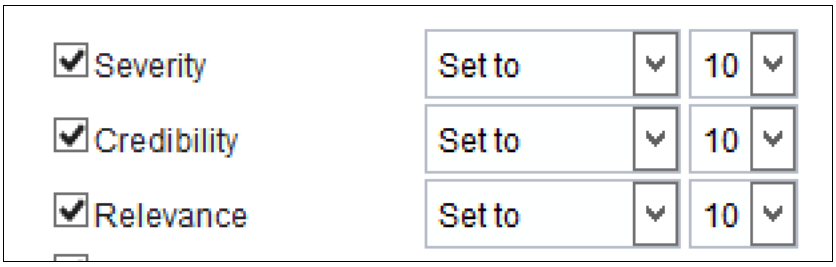


Figure 2-26 Events severity, credibility, and relevance

– Generation of custom properties

At times the DSM or, in other words, the module in charge of translating the information of the events in the fields that can be seen in QRadar, does not translate or places all the information that are really required to be able to make searches or rules more personalized and granular, in this case we must enhance what is known as creation of custom properties, for that we must also know how to work with regular expressions. See Figure 2-27.

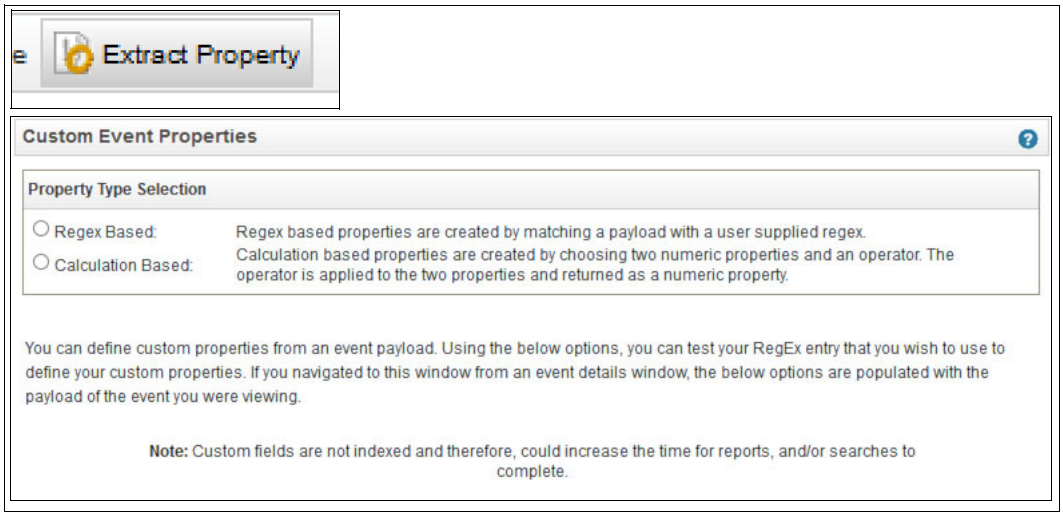


Figure 2-27 Custom Events Properties

Other admin tasks

You can also perform additional administrative tasks, which are not related to creating security alerts or getting information to address a potential attack investigation. The following admin tasks are important to the health and successful functioning of the QRadar console:

- Backups (Figure 2-28 on page 40)

  One of the most important tasks to perform after a QRadar installation is the configuration of a backup. For this you must have several things in mind:

  – Storage capacity of external backup media
  – Internal data management and data retention policies
  – Number of events and flows that QRadar is receiving and that will be supported

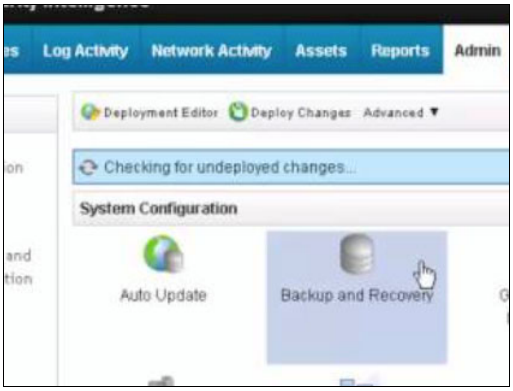


Figure 2-28 Backup and Recovery

Figure 2-29 shows the advanced settings for Backup and Recovery.

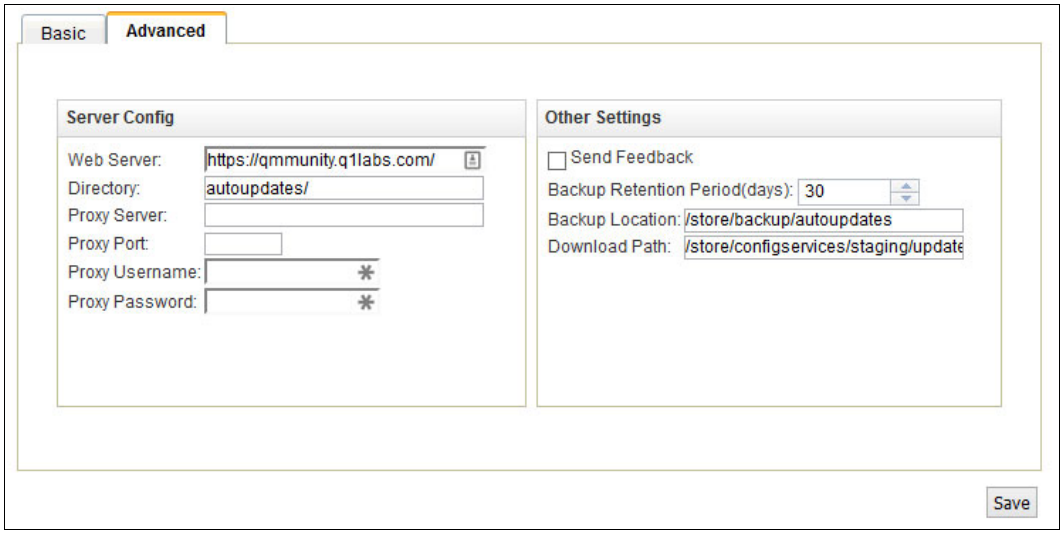


Figure 2-29 Backup and Recovery, advanced settings

- Network Hierarchy

  An important part of the structure of QRadar is the *Network Hierarchy* (Figure 2-30 on page 41), which must be kept orderly, updated, and consistent throughout the entire lifecycle of the platform so that the quests, logic of the offenses and alerts, and other components of the platform work correctly.

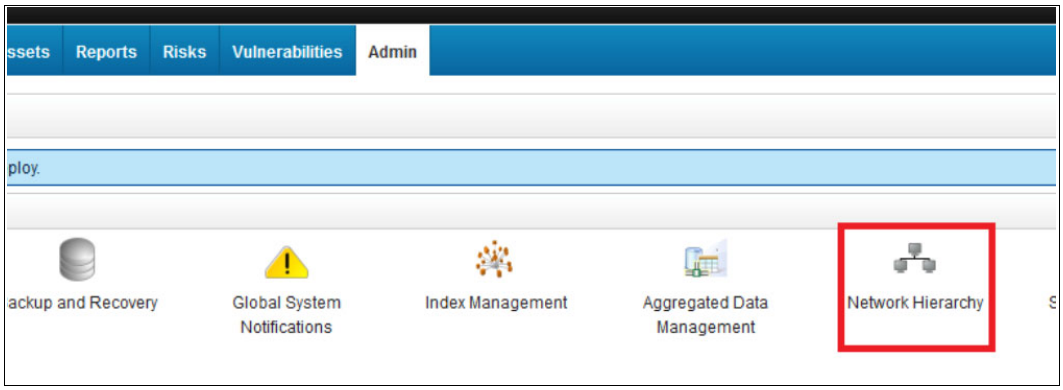


Figure 2-30 Network Hierarchy

To define your network IP parameters for the Network Hierarchy, edit each of the network names to assign the correct IP addressing scheme to match the real network design, as shown in Figure 2-31.

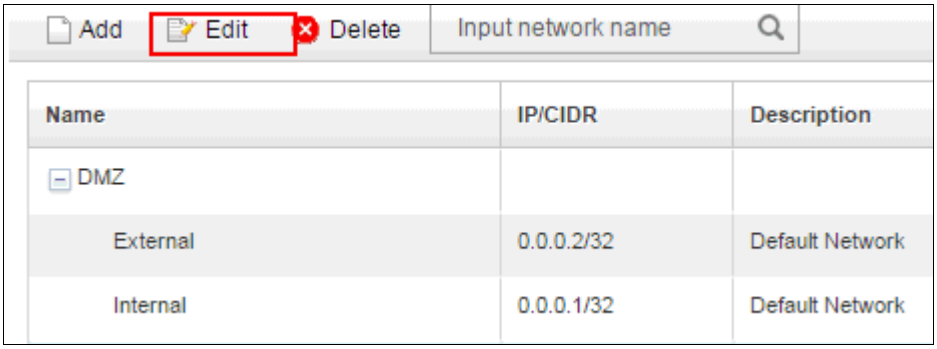


Figure 2-31 Networks IP parameters definition

- User roles

  It is extremely important to be able to validate that specific users with defined roles are counted based on the accesses that should be made by the people who are going to enter the QRadar platform. It is also extremely important to document user profiles created. See Figure 2-32.

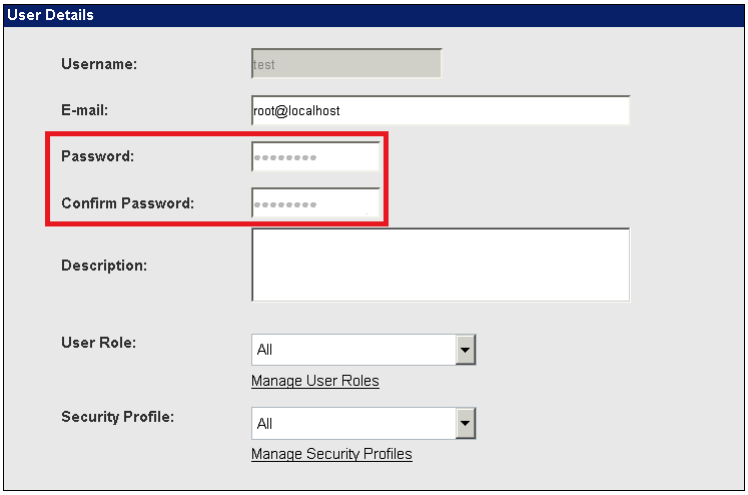


Figure 2-32 User Details

User roles can be configured with different characteristics (Figure 2-33).

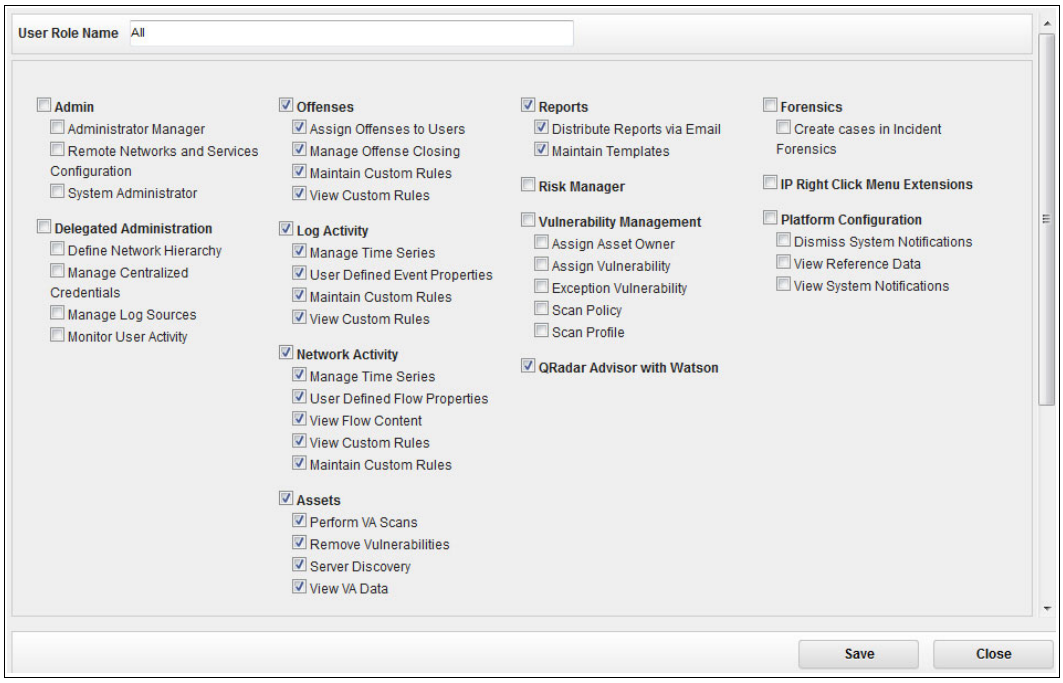


Figure 2-33 User roles

2.6 Requirements

This section provides information about the required software and hardware that is necessary to efficiently implement QRadar 7.3 into an environment. It also provides useful information to adapt to any possible scenario. For easier understanding of the requirements, it is divided into the following sections:

- Infrastructure
- System requirements for virtual appliances
- Memory and disk space requirements
- Prerequisites for installing QRadar on your own hardware

2.6.1 Infrastructure

IBM Security QRadar appliances are pre-installed with software and the Red Hat Enterprise Linux operating system. QRadar software can also be installed on your own hardware.

The IBM Security QRadar system can be installed on a single server for small enterprises, or across multiple servers for large enterprise environments. For maximum performance and scalability, a high-availability (HA) managed host appliance can be deployed for each system that requires HA protection. Further details about QRadar HA deployments are covered later in the book.

IBM Security QRadar V7.3.0 uses Red Hat Enterprise Linux V7.3, which makes QRadar more secure, Red Hat Enterprise Linux also supports Logical Volume Management (LVM) which provides flexible and advanced disk partitioning. With LVM, you can create partitions, resize them and aggregate clusters of storage together.

After installing the IBM Security QRadar system, you must apply the license keys, the system includes a temporary license key that provides access to QRadar software for five weeks, so it is required to add purchased licenses within the grace period. By default the temporary licenses uses a 5,000 Events Per Second (EPS) threshold and 200,000 Flows per interval.

Use Integrated Management Module (IMM) which is in the back panel of each appliance, for remote management of the hardware and operating systems, independent of the status of the appliance.

It is recommended to configure the IMM in dedicated mode, to reduce the risk of losing the connection when the appliance is restarted. To configure the IMM you need to access the system BIOS settings by pressing F1 when the IBM splash screen is displayed.

Install the IBM Security QRadar Console or managed host on the QRadar appliance or on your own appliance. Software versions for all QRadar appliances in a deployment must have the same version and fix level, if this is not the case the deployment won't be supported.

Recommendations

Before you begin ensure that the following requirements are met:

- The required hardware is installed.
- You have the required license key for the appliances.
- IMM access in enabled.
- There are no expired licenses on either the console or the managed hosts.

Note: If you are prompted for a user name and password before the installation wizard begins, type `root` for the user and `password` for the password.

Before installing the Red Hat Enterprise Linux operating system on your own appliance hardware, ensure that your system meets the system requirements that are detailed in Table 2-1.

Table 2-1 System requirements for Red Hat Enterprise Linux installations on your own appliance

Requirement	Description
Supported software version	V7.3
Bit version	64-bit
Kickstart disks	Not supported
Network Time Protocol	Optional, need to install NTP package to use this feature.
Memory (RAM) for Console systems	Minimum 32 GB
Memory (RAM) for Event Processor	24 GB
Memory (RAM) for QRadar QFlow Collector	16 GB
Free disk space for console systems	Minimum 256 GB **Important**: For optimal performance, ensure that an extra two to three times of the minimum disk space is available.
QRadar QFlow Collector primary drive	Minimum 70 GB

Requirement	Description
Firewall configuration	Allow HTTP and HTTPS protocols, SSH-enabled. **Note**: Before you configure the firewall, disable the Security-Enhanced Linux (SELinux) option. The QRadar installation includes a default firewall template that you can update in the System Setup window.

To install QRadar by using the virtual/software option, the device must meet the minimum requirements shown in Table 2-2.

Table 2-2 Minimum requirements for appliances using the virtual/software installation option

System classification	Appliance information	IOPS	Data transfer rate (MBps)
Minimum performance	Supports XX05 licensing	800	500
Medium performance	Supports XX28 licensing	1200	1000
High Performance	Supports XX48 licensing	10000	2000
Small All-in-one or 1600	Less than 500	300	300
Event/flow Collectors	Events and flows	300	300

You can also install IBM QRadar on a virtual appliance. Ensure that you use a supported virtual appliance that meets the minimum system requirements. Red Hat Enterprise Linux is included in the IBM QRadar software ISO image and is installed as part of the QRadar software installation process. The use of Red Hat Enterprise Linux requires entitlement to a IBM QRadar Software node. To install a virtual appliance, complete the following tasks in sequence:

1. Create a virtual machine.
2. Install IBM QRadar software on the virtual machine.
3. Add your virtual appliance to the deployment.

Before you install the virtual appliance, ensure that the primary and secondary hosts have at least 130 gigabytes (Gb) of storage available and that the minimum requirements listed in Table 2-3 are met.

Table 2-3 Requirements for virtual appliances

Requirement	Description
VMWare Client	VMWare ESXi 5.0 VMWare ESXi 5.1 VMWare ESXi 5.5 VMWare ESXi 6.0
Virtual disk size on appliances	256 GB to install QRadar

Table 2-4 describes the minimum memory requirements for QRadar virtual appliances.

Table 2-4 Minimum and optional memory requirements for QRadar virtual appliances

Appliance	Minimum memory requirement	Suggested memory requirement
QRadar QFlow Virtual 1299	6 GB	6 GB
QRadar Data Node Virtual 1400	12 GB	48 GB
QRadar Event Collector virtual 1599	12 GB	16 GB
QRadar SIEM Event Processor Virtual 1699	12 GB	48 GB
QRadar SIEM Flow Processor Virtual 1799	12 GB	48 GB
QRadar SIEM All-in-One Virtual 3199	24 GB	48 GB
QRadar Log Manager Virtual 3190	24 GB	48 GB
QRadar Risk Manager	24 GB	48 GB
QRadar Vulnerability Manager Processor	32 GB	32 GB
QRadar Vulnerability Manager Scanner	16 GB	16 GB

Table 2-5 includes the supported virtual machine hardware versions.

Table 2-5 Supported virtual machine hardware versions

VMWare ESXi version	Virtual machine hardware versions
VMWare ESXi 6.0	Versions 7 – 11
VMWare ESXi 5.5	Versions 7 – 10
VMWare ESXi 5.1	Versions 7 – 19
VMWare ESXi 5.0	Versions 7 and 8

QRadar deployment in a cloud environment

Instances of IBM Security QRadar software can be installed on a cloud server that is hosted by Amazon Web Services (AWS). To establish secure communications, it is recommended to configure a Virtual Private Network (VPN) connection.

You can configure an Open VPN connection or use another mechanism, such as a cloud provider VPN infrastructure.

Important: Ensure that the following requirements are met to avoid compromised security data:

- Set a strong root password.
- Allow only specific connections to ports 443 (HTTPS), 22 (SSH), 10,000 (webmin) and 1194 (UDP, TCP for OpenVPN).

Network settings management

Use the `qchange_netsetup` script to change the network settings of the IBM Security QRadar system. Network settings that can be configured include host name, IP address, network mask, gateway, DNS addresses, public IP, and email server.

Table 2-6 includes descriptions and notes to help you configure the network settings.

Table 2-6 Description of network settings for an all-in-one QRadar console

Network settings	Description
Internet Protocol	IPv4 or IPv6
Host name	Fully qualified domain name (FQDN)
Secondary DNS server address	Optional
Public IP address for networks that use Network Address Translation (NAT)	Optional
Email server name	If you do not have an email server, use `localhost`

Common ports and services used by QRadar

Table 2-7 shows the most common ports used by QRadar that are open in a LISTEN state. The LISTEN ports are valid only when is enabled on your system.

Table 2-7 Common ports used by QRadar services and components

Port	Description	Protocol	Direction	Requirement
22	SSH	TCP	Bidirectional	Remote management access
25	SMTP	TCP	From all managed hosts to the SMTP gateway	Emails from QRadar to an SMTP gateway
443	Apache/HTTPS	TCP	Bidirectional	Configuration downloads to manage hosts from the QRadar Console
514	Syslog	UDP/TCP	Bidirectional	External network appliances that provide TCP syslog events use bidirectional traffic
2055	NetFlow data	UDP	From the log source to the collector	NetFlow datagram form components, such as routers
6543	High-availability heartbeat	TCP/UDP	Bidirectional	Heartbeat ping from a secondary host to a primary host in an HA cluster to detect hardware or network failure
8413	WinCollect agents	TCP	Bidirectional	Generated by the WinCollect agent

Log Sources types and configurations

A log source is any external device, system, or cloud service that is configured to either send events to the IBM Security QRadar system or to be collected by the QRadar system itself. For example, a firewall or intrusion protection system (IPS) logs security-based events and switches or routers log network-based events. To receive raw events from log sources, QRadar supports many protocols. Passive protocols listen for events on specific ports.

QRadar supports protocols, including syslog from operating system applications, firewalls, IPS/IDS, SNMP, SOAP, and JDBC for data from database tables and views. QRadar also supports proprietary vendor-specific protocols such as OPSEC/LEA that are used by Checkpoint systems.

To configure a log source for QRadar, complete the following tasks:

1. Download and install a device support module (DSM) that supports the log source. A DSM is software application that contains the event patterns that are required to identify and parse events from the original format of the event log to the format that QRadar can use.
2. If automatic discovery is supported for the DSM, wait for QRadar to automatically add the log source to your list of configured log sources as described on the components section before.
3. If automatic discover is not supported for the DSM, manually create the log source configuration.

If a log source is not automatically discovered, a log source can be manually added to receive events from the network devices or appliances.

Table 2-8 describes the common log sources parameters for all log source types.

Table 2-8 Log source parameters

Parameter	Description
Log Source Identifier	The IPv4 address or host name that identifies the log source. A unique identifier for each, such as an IP address, prevents event searches from identifying the management console as the source for all of the events.
Enabled	When this option is not enabled, the log source does not collect events and the log source is not counted in the license limit.
Credibility	The credibility of events from log sources contributes to the calculation of the offense magnitude and can increase or decrease the magnitude value of an offense.
Target Event Collector	Specifies the QRadar Event Collector that polls the remote log source.
Coalescing Events	Increases the event count when the same event occurs multiple times within a short time interval. Coalesced events provide a way to view and determine the frequency with which a single event type occurs on the Log Activity tab.

Adding bulk log sources

You can add up to 500 Microsoft Windows or Universal DSM log sources at one time. When you add multiple log sources at one time, you add a bulk log source in QRadar. Bulk log sources must share a common configuration.

Log Source Extensions

A Device Support Module (DSM) is a configuration file that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as an output. Each type of log source has a corresponding DSM.

After the events are collected and before the correlation can begin, individual events from the devices must be properly normalized (normalization means to map information to common field names, such as event name, IP address, protocol and ports).

If an enterprise network has one or more network or security devices that QRadar does not provide a corresponding DSM, you can use the Universal DSM or log source extension. To configure the Universal DSM, you must use device extension to associate a Universal DSM to devices.

An extension document can extend or modify how the elements of a particular log source are parsed. You can use the extension document to correct a parsing issue or override the default parsing for an event from an existing DSM.

An extension document can also provide event support when a DSM does not exist to parse events for an appliance or security device in your network. An extension document is an Extensible Markup Language (XML) formatted document that can be created or edited by using any common text, code or markup editor.

Multiple extension documents can be created but a log source can have only one applied to it.

The XML format requires that all regular expression (regex) patterns be contained in character data (CDATA) sections to prevent the special characters that are required by regular expressions from interfering with the markup format. For example, the following code shows the regex for finding protocols:

```
<pattern id="ProtocolPattern" case-insensitive="true" xmlns="">
<![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
(TCP|UDP|ICMP|GRE) is the regular expression pattern.
```

The log sources extension configuration consists of the following sections:

- Pattern

  Regular expressions patterns that you associate with a field name. Patterns are referenced multiple times within the log source extension file.

- Match groups

  An entity within a match group that is parsed, for example, `EventName`, and is paired with the appropriate pattern and group for parsing. Any number of match groups can appear in the extension document.

2.6.2 System requirements for virtual appliances

The ensure that IBM QRadar has optimal performance, refer to the requirements listed in Table 2-3 on page 44 for virtual designs. In addition, Table 2-4 on page 45 describes the minimum memory requirements for QRadar virtual appliances.

Table 2-9 lists sample CPU page settings.

Table 2-9 Sample CPU page settings

Number of processors	Performance based on QRadar appliances
4	Log manager 3190: 2500 events per second or less
	Log manager Event Processor 1690, or SIEM Event Processor 1690: 2500 events per second or less
	All-in-One 3190: 25000 flows per minute or less, 500 events per second or less
	Flow Processor 1790: 150,000 flows per minute
	Dedicated Console 3190

Number of processors	Performance based on QRadar appliances
8	Log manager 3190: 5000 events per second or less
	Log manager Event Processor 1690, or SIEM Event Processor 1690: 5000 events per second or less
	All-in-One 3190: 50000 flows per minute or less, 1000 events per second or less
	Flow Processor 1790: 300,000 flows per minute
12	All-in-One 3190: 100,000 flows per minute or less, 1000 events per second or less
16	Log manager Event Processor 1690, or SIEM Event Processor 1690: 20,000 events per second or less
	All-in-One 3190: 200,000 flows per minute or less, 5000 events per second or less
4	QRadar Vulnerability Manager scanner
	Use four CPUs for best performance
8	QRadar Risk Manager
	Use 8 CPUs for best performance

2.6.3 Memory and disk space requirements

Table 2-10 describes the minimum and suggested memory requirements for QRadar appliances. The minimum requirements define the amount of memory required for the software features to run. The suggested requirements include the optimal amount of memory for current and future software futures. Appliances that have less than the suggested requirements might experience performance issues during periods of excessive event and flow traffic.

Table 2-10 Minimum and optional memory requirements for QRadar appliances

Appliance	Minimum memory requirement	Suggested memory requirement
QFlow Collector 1201	6 GB	6 GB
QFlow Collector 1202	6 GB	6 GB
QFlow Collector Virtual 1299 without QRadar Vulnerability Scanner	2 GB	2 GB
QFlow Collector Virtual 1299 with QRadar Vulnerability Scanner	6 GB	6 GB
QFlow Collector 1301	6 GB	6 GB
QFlow Collector 1310	6 GB	6 GB
QRadar Event Collector 1501	12 GB	16 GB
QRadar Event Collector Virtual 1599	12 GB	16 GB
QRadar Event Processor 1601	12 GB	48 GB
QRadar Event Processor 1605	12 GB	48 GB

Appliance	Minimum memory requirement	Suggested memory requirement
QRadar Event Processor 1624	64 GB	64 GB
QRadar Event Processor 1628	128 GB	128 GB
QRadar Event Processor Virtual 1699	12 GB	48 GB
QRadar Flow Processor 1701	12 GB	48 GB
QRadar Flow Processor 1705	12 GB	48 GB
QRadar Flow Processor 1724	64 GB	64 GB
QRadar Flow Processor 1728	128 GB	128 GB
QRadar Flow Processor Virtual 1799	12 GB	48 GB
QRadar Event and Flow Processor 1805	12 GB	48 GB
QRadar Event and Flow Processor 1824	64 GB	64 GB
QRadar Event and Flow Processor 1828	128 GB	128 GB
QRadar SIEM 2100	24 GB	24 GB
QRadar SIEM 2100 Light	24 GB	24 GB
QRadar SIEM 3100	24 GB	48 GB
QRadar SIEM 3105	24 GB	48 GB
QRadar SIEM 3124	64 GB	64 GB
QRadar SIEM 3128	128 GB	128 GB
QRadar SIEM Virtual 3199	24 GB	48 GB
QRadar xx48	128 GB	128 GB
QRadar Network Packet Capture	128 GB	128 GB
QRadar Network Insights	128 GB	128 GB
QRadar xx48	128 GB	128 GB
QRadar Log Manager 1605	12 GB	48 GB
QRadar Log Manager 1624	64 GB	64 GB
QRadar Log Manager 1628	128 GB	128 GB
QRadar Log Manager 2100	24 GB	24 GB
QRadar Log Manager 3105	24 GB	48 GB
QRadar Log Manager 3124	64 GB	64 GB
QRadar Log Manager 3128	128 GB	128 GB
QRadar Log Manager 3199	24 GB	48 GB

Other memory requirements

If the following conditions are met, extra memory might be required:

- If you plan to enable payload indexing, your system requires a minimum of 24 GB of memory. However, 48 GB of memory is suggested.
- If you install QRadar software on your own hardware, your system requires a minimum of 24 GB of memory.

Disk space requirements

Before installing or upgrading QRadar V7.3.0, ensure that the total size of the primary disk is at least 130 GB. The upgrade pretest determines whether a partition includes enough free space to complete an upgrade. Before you can upgrade, you must free sufficient disk space on the partition that is defined in the pretest error message.

2.6.4 Prerequisites for installing QRadar on your own hardware

Before you install the Red Hat Enterprise Linux operating system on your own appliance hardware, ensure that your environment meets the system requirements. Red Hat Enterprise Linux is included in the QRadar ISO image and is installed as part of the QRadar software installation process. Use of Red Hat Enterprise Linux requires entitlement to a QRadar Software Node. Contact your sales representative for entitlement to a QRadar Software Node.

Make sure you disable Security-Enhanced Linux (SELinux), and restart your appliance before your begin with the QRadar installation.

Table 2-11 lists the system requirements for Red Hat Enterprise Linus installations on your own appliance.

Table 2-11 System requirements for Red Hat Enterprise Linux installations on your own appliance

Requirement	Description
Supported software version	V7.3
Bit version	64-bit
KickStart disks	Not supported
Network Time Protocol (NTP) package	Optional If you want to use NTP as your time server, ensure that you install the NTP package.
Memory (RAM) for Console systems	Minimum 32 GB **Important**: You *must* upgrade your system memory *before* you install QRadar.
Memory (RAM) for Event Processor	24 GB
Memory (RAM) for QRadar QFlow Collector	16 GB
Free disk space for Console systems	Minimum 256 GB **Important**: For optimal performance, ensure that an extra two to three times of the minimum disk space is available.
QRadar QFlow Collector primary drive	Minimum 70 GB

Requirement	Description
Firewall configuration	WWW (HTTP, HTTPS) enabled SSH-enabled **Important**: Before you configure the firewall, disable the SELinux option. The QRadar installation includes a default firewall template that you can update in the System Setup window.

Storage

Storage works in a similar manner in all information systems. All data that needs to be saved, requires a *storage architecture*. QRadar is not the exception for these kinds of situations and a good storage architecture and policies can ensure that the system will run at optimal performance. Many different architectures can be applied to the QRadar solution, and it can be adapted to almost all environments.

QRadar storage requirements

As mentioned previously, the QRadar platform allows multiple methods of deployment regarding storage. The storage subsystem in use can directly impact the performance of the system, for example external storage, iSCSI, Fibre Channel, and or virtual devices.

Depending on the infrastructure where QRadar will be deployed, you need to take into consideration the size of the solution, the storage capacity, I/O operations, disk latency, and other factors. In other words, a higher level of storage can translate into better performance for the QRadar and can write, index, and query data.

When looking for storage requirements, take into consideration the following aspects for building a storage architecture:

- Number of users: This value is translated into the amount of I/O operations, queries, and reports that each user performs in QRadar. The data querying is the most impacted by the I/O operations of the storage.
- Capacity of Storage: This value is entirely dependant of how much data is required to be saved. At the end of each hour, the system consolidates indexes that are created on a minute-by-minute basis. This process allows fewer search queries when looking for data and larger reads to be performed. Subsequently, higher throughput capacity on storage devices reduces the impact in I/O operations and latency when consulting data in storage systems.

Techniques to reduce storage

As data is saved in QRadar's storage, more and more information is accumulated and occupies all capacity in your storage architecture. The following items can help to reduce and manage data more efficiently:

- Force deletion of data outside retention requirements. You can enable an option in your retention requirements to delete data outside the scheduled retention window.
- Use retention buckets to partition data. Retention buckets allow you to partition and segregate data into multiple containers. These containers can be modified with specific retention or deletion options. You can store pieces of data within short periods of time and put them into a retention bucket with a force-delete option with the date and time that it is required to be deleted.

- Disable unused indexes. Data on disks is indexed across all the storage unit. There are around 15 properties enabled by default in QRadar regarding data indexing. Indexes are often used for searches, and unused properties can be disabled in the Index Management to reduce space utilization.

Impacts of storage hardware speed

Each QRadar subsystem uses storage in its own way. Whether it is saving user queries or searches, storing offenses, editing or eliminating rules, or user management. Each of these subsystems can have various impacts to the storage of the system.

Postgres, data updates, and user interface

These components affects directly the disk latency, seek times, and I/O per second (IOPS), The component that impacts with high latency is “postgresql database” inside QRadar. Records inside QRadar are constantly being updated. If your postgresql database function (`/store/postgres/`) is on an external storage source it is prone to have delays and high latency. This delay can be perceived immediately as significant delay while browsing within the console.

Data collected and written to disk

This impact is more related to performance degradation of the console while collecting data. If the storage is not fast enough for high peaks of data bursts, it is possible that the processing pipeline will fill up the memory and cause data to not be written.

Data nodes and data storage

The QRadar all-in-one solution can store data within its infrastructure; however, this solution might not be the case with many users who require different sets of stand-alone storage and processing capabilities of a data node to handle specific storage requirements and to help with data retention policies.

Data node information

The following information is stored inside data nodes:

- Data nodes add storage and processing capacity.
- Data nodes are plug and play and can be added to a solution anytime.
- They integrate seamlessly within solution.
- Users can scale storage and processing power independently of data collection.

Figure 2-34 shows an example of a QRadar solution that implements data nodes.

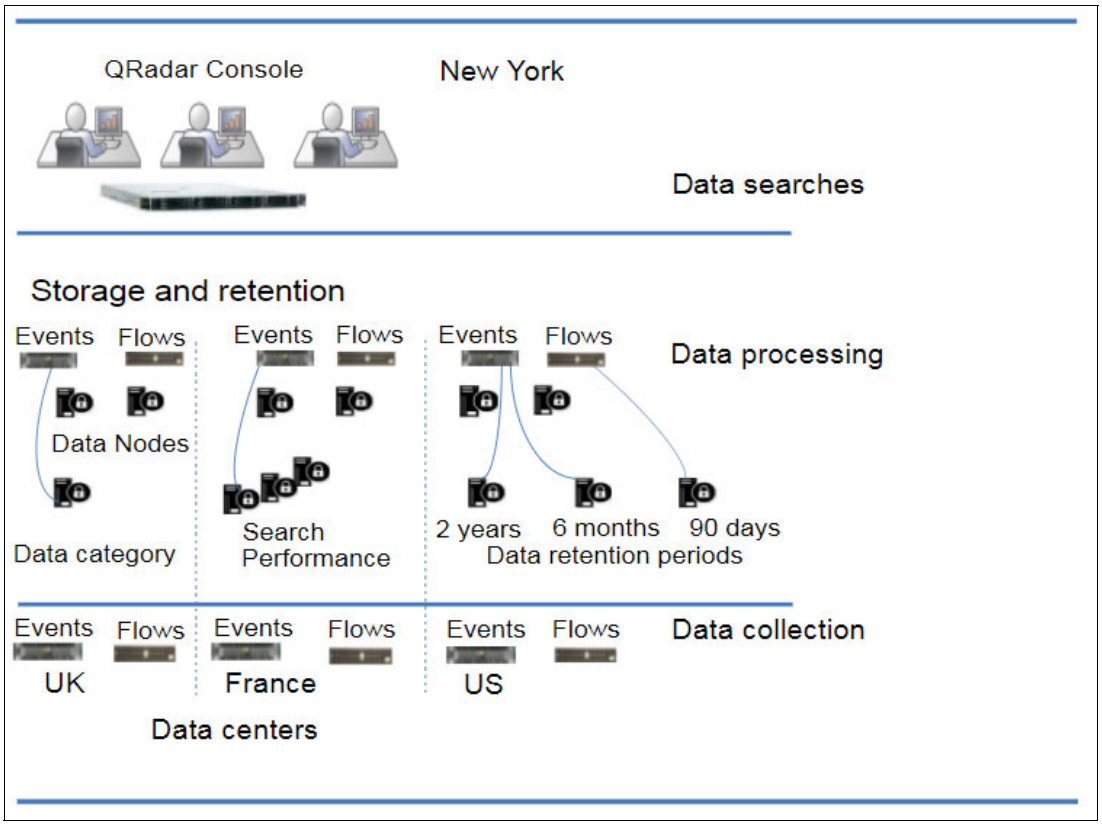


Figure 2-34 Using data node appliances to manage data storage

Data clustering

Data nodes can add storage capacity to deployment, which can improve the performance by distributing data across different storage volumes. The cluster can improve search performance but doesn't require adding multiple event processors. You can connect a data node to only one processor at a time, but a process cannot handle multiple data nodes.

Deployment considerations

The following set of parameters must be considered if it is required to install a data node:

- Data nodes are available on QRadar versions v7.2.2 and later.
- Data nodes can offer similar search speed and functions as events and flow processors. The data node system performance improves if it is sized similarly to event and flow processors within a solution.
- Data nodes are available in three formats: software, physical and in appliances.

Data nodes are compatible with all existing QRadar appliances that have event and flow processor components, including all-in-one appliances. However, they are not compatible with PCAP appliances.

Installation of Data Nodes

Data nodes use standard TCP/IP networking and do not require specialized interconnection hardware. Each data node is installed as any other QRadar appliance. It is required that the node is associated with the event or flow processors in the QRadar Deployment editor.

When deploying in high availability pairs with data node appliances, it is required to install, deploy and rebalance the HA appliance before synchronizing the HA pair. The process of removing an existing HA pair and re-synching with the new HA appliances, is mainly to avoid any performance degradation or high latency to the deployed environment.

With the deployment editor, you can decommission nodes the same way you decommission any other QRadar appliance. By decommissioning the node, it does not erase data on the host, nor does it move the information to other appliances. If it's required to keep access to the data, make sure to identify where the information was moved to.

Data rebalancing

In a data node cluster environment, data rebalancing tries to maintain the same percentage of available storage on each data node. When adding new nodes to a cluster, rebalancing is required to keep efficient disk usage on the newly added node appliances. Starting in QRadar V7.2.3, data rebalancing is automatic and concurrent with other cluster activity, and no downtime is experienced during data rebalancing.

The rebalancing can cause minor performance degradation during search operations, but data collection and processing continue unaffected.

If a data node fails, the remaining members of the cluster continue to process data. When a failed data node returns to service, data rebalancing can occur to maintain proper data distribution in the cluster. During downtimes, data on the failed nodes is unavailable, and I/O errors that occur appear in search results from the log and network activity viewers in the QRadar interface.

In case of catastrophic failures that require appliance replacement or the reinstallation of QRadar, decommission data nodes from the deployment and remove them using standard installation steps.

In storage overview

To increase the amount of storage space on your appliance, you can move the data to an off-board storage device. You can move files directories such as `/store`, `/store/ariel`, or `/store/backup` to iSCIS, Fibre Channel, or Network File System (NFS) external storage solutions. The off-board storage solution can be implemented on the QRadar primary console. When using iSCSI or Fiber Channel with HA, the external storage device ensures data consistency if your primary host fails. Before installing any off-board storage solution, it is required to consider the local storage options, existing hardware infrastructure and the fault tolerance requirements:

- Local storage: The disk on the QRadar appliance is faster than external storage and supports up to 16 TB of data. When possible, use local storage as an alternative to an external storage device.
- Multiple appliances: If larger storage capacity is required, multiple appliances can be used. In case this is not feasible, external storage might be appropriate to increase capacity.
- Hardware and infrastructure: Certain off-board devices require less configuration and might be able to use existing network infrastructures, for example, iSCSI uses existing Ethernet networking, while Fiber Channel uses more specialized hardware and SAN capabilities.
- Data Retention and fault tolerance: Each QRadar solution comes with a default data retention policy. It is important to consider this policy while implementing or deploying an off-board storage solution. It can also improve the fault tolerance and disaster recovery capabilities.

Reaching data storage limits

Reaching the limit of storage capacity is not an isolated issue on QRadar, it happens to countless other solutions, and the reason why it happens can vary because of different situations, including the topics mentioned previously regarding data burst, license levels, latency, and so on. In some instances, administrators have found they are collecting more data on one or more of their appliances than what they can store.

The following approaches address the capacity limits on the storage infrastructure:

- Optimizing space usage

  In many environments, disk usage can be brought down by tuning the QRadar storage and data retention policies. In most cases, storage space is being used for unused backups, which in some cases it is best to be stored off-board. Of all the data required to be processed and stored, some are required to be retained for shorter periods of time than others.

  - Moving backups: By default, QRadar stores its backups in the `/store/backup` directory and the backups utilize the same disk space as the main data storage. Depending on the data retention policy, the backups might be using some of the main storage space. This situation can be remediated by moving all the backups to an NFS or other off-board storage solution.
  - Tuning retention policies: Under normal circumstances, the largest and the obvious consumer of data storage space is event and flow data. In most environments, not all logs and flows require to be saved for the same periods of time. By tuning the retention policies regarding events and flows, the amount of storage usage will drop significantly. All storage retention policies can be found in the QRadar under **Admin** → **Data Sources** → **Events** → **Event Retention**.
  - Enabling coalescing: Certain data sources are repetitive and can log the same event multiple times. If the coalescing option is enabled, QRadar can correlate these repetitive events into a single event.

- Increasing storage space

  In QRadar V7.2.8, there are no supported ways to resize any of the partitions, including the data storage partition `/store`. In some cases, when a virtual appliance is being used, the installation of QRadar wants to expand the virtual disks that are assigned to their virtual appliance. On physical drives, other solutions must be implemented. Typical solutions for expanding physical storages are either deploying data nodes or checking off-board storage. Both can increase the size of storage capacity and will not impact directly in latency or access times. In the case of data nodes, they can be deployed as appliances or even as clusters for the event and flow processor to connect. Off-board storage can also be used without much configuration to migrate all data to an external storage appliance.

Check your environment requirements to see which option works best without impacting performance.

3

Installing IBM QRadar V7.3

Installing QRadar 7.3 is an easy procedure after you identify all the components and meet all the requirements.

This chapter covers the installation procedure of the tool from the scratch, including the operative system configuration, network settings, licensing configuration, and so on. The installation procedure is explained using images to help the you during this critical phase of QRadar implementation. It includes the following topics:

- Installation process
- Installing QRadar licenses
- Setting up high availability
- Installing apps
- Installation order of managed hosts
- Upgrading HA deployments
- Following the correct upgrade path

3.1 Installation process

To install QRadar on your server, first download the ISO from IBM FixCentral. After you have the ISO, you can burn it into a CD/DVD or create a bootable USB and boot from it.

To complete the installation, follow these steps:

1. Select **Install Red Hat Enterprise Linux 7.3** when presented with a menu of options, as shown in Figure 3-1.

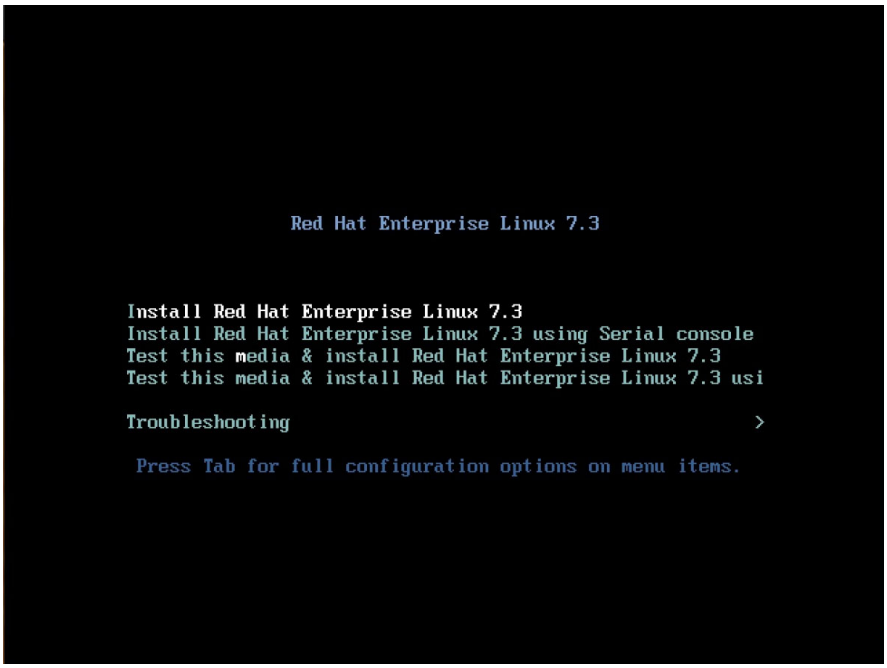


Figure 3-1 Installing Red Hat Enterprise Linux 7.3

2. Select the type of installation. This example installs as though the hardware and software came from IBM (purchased as an appliance), as shown in Figure 3-2.

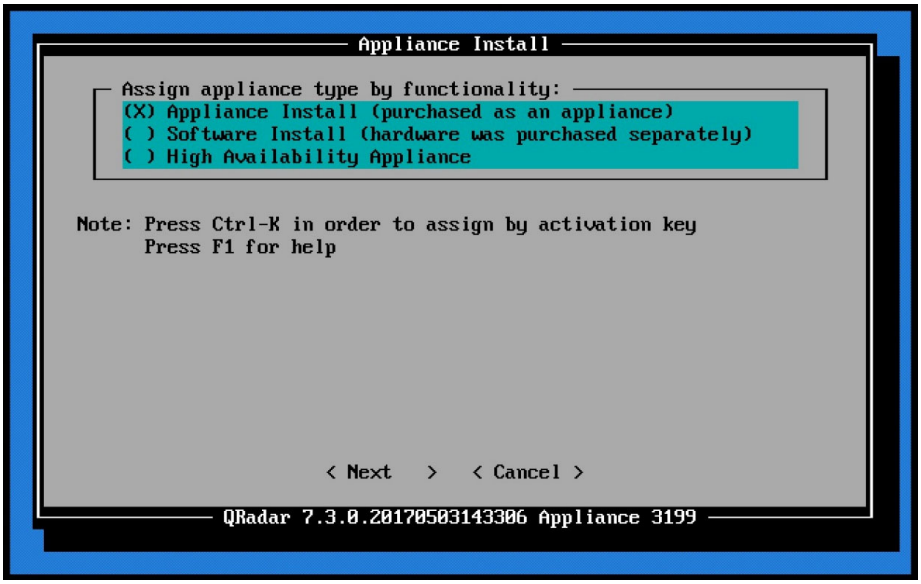


Figure 3-2 Appliance Install

3. Then select the type of setup, in this case it is a normal installation, as shown in Figure 3-3.

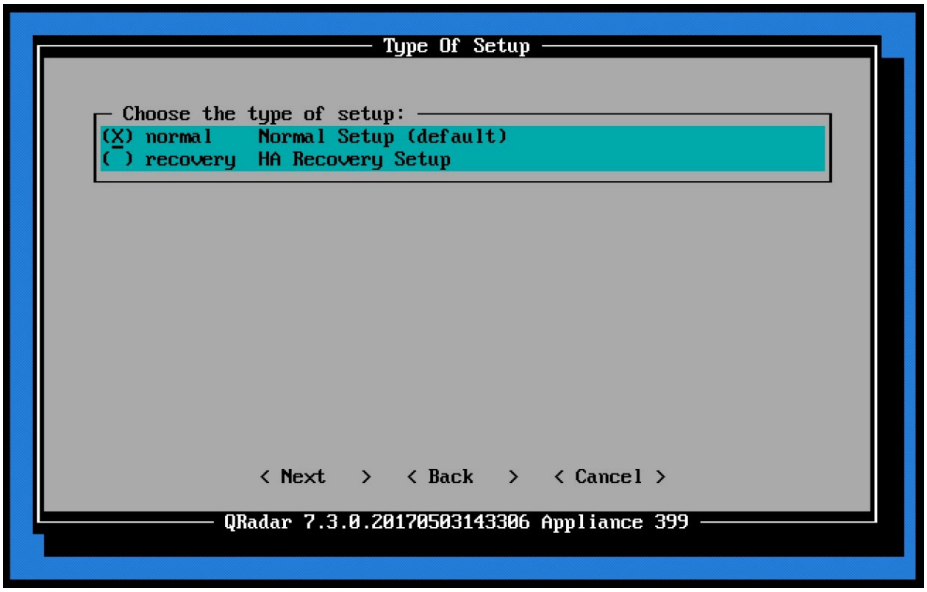


Figure 3-3 Type Of Setup

4. Next, configure the date and time manually. You can also configure time server, either by name or IP. See Figure 3-4.

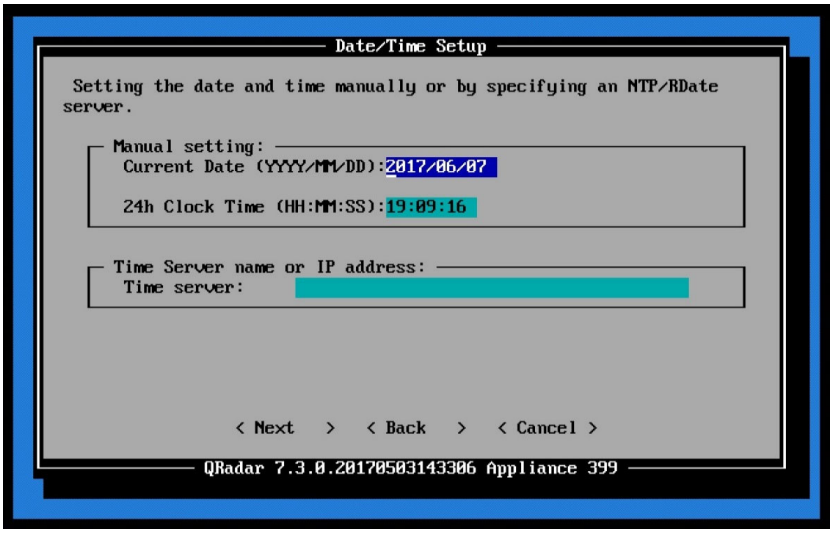


Figure 3-4 Date/Time Setup

5. Then configure the time zone of the device. In this example, configure this device to use Eastern time (New York), as shown in Figure 3-5 and Figure 3-6 on page 61.

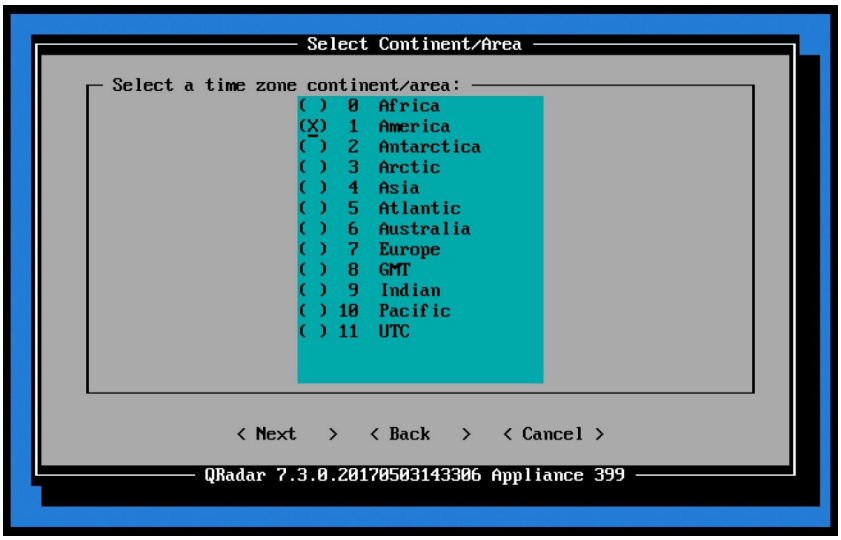


Figure 3-5 Select Continent/Area

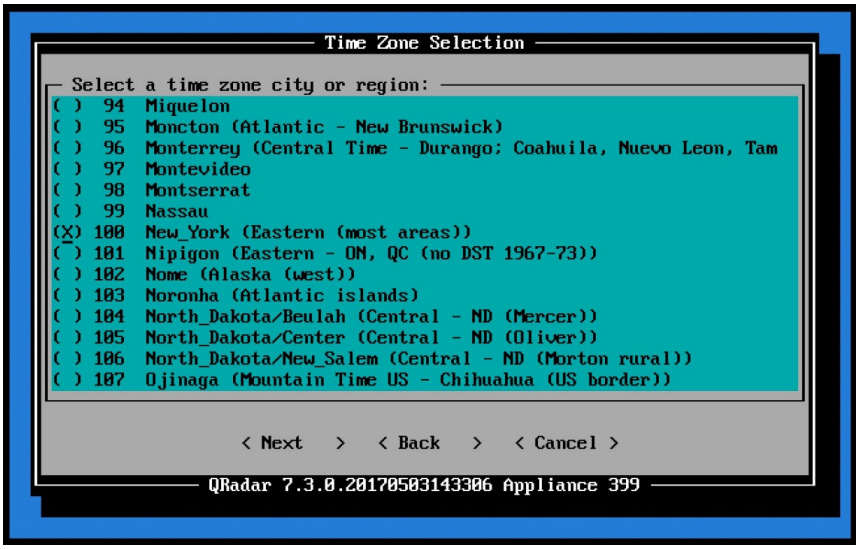


Figure 3-6 Time Zone Selection

6. Next, configure the network interface. In this example, we use IPV4, as shown in Figure 3-7.

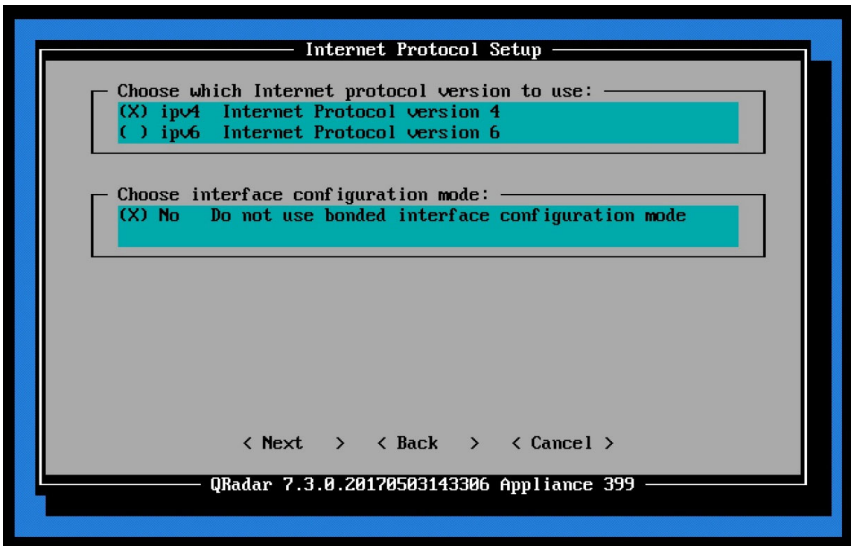


Figure 3-7 Internet Protocol Setup

7. Then, select the management interface. In this case, we have only one NIC, as shown in Figure 3-8.

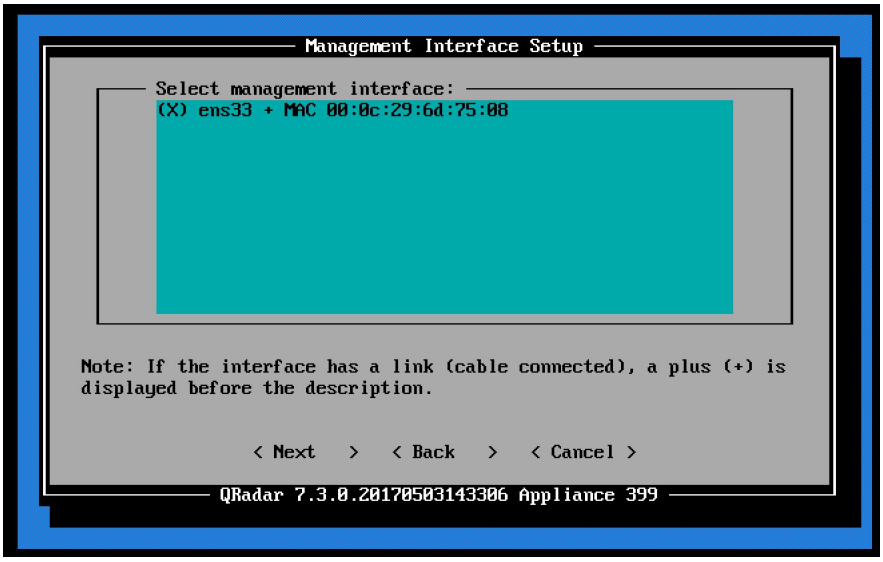


Figure 3-8 Management Interface Setup

8. Enter network information (such as the IP address, host name, netmask, and so on) as shown in Figure 3-9. You need to enter the fully qualified domain name. (In case you are installing an HA appliance, *do not* add primary or secondary to the host name, because this information is added automatically by QRadar later).

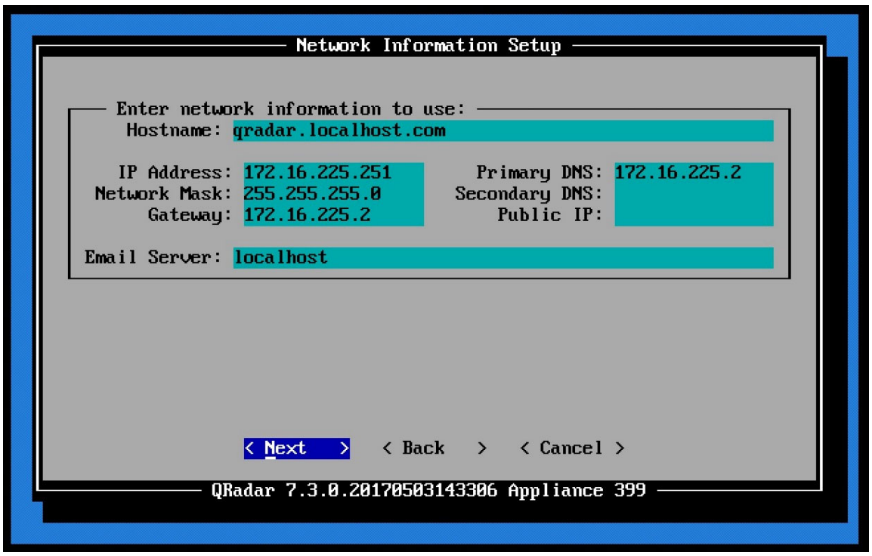


Figure 3-9 Network Information Setup

9. Enter the Admin Password, which is the password for the user admin and is used to log in via web access. See Figure 3-10.

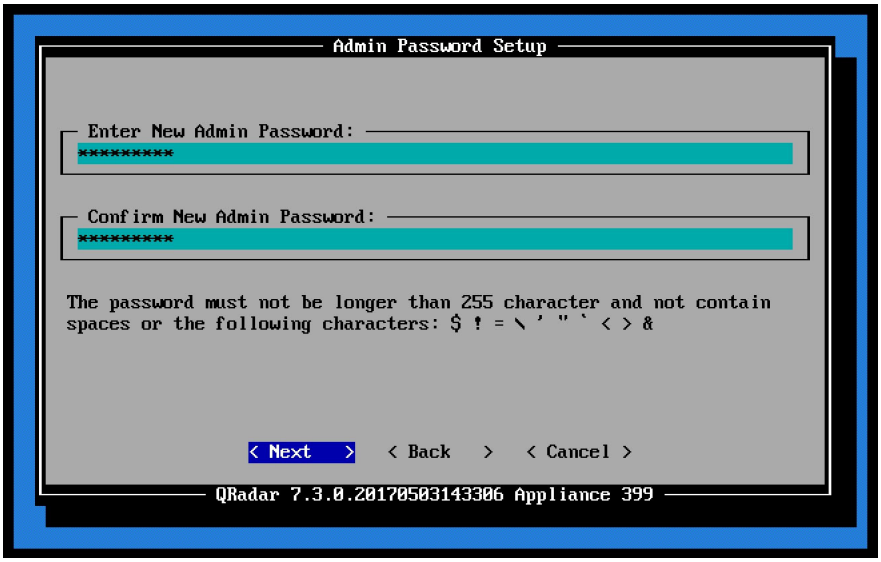


Figure 3-10 Admin Password Setup

10. Then set the root password. This root password is the user for SSH (CLI) access. See Figure 3-11.

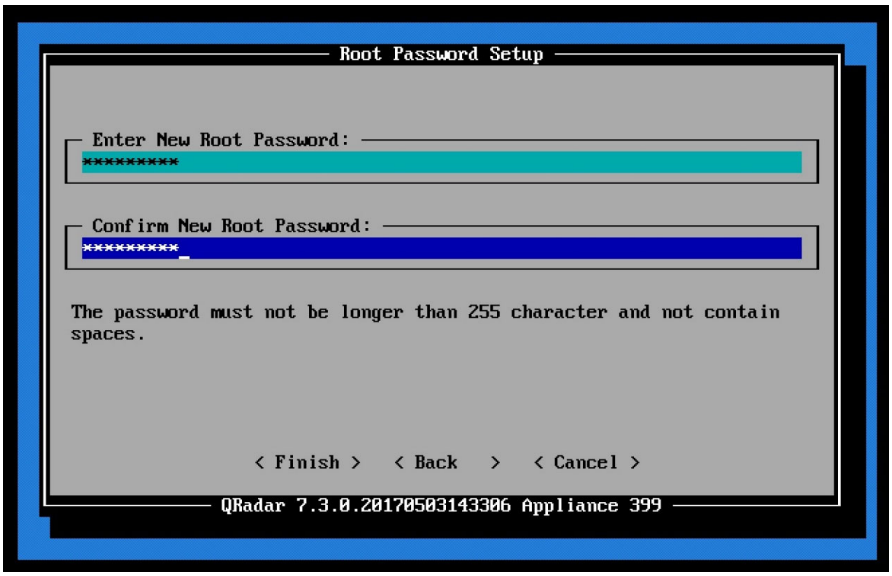


Figure 3-11 Root Password Setup

At this point, the installer continues its process automatically, as shown in Figure 3-12.

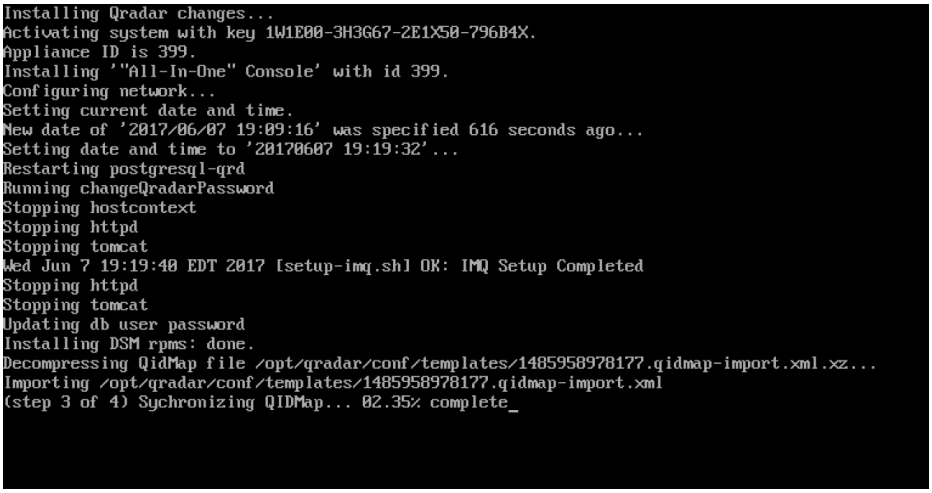


Figure 3-12 QRadar Activity Logging

When the installation process is complete, you receive the notification shown in Figure 3-13.

Figure 3-13 QRadar installation complete

3.2 Installing QRadar licenses

After the installation process is complete, you need to apply the license to the newly installed device. To apply the license:

1. Log in to the QRadar web console. Use the IP that you configured on the QRadar console:

   `https://<ip address of the console>`

2. Then, log in with the user admin and the credentials set during the installation (Figure 3-14).

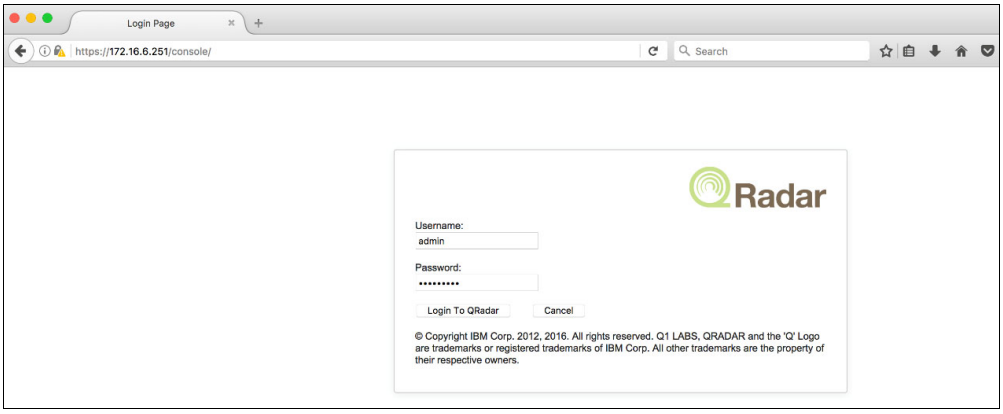


Figure 3-14 QRadar login page

3. Go to the Admin tab, as shown in Figure 3-15.

Figure 3-15 QRadar main menu

4. From there, click the System and License Management menu, as shown in Figure 3-16.

Figure 3-16 System and License Management icon

5. From the pop window, click the Upload License menu (Figure 3-17).

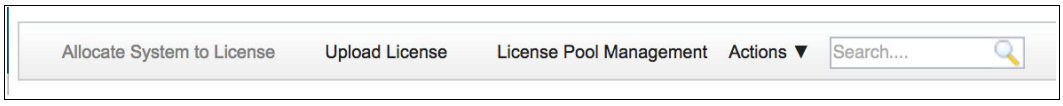


Figure 3-17 Upload License

6. Browse to select the license file for the desired device (Figure 3-18), in this case is for a console, but the process is the same for any QRadar device. After you select the fill, click the **Upload License** button.

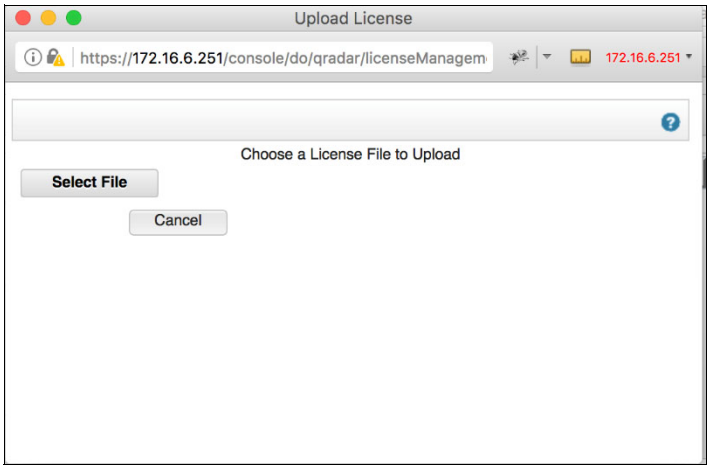


Figure 3-18 Select the desired device

7. After the license is uploaded to the console, you need to allocate it to the correct device. From the System and License Management menu, select the License Display, click the license, and then click **Allocate License to System**, as shown in Figure 3-19.

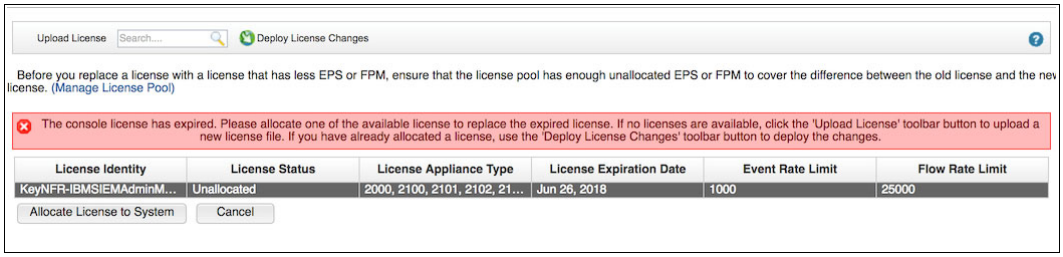


Figure 3-19 Unallocated license

8. Confirm that this is the license, and the correct device that the license needs to be allocated to. Then, click **Confirm**, as shown in Figure 3-20.

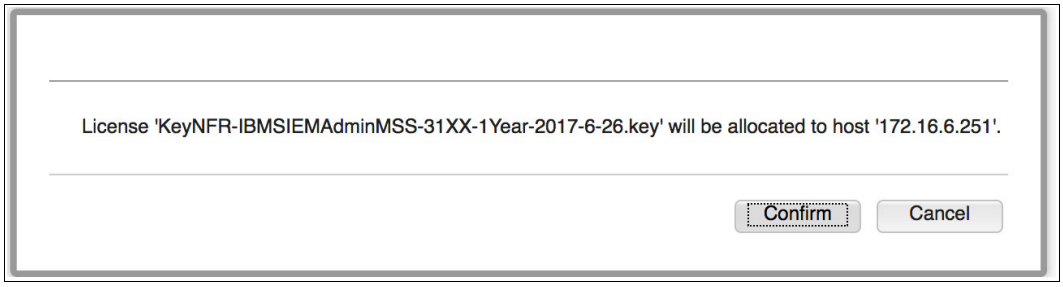


Figure 3-20 License allocation

If the process succeeds, a message displays, as shown in Figure 3-21.

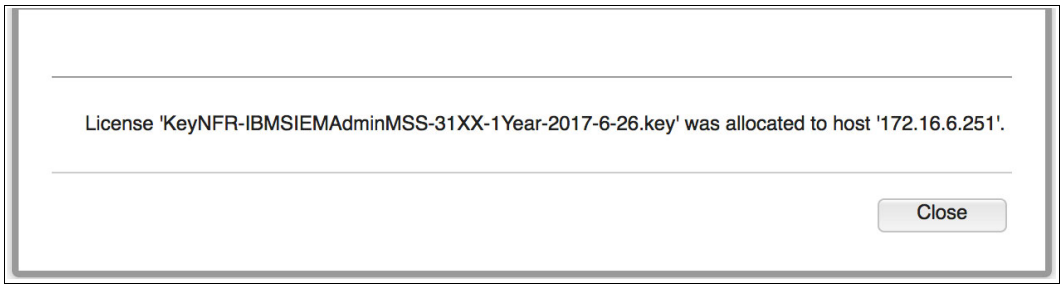


Figure 3-21 Allocation successful

9. After the license is applied and allocated to the correct device, click **Deploy License Changes** and then click **Continue**, as shown in Figure 3-22.

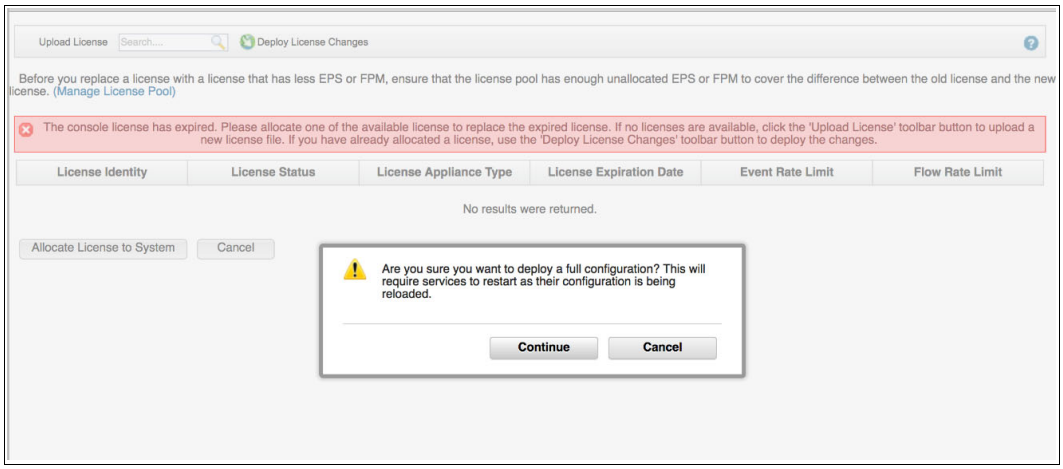


Figure 3-22 License deployment

At this point, the device is now ready to start working. A “There are no changes to deploy” message displays from the Admin tab, as shown in Figure 3-23.

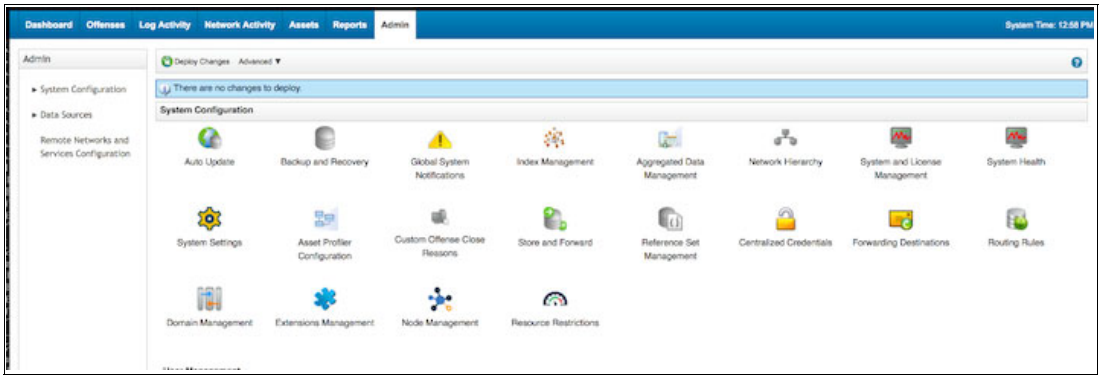


Figure 3-23 QRadar Admin tab

3.3 Setting up high availability

To set up a high availability, you need both a primary and a secondary device. You also need three IP addresses, one for each device and one for the virtual IP, which is configured on the active device and which switches between devices in case of a failure.

When installing the devices that will be part of an HA, *do not* add primary or secondary to the host name, because QRadar automatically adds this information when creating the HA. Also, the device that will act as the primary device must be configured with the virtual IP. QRadar asks the administrator for the IP of the primary devices later.

To start this process, complete these steps:

1. Go to the Admin tab and then click the System and License Management icon, shown in Figure 3-24.

Figure 3-24 System and License Management icon

2. The primary devices is added to the deployment first. Make sure you are on the Systems display, as shown in Figure 3-25.

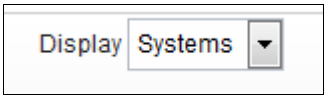


Figure 3-25 Systems display selection

3. Click the **Deployment Actions** menu and then click **Add Host**, as shown in Figure 3-26.

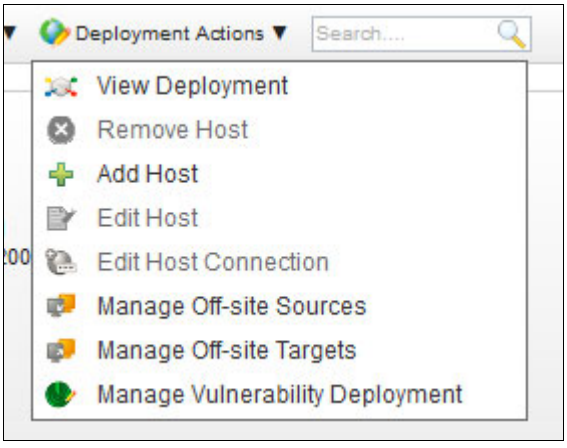


Figure 3-26 Deployment actions menu

4. Use the IP and root password of the new device to add it to the deployment, as shown in Figure 3-27.

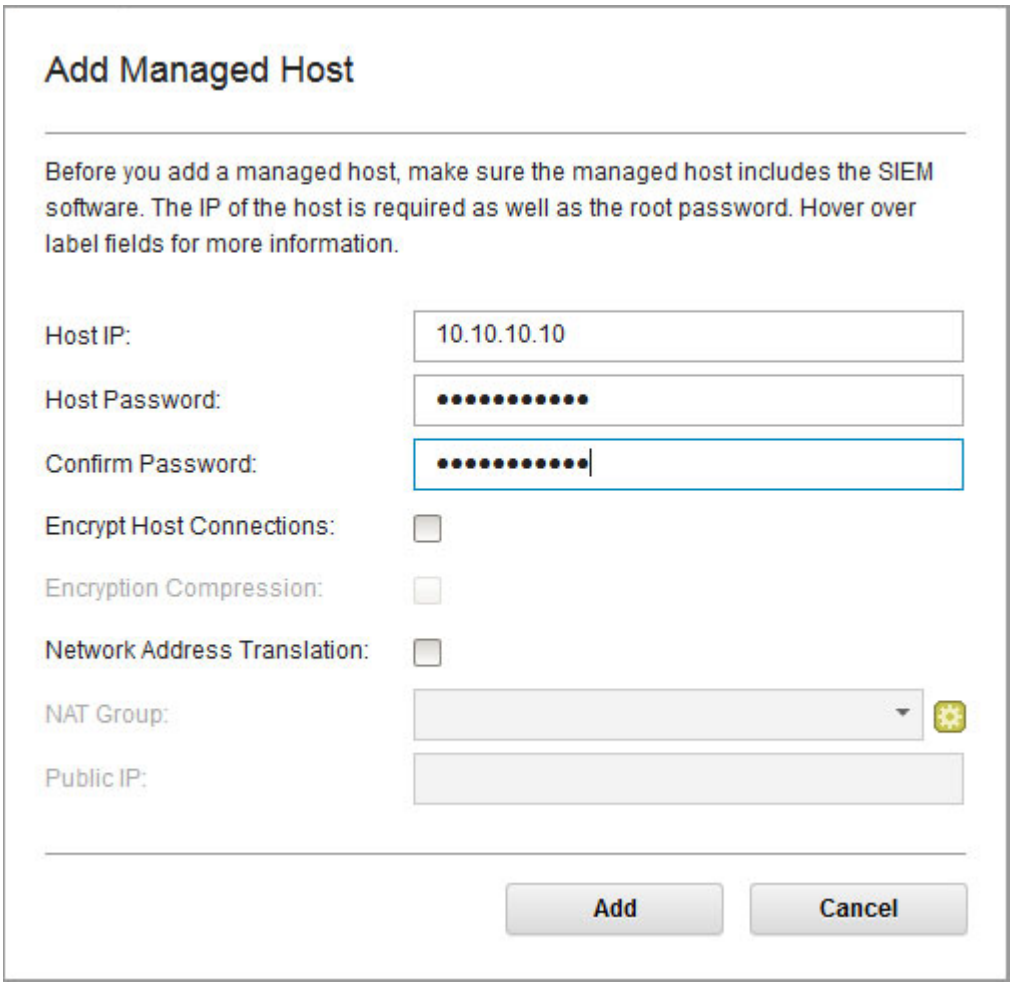


Figure 3-27 Add Managed Host form

5. After the device is part of the deployment, you can create the HA pair. Right-click the device that is going to be part of the HA pair and then click **Add HA Host**, as shown in Figure 3-28.

Figure 3-28 Add HA Host

6. The wizard prompts the administrator for the information that is needed to create the HA pair (Figure 3-29). For the Primary Host IP Address, enter the IP address of the primary devices. QRadar configures this IP address for the primary devices and uses the other IP address on the primary as the virtual IP address.

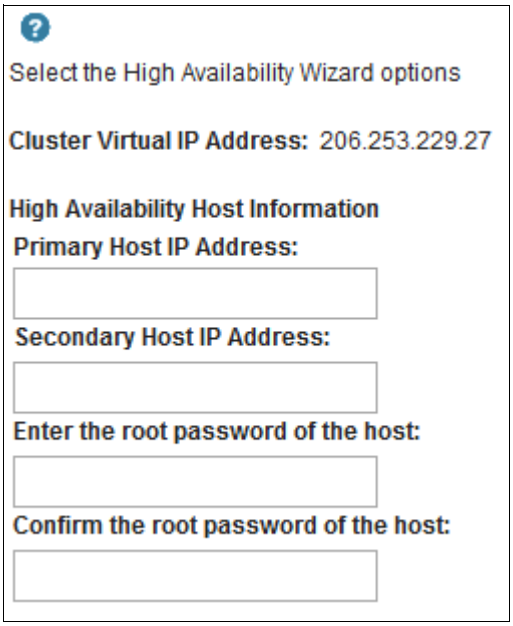


Figure 3-29 High Availability Host Information

One full deployment is needed. When that is complete, QRadar will sync the primary device with the secondary device.

7. You can configure a crossover cable between the primary device and the secondary device to make data replication more efficient and on its own interface. Click the Show Advance Options. Then, the administrator can configure the heartbeat interval, timeout, crossover interface, and IP addresses to use for the crossover cables. See Figure 3-30.

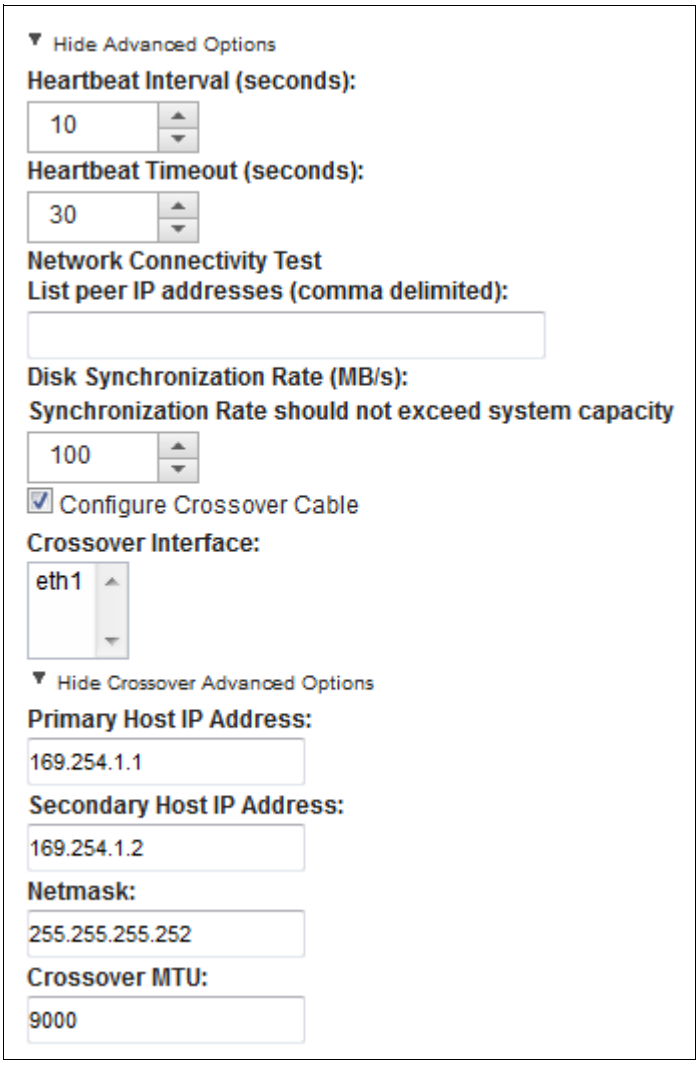


Figure 3-30 HA advanced options

3.4 Installing apps

To install apps in QRadar:

1. Go to the Admin tab and click the Extensions Management icon, shown in Figure 3-31.

Figure 3-31 Extensions Management icon

2. From there, you can manage your installed apps. To install a new app, click the IBM Security App Exchange menu to go the official page. See Figure 3-32.

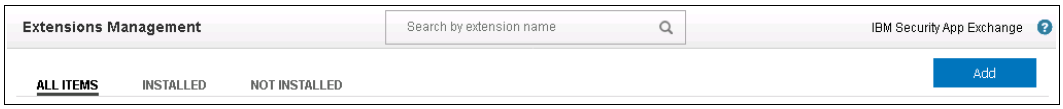


Figure 3-32 IBM Security App Exchange menu

From the website, shown in Figure 3-33, you can search all the available apps.

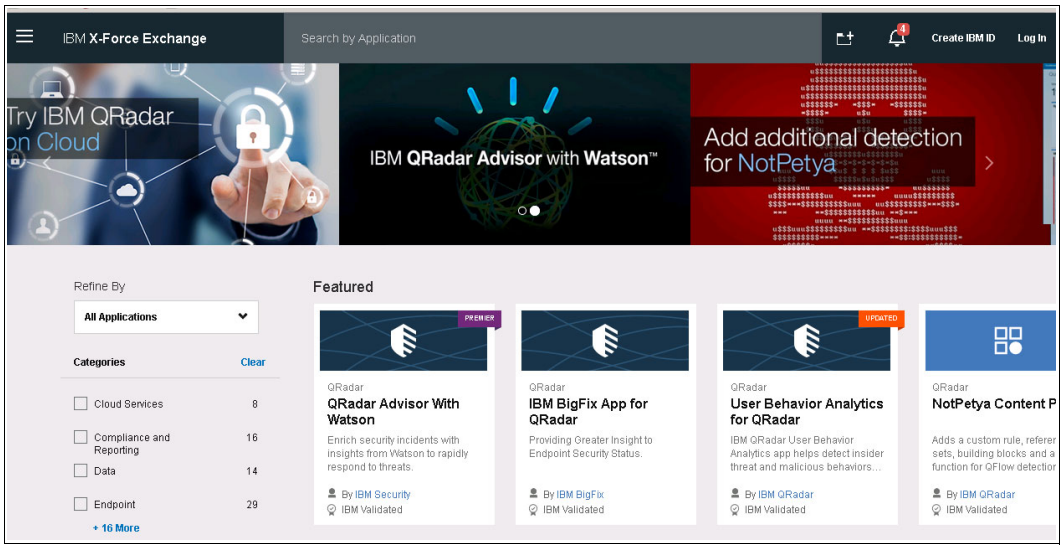


Figure 3-33 IBM Security App Exchange official web page

3. To download any apps, you need to log in first. Click the login button, and enter your credentials, as shown in Figure 3-34.

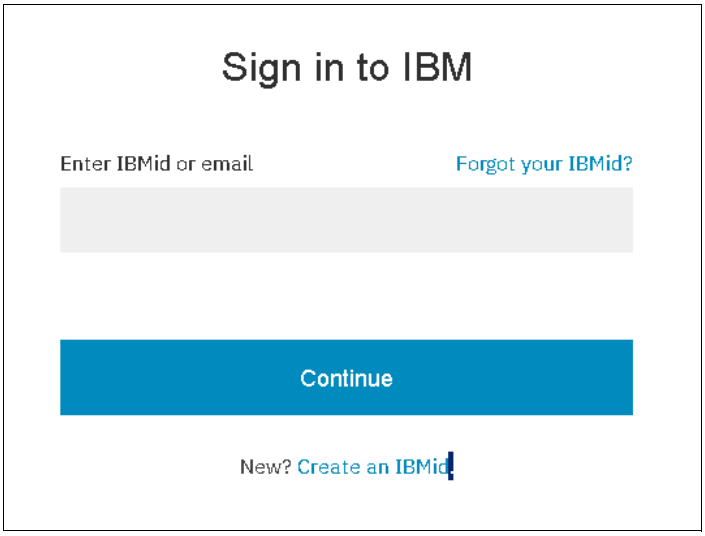


Figure 3-34 Sign in to IBM

4. After you are logged in, search for the app using its name, for example *UBA*, as shown in Figure 3-35.

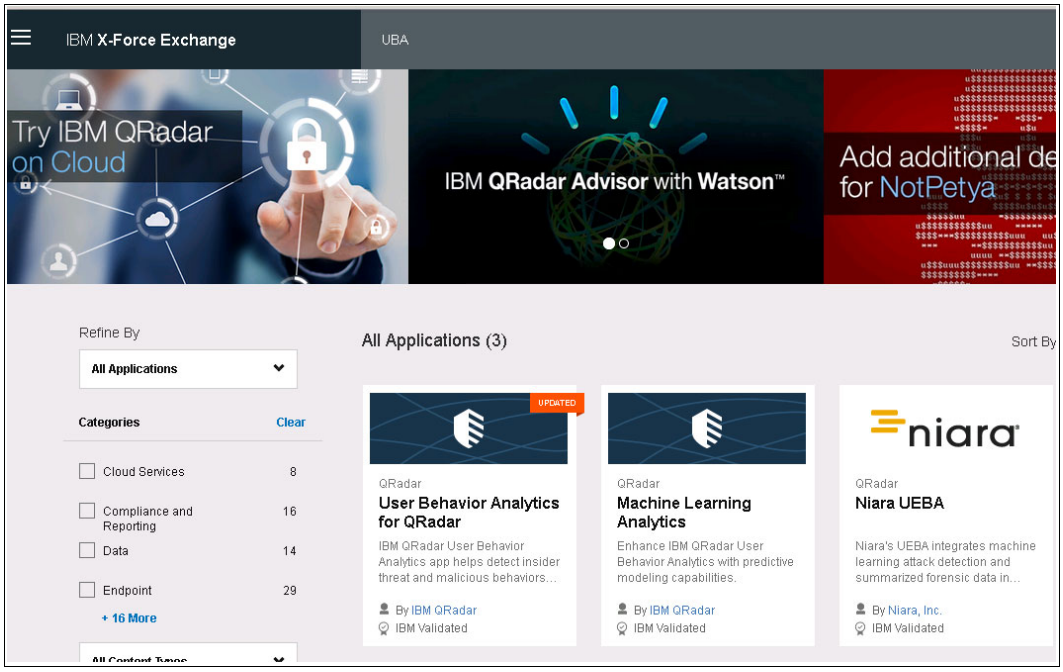


Figure 3-35 App searches from the main page

5. After you locate the app, click the name of the app, and then click **Download** (Figure 3-36).

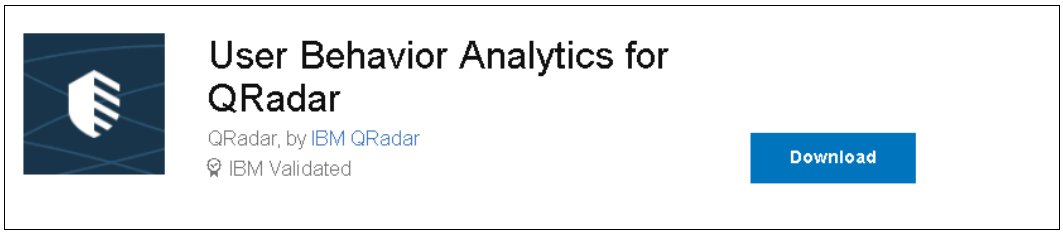


Figure 3-36 App download

6. After the download is complete, go back to the Extensions Management window and click **Add**, as shown in Figure 3-37.

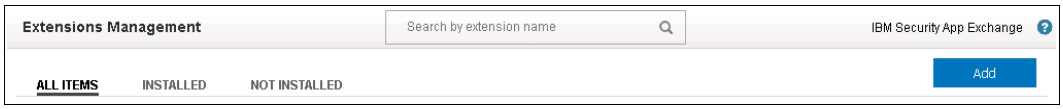


Figure 3-37 Extensions Management

7. Click **Browse** and search for the recently downloaded file. You can select the “Install immediately” option for the app to be installed right away. To install click **Add**. See Figure 3-38.

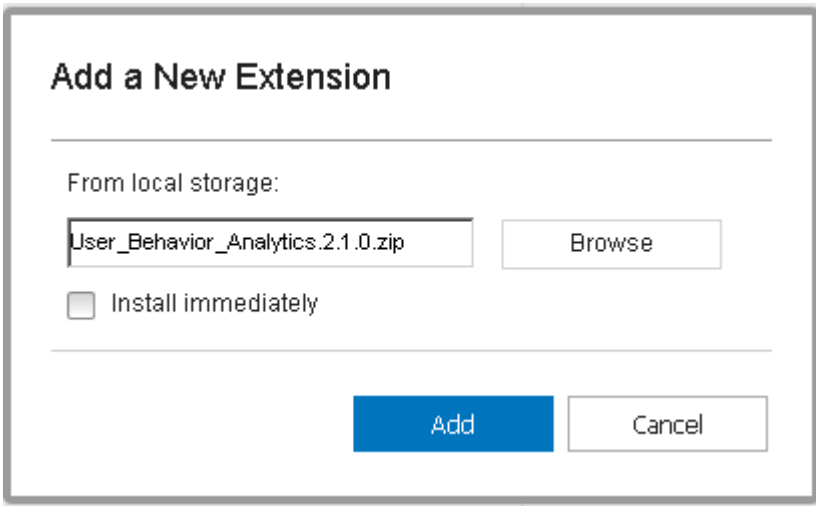


Figure 3-38 Add a New Extension

The Extensions Management window shows the status of the app (Figure 3-39). You can also uninstall the app from this window, if needed.

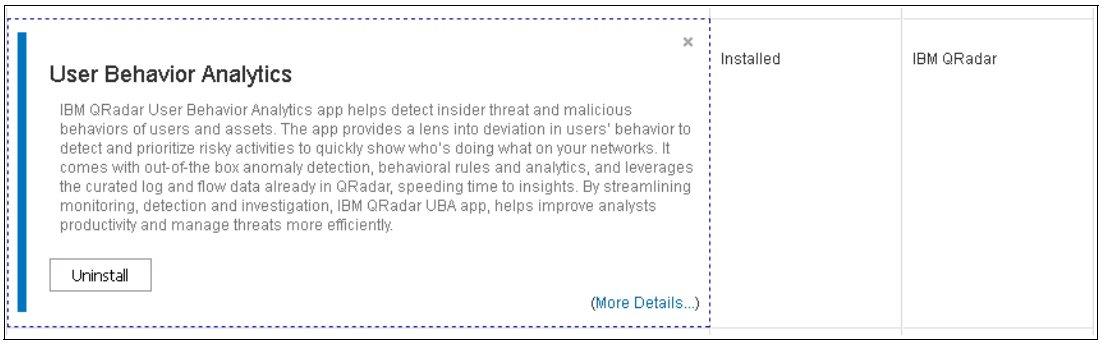


Figure 3-39 Extensions status

3.5 Installation order of managed hosts

After installing the console, you can add the managed hosts to the deployment. You can install the devices in any order, but use the following order to add them to the deployment:

1. Console
2. The following QRadar systems can be upgrade concurrently:
   - Event Processors
   - QRadar Event Collectors
   - Flow Processors
   - QFlow Collectors
   - QRadar Data Nodes
   - QRadar specialized appliances (QIF, QVM, and so on)

3.6 Upgrading HA deployments

When upgrading an HA deployment, verify that the primary device is the active device and that the secondary device is in standby. The installer applies the upgrade to the secondary device automatically.

3.7 Following the correct upgrade path

Table 3-1 shows the upgrade path that you need to follow if your QRadar is in a version lower than V7.2.4. If your QRadar is running V7.2.4 or later, you can upgrade to any other version without having to go through all the versions in between. For example, you can go from V7.2.5 to V7.3 in one step.

Table 3-1 Upgrade path

Current version	Step 1	Step 2	Step 3
7.1 (MR2) (7.1.0.501605) or later	7.2.4 (SFS)		
7.1 GA to 7.1 (MR1) Patch 3 (7.1.0.380596 to 7.1.0.495292)	7.1 MR2 Patch 2 (7.1.0.599086) (SFS)	7.2.4 (SFS)	

Current version	Step 1	Step 2	Step 3
7.0 (MR5) to 7.0 (MR5) Patch 7 (7.0.0.301503 to 7.0.0.672904)	7.1 MR2 Patch 2 (7.1.0.599086) (ISO)	7.2.4 (SFS)	
7.0 GA to 7.0 MR4 Patch 2 (7.0.0.167618 to 7.0.0.276729)	7.0 MR5 (7.0.0.301503) (SFS)	7.1 MR2, (7.1.0.599086) (ISO)	7.2.4 (SFS)

4

After the installation

This chapter covers additional steps that the administrator can follow after QRadar V7.3 is installed. Remember that no two network configurations have the same components, requirements, traffic patterns, or log sources. Therefore, you need to customize and adjust the configuration of QRadar to your environment.

This chapter is intended to provide a description of several available components that the administrator can add to the basic setup of QRadar. The administrator can use this information to understand which components can provide additional value to the console.

This chapter includes the following topics:

- Event monitoring
- Events Per Second
- Features check
- Upgrades and patching
- Health checks, monitoring tools

4.1 Event monitoring

From the Log Activity tab, shown in Figure 4-1, you can review the logs received by QRadar.

Figure 4-1 QRadar main menu

From here, you can perform searches against the logs that are stored on the system or the logs that are coming real time. You can also filter events by time by selecting from the drop-down menu. In the example shown in Figure 4-2, QRadar is showing the events from the last 5 minutes.

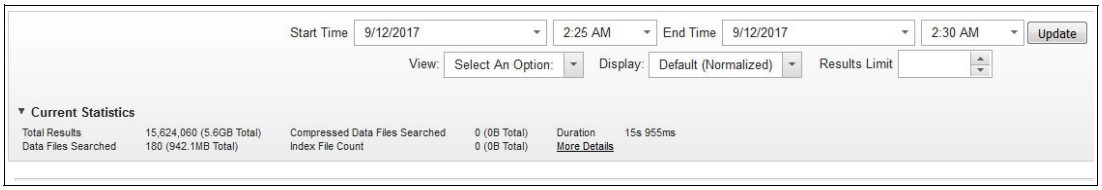


Figure 4-2 Log activity criteria

You can quickly determine if events are flowing into QRadar by viewing the Log Activity tab. You can also complete more detailed searches. For example, you can determine if a specific event processor is receiving events. Using Add Filter (Figure 4-3) and choosing the Event Processor from there (Figure 4-4) can quickly show whether events are flowing to the EP.

Figure 4-3 Filtering options

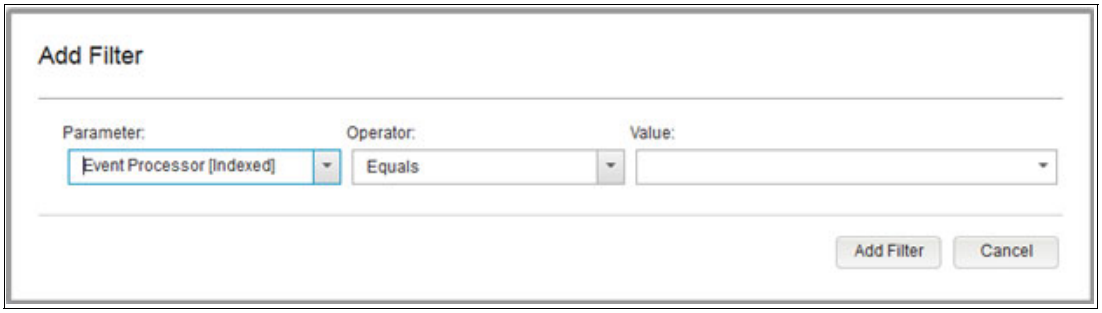


Figure 4-4 Add filter parameters

You can also create a new search from the New Search menu, as shown in Figure 4-5.

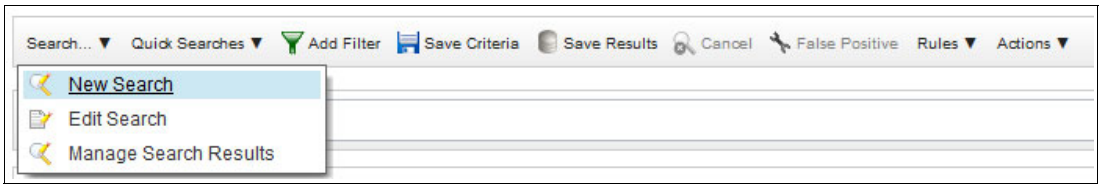


Figure 4-5 New Search option

You can filter by saved searches, as shown in Figure 4-6.

Figure 4-6 Filtering Saved Searches

The data that is going to contain the search can then be manipulated from here. You can select what columns the search is going to have and group the data by a specific column, as shown in Figure 4-7.

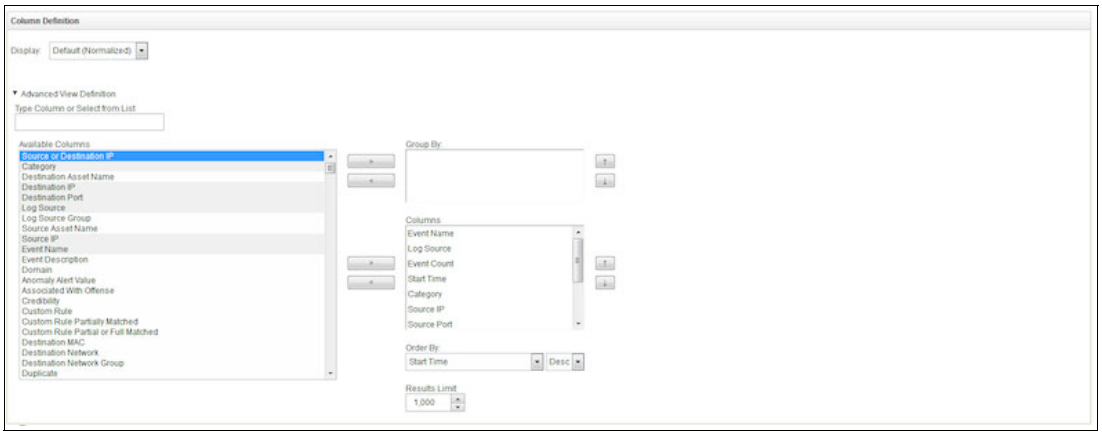


Figure 4-7 Column definition

Specifying the search parameters helps to narrow down the search to make it as accurate as possible. Parameters can, for example, help to find a specific event type by using the Event Name parameter, as shown in Figure 4-8.

Figure 4-8 Search parameters

For better performance searches, filter by the less specific to the most specific, so that the search looks like an inverted pyramid—going from the more general to the more specific.

4.2 Events Per Second

QRadar comes with a pre-built search for monitoring the Events Per Second (EPS). This search allows you to quickly determine if the number of events coming to QRadar are going over the license for each Event Processor.

To use this feature, go to the Log Activity tab, and then in Quick Searches, look for the searches named *Event Rate (EPS) – Last 15 Minutes*, as shown in Figure 4-9.

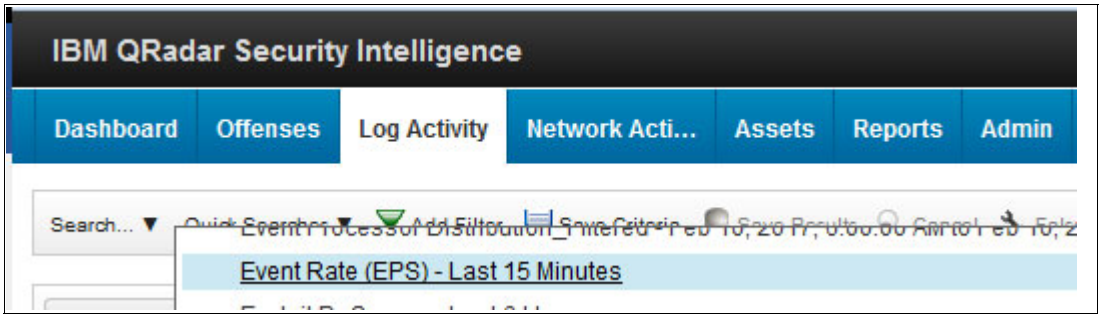


Figure 4-9 Log Activity, Event Rate (EPS)

When the search completes, you can modify it by clicking the green gear icon. There are several types of values that you can graph. The *Events per Second Raw – Peak 1 Sec* graph (Figure 4-10) gives a good picture of the EPS for each EP and the console.

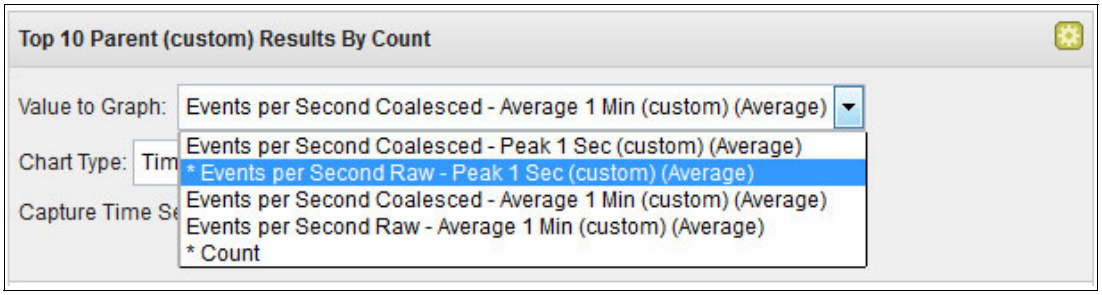


Figure 4-10 Top 10 Parent Results by Count

4.3 Features check

IBM Security QRadar can serve as a security solution for a small, medium, or large organization. It also integrates with many other products and provides complete, unified visibility to security events in on-premises, hybrid, and cloud environments. This section describes some of the most important features that are available for IBM Security QRadar.

4.3.1 IBM Security QRadar Vulnerability Manager

IBM QRadar Vulnerability Manager senses security vulnerabilities, adds context, and helps prioritize remediation activities. It uses advanced analytics to enrich the results of vulnerability scans to lower risk and achieve compliance. QRadar Vulnerability Manager correlates

vulnerability data with network topology and connection data to intelligently manage risk. A policy engine automates compliance checks. Using QRadar Vulnerability Manager can help your security team to develop an optimized action plan to address security exposures to work more efficiently and decrease costs.

Figure 4-11 shows the QRadar Vulnerability Manager dashboard.

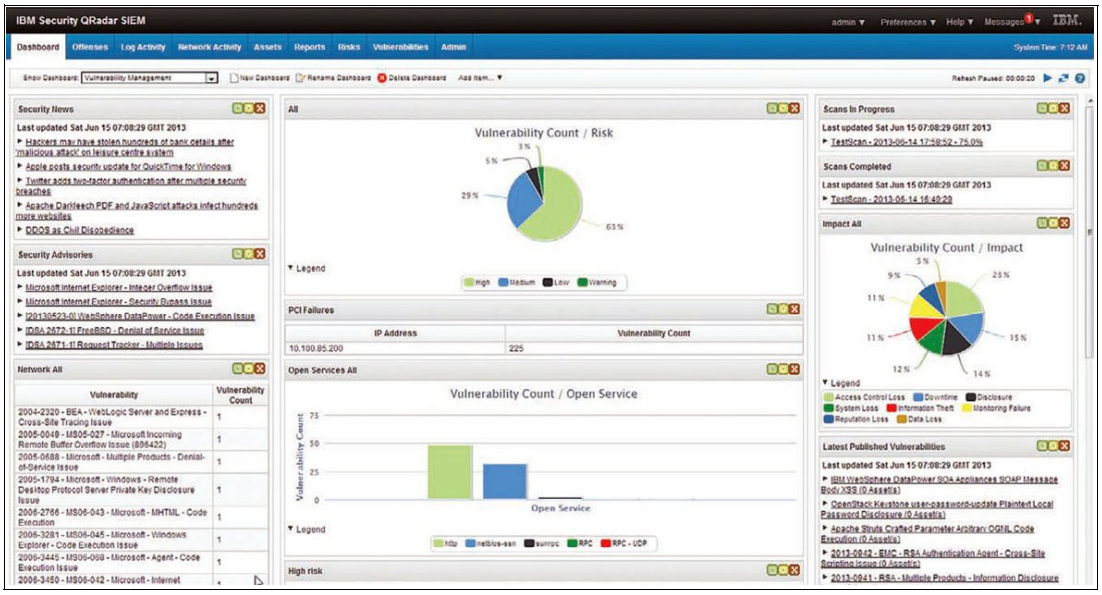


Figure 4-11 QRadar Vulnerability Management dashboard

4.3.2 The Health Check Framework for IBM Security QRadar SIEM

The Health Check Framework for IBM Security QRadar SIEM is an automated monitoring tool that allows you to continuously sustain the platform's operability and to perform periodical monitoring of a range of statistical, performance, and behavioral parameters of QRadar deployment. This tool allows you to continuously sustain the platform's operability.

The Health Check Framework (HCF) Manager, installed as a QRadar tab, is a user-side tool for HCF administrating, which provides HCF updating, report execution and scheduling, mailing list management, and reports download. This tool can be download from the this official IBM website.

The HCF Manager generates an Excel report containing all the details of the QRadar environment disk, CPU, and memory usage on managed hosts, system warning and errors, correlation rules, and reports performance, and a console summary of the system's state that includes the number of active log sources and assets, storage and memory available.

Figure 4-12 on page 82 shows the Health Check Console Summary.

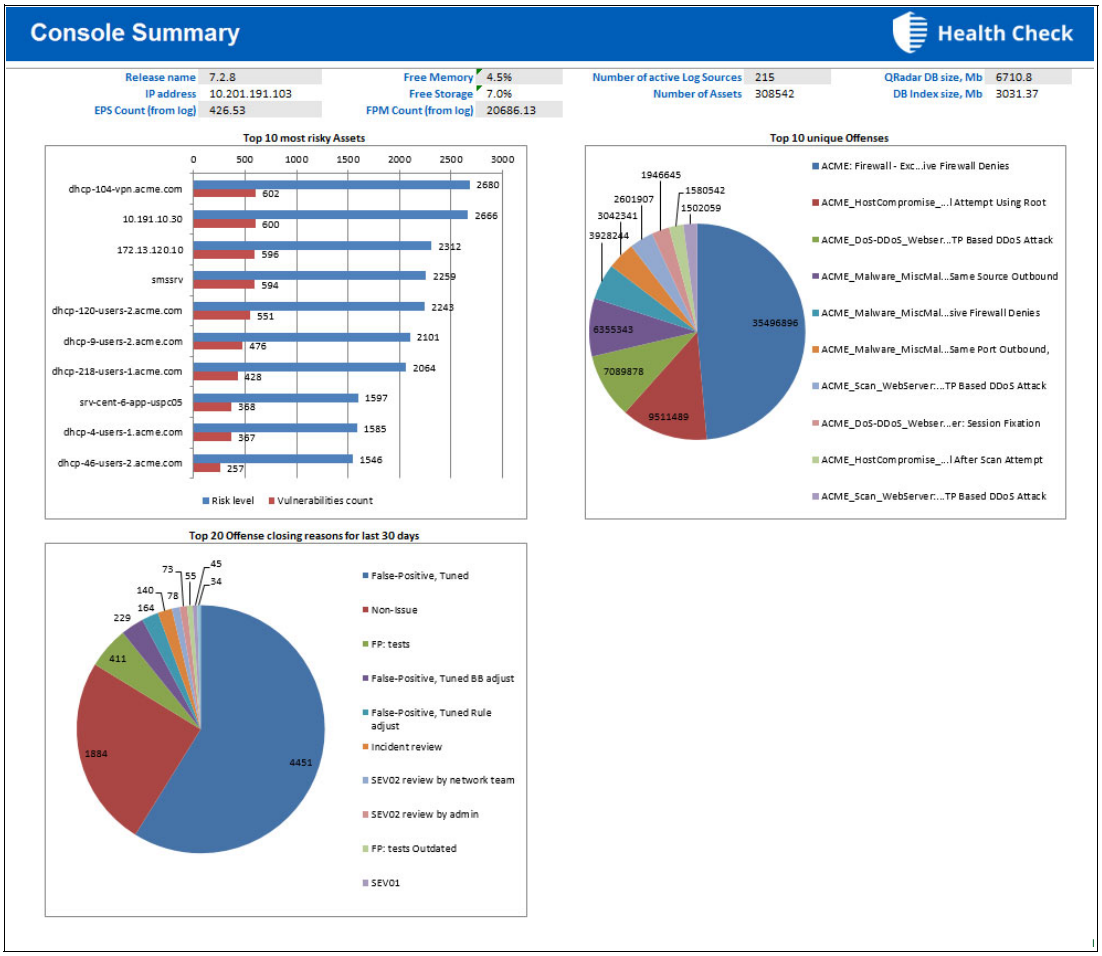


Figure 4-12 Heath Check, Console Summary

4.3.3 IBM QRadar Incident Forensics

IBM QRadar Incident Forensics (shown in Figure 4-13 on page 83) allows you to retrace the step-by-step actions of a potential attacker and then to quickly and easily conduct an in-depth forensics investigation of suspected malicious network security incidents. It reduces the time it takes for security teams to investigate QRadar offense records, in many cases from days to hours or even minutes. It can also help you to remediate a network security breach and to prevent it from happening again. IBM QRadar Packet Capture appliances are also available to store and manage data if no other network packet capture (PCAP) device is deployed.

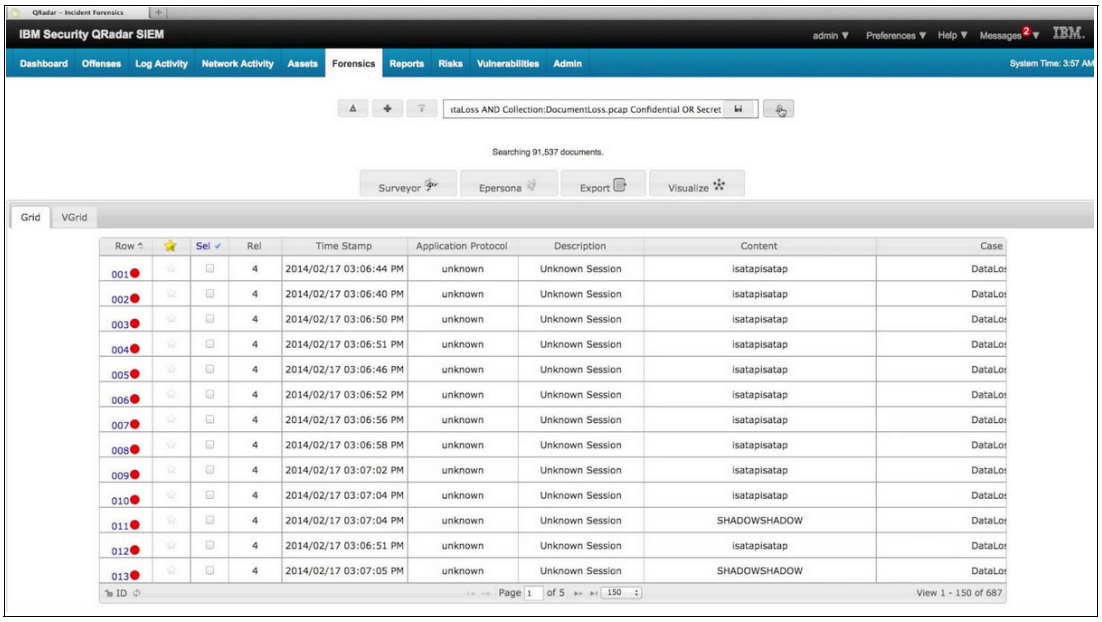


Figure 4-13 The Forensics tab

4.3.4 IBM QRadar Network Insights

IBM QRadar Network Insights (shown in Figure 4-14) analyzes network data in real time to uncover an attacker's footprints and to expose hidden security threats in many scenarios before they can damage the organization, including phishing e-mails, malware, data exfiltration, lateral movement, DNS, and other application abuse and compliance gaps. This features helps the security teams with the huge quantity of log activity that the company generate every day.

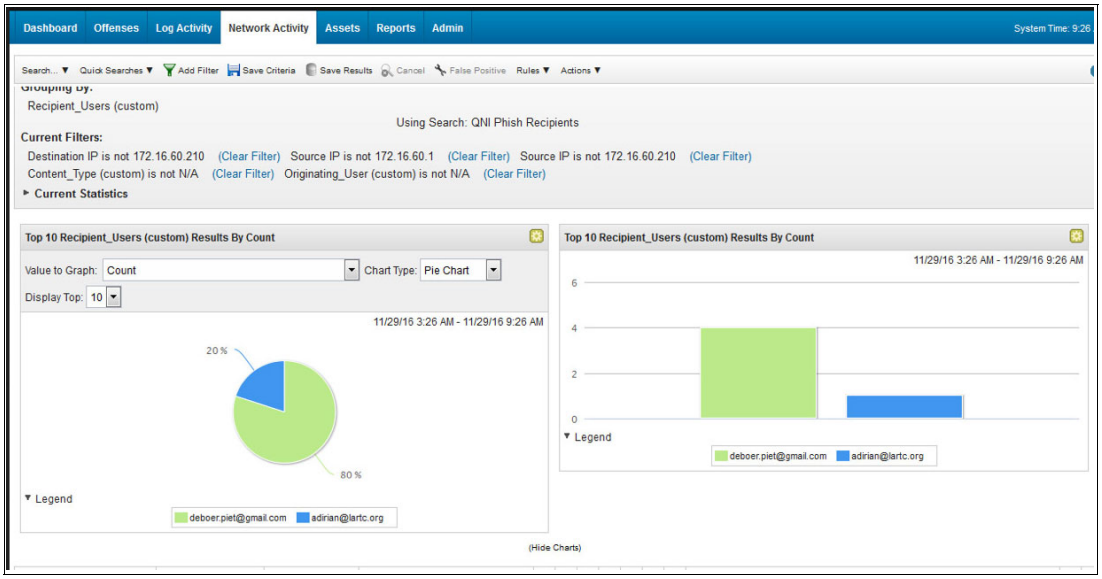


Figure 4-14 Network Activity tab

4.4 Upgrades and patching

As any other IT tool or application, you need to continually update QRadar so that it is adjusted for any new requirements. New features can be added through console upgrades, but also patching helps to fix any identified software bugs.

4.4.1 Preparing for the upgrade

To successfully upgrade an IBM Security QRadar system, verify the upgrade path when upgrading from older versions that require intermediate steps. The administrator must also review the software, hardware, and high availability requirements.

Is important to notice that when you upgrade to QRadar V7.2.6 or later that the SSH keys on every managed host are replaced. If you are connecting to or from a QRadar managed host and if you are using key-based authentication, *do not* remove or alter the SSH keys. Removing or altering the keys might disrupt communication between the QRadar Console and the managed hosts and can result in lost data. Consider to update the firmware on IBM Security QRadar appliances to take advantage of additional features and updates for the internal hardware components. You can find more information at IBM Support.

To ensure that IBM Security QRadar upgrades without errors, use only the supported versions of QRadar software V7.2.8 (20161118202122 and later). Check the software version in the software by clicking **Help** → **About**.

Memory and disk space requirements

Before the upgrade, ensure that IBM Security QRadar meets the minimum or suggested memory and disk space requirements shown in Table 4-1. Also, if you plan to enable payload indexing, the system requires a minimum of 24 GB of memory. However, 48 GB of memory is suggested. If you install QRadar software on your own hardware, your system requires a minimum of 24 GB of memory. Also before you upgrade to QRadar V7.3.0, ensure that the total size of the primary disk is at least 130 gigabytes (GB).

Table 4-1 Upgrade path

Appliance	Minimum memory requirement	Suggested memory requirement
QFlow Collector 1201	6 GB	6 GB
QFlow Collector 1202	6 GB	6 GB
QFlow Collector Virtual 1299 without QRadar Vulnerability Scanner	2 GB	2 GB
QFlow Collector Virtual 1299 with QRadar Vulnerability Scanner	6 GB	6 GB
QFlow Collector 1301	6 GB	6 GB
QFlow Collector 1310	6 GB	6 GB
QRadar Event Collector 1501	12 GB	16 GB
QRadar Event Collector Virtual 1599	12 GB	16 GB
QRadar Event Processor 1601	12 GB	48 GB
QRadar Event Processor 1605	12 GB	48 GB

Appliance	Minimum memory requirement	Suggested memory requirement
QRadar Event Processor 1624	64 GB	64 GB
QRadar Event Processor 1628	128 GB	128 GB
QRadar Event Processor Virtual 1699	12 GB	48 GB
QRadar Flow Processor 1701	12 GB	48 GB
QRadar Flow Processor 1705	12 GB	48 GB
QRadar Flow Processor 1724	64 GB	64 GB
QRadar Flow Processor 1728	128 GB	128 GB
QRadar Flow Processor Virtual 1799	12 GB	48 GB
QRadar Event and Flow Processor 1805	12 GB	48 GB
QRadar Event and Flow Processor 1824	64 GB	64 GB
QRadar Event and Flow Processor 1828	128 GB	128 GB
QRadar SIEM 2100	24 GB	24 GB
QRadar SIEM 2100 Light	24 GB	24 GB
QRadar SIEM 3100	24 GB	48 GB
QRadar SIEM 3105	24 GB	48 GB
QRadar SIEM 3124	64 GB	64 GB
QRadar SIEM 3128	128 GB	128 GB
QRadar SIEM Virtual 3199	24 GB	48 GB
QRadar xx48	128 GB	128 GB
QRadar Network Packet Capture	128 GB	128 GB
QRadar Network Insights	128 GB	128 GB
QRadar xx48	128 GB	128 GB
QRadar Log Manager 1605	12 GB	48 GB
QRadar Log Manager 1624	64 GB	64 GB
QRadar Log Manager 1628	128 GB	128 GB
QRadar Log Manager 2100	24 GB	24 GB
QRadar Log Manager 3105	24 GB	48 GB
QRadar Log Manager 3124	64 GB	64 GB
QRadar Log Manager 3128	128 GB	128 GB
QRadar Log Manager 3199	24 GB	48 GB

Backing up third-party data

Before the upgrade, be sure to back up all third-party data on the system. All third-party data on the system is removed during the OS upgrade portion of the QRadar upgrade. Only data stored in the /store partition is preserved. Back up the following data before performing the upgrade:

- Any third-party user accounts and data
- Any static route files for network interfaces
- Any files, scripts, or data in /root

Upgrade sequence in distributed deployments

When upgrading IBM Security QRadar systems, the administrator must complete the upgrade process on the QRadar Console first. You must be able to access the user interface on the desktop system before upgrading the secondary QRadar Console and managed hosts.

Upgrade QRadar systems in the following order:

1. Console
2. The following QRadar systems can be upgraded concurrently:
   - Event Processors
   - QRadar Event Collectors
   - Flow Processors
   - QFlow Collectors

Precautions for upgrading appliances

Follow these precautions before upgrading QRadar appliances:

- Back up the data, and confirm that backups are complete before you begin the upgrade.
- Ensure either that you have a QRadar Console connected to the hardware or that you have a remote connection to the management port (often called an *out of band management setup*). This connection is important because if a problem is detected while reinstalling RHEL the administrator needs to access the server through one of these connections.
- Ensure that the appliance is updated with the most recent BIOS or UEFI firmware version.
- Upgrade all managed hosts before deploying changes.
- To avoid access errors in the log file, close all open QRadar sessions.
- Confirm that the appliance meets the minimum requirements for QRadar.
- Disconnect high availability hosts before the upgrade if the entire /store directory is mounted on offboard storage.
- Ensure that the following order of mount points in the /etc/fstab file matches on both the primary and secondary HA hosts:
  - /store
  - /store/tmp
  - /store/transient
  - Any subdirectory of /store if the partition is mounted on offboard storage

  Restart the system after any updates to the /etc/fstab file.
- If the entire /store directory is mounted on offboard storage, run the following command to prepare the system for the upgrade:

  ```
  /media/cdrom/post/prepare_offboard_storage_upgrade.sh
  ```

- If you are not prompted to remount your offboard storage solution during the upgrade, remount the storage when the upgrade finishes.
- Before you upgrade to QRadar V7.3.0, ensure that the QRadar Console doesn't have a QRadar Incident Forensics license allocated to it. Upgrading a QRadar Console that uses a QRadar Incident Forensics license might cause the shared license pool to become over-allocated and can prevent you from using some features on the Log Activity and Network Activity tabs. To avoid this issue, remove the QRadar Incident Forensics license and re-add it after the upgrade completes.

4.4.2 Upgrading QRadar appliances

Before you upgrade QRadar, ensure that you take the following appropriated precautions:

- Ensure that you have sufficient RAM according to the product specification.
- Back up all your data, and confirm that backups are complete before you begin the upgrade.
- Disconnect your offboard storage (if your deployment includes offboard storage solutions).
- Close all open QRadar product sessions to avoid access errors in your log file.

During the upgrade, a system pretest checks that the minimum amount of RAM is available. If there is not enough RAM, the upgrade stops.

After you complete the upgrade, you can remount your external storage solutions

Procedure

The first time that you run the patch installer script, there is expected delay before the first patch installer menu displays.

Remember that If the SSH session is disconnected while the upgrade is in progress, the upgrade continues. When you reopen your SSH session and rerun the installer, the installation resumes.

To upgrade QRadar, complete these steps:

1. If you are not on QRadar V7.2.8.1 or later, complete the following steps to update to the minimum QRadar software version patch that is required for the QRadar V7.3.0 upgrade. Otherwise, skip to step 2.
   a. Download the `<QRadar_patchupdate>.sfs` file from IBM Fix Central.
   b. Use SSH to log in to your system as the root user.
   c. Copy the patch file to the `/tmp` directory or to another location that has sufficient disk space. Is import to remember not to copy the file to an existing QRadar system directory, such as `/store` or `/root`.
   d. Create the `/media/updates` directory by entering the following command:

      ```
      mkdir -p /media/updates
      ```

   e. Change to the directory where you copied the patch file.
   f. Mount the patch file to the `/media/updates` directory by entering the following command:

      ```
      mount -o loop -t squashfs <QRadar_patchupdate>.sfs /media/updates/
      ```

   g. Run the patch installer by entering the following command:

      ```
      /media/updates/installer
      ```

h. Provide answers to the pre-patch questions based on your QRadar deployment.

i. Apply the software fix to all systems in the deployment using the patch installer.

The patch installer menu lists the following options:

- Console
- All

If you select **Console**, the software fix is applied only to the QRadar Console. If you select **All**, the software fix is applied to the QRadar Console first, and then to all managed hosts. After the software fix is applied to the QRadar Console, the menu lists the remaining managed hosts and the **All** option.

j. After the upgrade is complete, unmount the software update by using the following command:

```
umount /media/updates
```

k. Finally, complete an automatic update to ensure that your configuration files include the latest network security information.

2. To upgrade, download the `<QRadar>.iso` file from IBM Fix Central.

a. Use SSH to log in to your system as the root user.

b. Copy the ISO file to the `/tmp` directory or to another location that has sufficient disk space. Is important to remember to avoid copy the file to an existing QRadar system directory, such as `/store` or `/root`.

c. Create the `/media/cdrom` directory by entering the following command:

```
mkdir -p /media/cdrom
```

d. Change to the directory where you copied the ISO file.

e. Mount the ISO file to the `/media/cdrom` directory by entering the following command:

```
mount -o loop <QRadar>.iso /media/cdrom/
```

f. Pretest the installation by entering the following command:

```
/media/cdrom/setup –t
```

g. Review the pretest output and, if your deployment fails any pretests, take any of the suggested actions.

h. Run the installer by entering the following command:

```
/media/cdrom/setup
```

The SSH connection pauses for 20 minutes because the system restarts. Monitor the console screen to confirm when the SSH becomes available after the system restart.

i. Complete an automatic update to ensure that your configuration files include the latest network security information.

j. Clear your web browser cache. After you upgrade QRadar, the Vulnerabilities tab might not display. To use QRadar Vulnerability Manager after you upgrade, you must upload and allocate a valid license key.

4.4.3 Upgrading QRadar software installations

Upgrade IBM Security QRadar V7.2.8 to V7.3.0 on your own appliance with a QRadar software installation. A software installation includes custom Red Hat Enterprise Linux partitions that are already configured.

Upgrading the QRadar Console to V7.3.0 can take approximately 3 hours. Upgrading managed hosts can take approximately 1:30 hours. If you experience extended upgrade times, contact IBM Support to review the progress of the upgrade.

The administrator must have the QRadar v7.2.8 -QRFULL- 20161118202122 fix pack and later installed before you can upgrade to QRadar V7.3.0. Click **Help** → **About** to view the QRadar version, and download the software fix from IBM Fix Central.

The administrator must complete the following tasks to upgrade QRadar with customer Red Hat Enterprise Linux partitions:

1. Copy the required files to the appliance and start the upgrade.
2. Install Red Hat Enterprise Linux V7.3 and configure partitions.
3. Follow the installation wizard to complete the QRadar installation.

Copying the required files

Copy the files to the host where you want to upgrade IBM Security QRadar, and begin the setup process.

Before you begin

Before you begin the installation, ensure that you have completed the following actions:

- Download the QRadar release ISO file from IBM Fix Central.
- Obtain the Red Hat Enterprise Linux V7.3 ISO.
- Confirm that your appliance meets the minimum requirements for QRadar
- Upgrade all managed hosts before you deploy changes.
- Disconnect HA hosts before the upgrade if the entire `/store` directory is mounted on offboard storage.
- Ensure that the order of mount points in the `/etc/fstab` file matches on both the primary and secondary HA host:
  - `/store`
  - `/store/tmp`
  - `/store/transient`

  Any subdirectory of `/store` if the partition is mounted on offboard storage.
- Restart the system after any updates to the `/etc/fstab` file.
- Run the following command to prepare the system for the upgrade, if the entire `/store` directory is mounted on offboard storage:

  ```
  /media/cdrom/post/prepare_offboard_storage_upgrade.sh
  ```
- If you are not prompted to remount your offboard storage solution during the upgrade, remount the storage when the upgrade finishes.

Procedure

To upgrade QRadar with customer Red Hat Enterprise Linux partitions, complete the following steps:

1. Copy the Red Hat Enterprise Linux operating system DVD ISO to one of the following portable storage devices:
   - Digital Versatile Disk (DVD)
   - Bootable USB flash drive

2. Using a Secure File Transfer Protocol (SFTP) program, such as WinSCP, copy the QRadar ISO to the host where you want to install QRadar.
3. Use SSH to log in to the system as the root user.
4. Create the installation directory by typing the following command:

   ```
   mkdir -p /media/cdrom
   ```

5. Mount the QRadar ISO by entering the following command:

   ```
   mount -o loop <QRadar_ISO> /media/cdrom
   ```

6. Start the QRadar setup by entering the following command:

   ```
   /media/cdrom/setup
   ```

4.4.4 Installing Red Hat Enterprise Linux V7.3 and configuring partitions

When you initiate an IBM Security QRadar upgrade on a host that has custom Red Hat Enterprise Linux partitions configured, a message appears stating that a Red Hat Enterprise Linux Software Installation exists. Copy the recommendations for sizing your existing partitions for Red Hat Enterprise Linux V7.3 to use later in the procedure.

Procedure

To install Red Hat Enterprise Linux and configure partitions, follow these steps:

1. Insert the portable storage device into your appliance and restart your appliance.
2. From the starting menu, select one of the following options:
   - Select the USB or DVD drive as the boot option.
   - To install on a system that supports Extensible Firmware Interface (EFI), the administrator must start the system in *legacy* mode.
3. Follow the instructions in the wizard to begin the installation:
   a. Select the language.
   b. Click **Date & Time** and set the time for your deployment.
   c. Click **Installation Destination**, select the “I will configure partitioning” option, and then click **Done**.
4. Adjust the partition sizes according to the recommendations for the deployment that is listed in the installation window. The following steps are an example of adjusting partition sizes to upgrade a deployment with a /root partition that is 20,000 MB.

   In the Red Hat Enterprise Linux Server Linux V6.8 for x86_64 section, modify the following partitions:

   a. Select **Swap**, and select the **Reformat** option.
   b. Select `/store`, and enter `/store` in the Mount Point field.

      This option is not available in HA deployments.
   c. Select `/storetmp`, and enter `/storetmp` in the Mount Point field.
   d. Select `/transient`, and enter `/transient` in the Mount Point field.
   e. Select `/boot`, and enter the new value of `/bootold` in the Mount Point field.
   f. Delete /.

In the New Red Hat Linux Enterprise V7.X Installation section, click **+** to create the new Red Hat Linux Enterprise V7.3 partitions:

Important: Click **Update Settings** after you create each partition.

a. Create a /boot mount point that is 1024 MB in size, with XFS for a file system, and Standard Partition for the device type.

b. Create a / mount point that is 6672 MB in size, with XFS for a file system, and LVM for the device type.

c. With the / partition still selected, click **Modify** under the Volume Group button to create a rootrhel volume group, and select **Size Policy** → **As large as possible**.

d. Create a /var mount point that is 2594 MB in size, with XFS for a file system, and LVM for the device type. Ensure that rootrhel is selected for the Volume Group.

e. Create a /opt mount point that is 6672 MB in size, with XFS for a file system, and LVM for the device type. Ensure that rootrhel is selected for the Volume Group.

f. Create a /tmp mount point that is 1482 MB in size, with XFS for a file system, and LVM for the device type. Ensure that rootrhel is selected for the Volume Group.

g. Create a /home mount point that is 370 MB in size, with XFS for a file system, and LVM for the device type. Ensure that rootrhel is selected for the Volume Group.

h. Delete the /var/log partition in the Red Hat Enterprise Linux Server V6.8 for x86_64 section.

Note: Do *not* select the “Delete all other file systems in the Red Hat Enterprise Linux Server Linux V6.8 for x86_64 root as well” option.

i. Create a new /var/log mount point that is 8063 MB in size, with XFS for a file system, and LVM for the device type.

j. With the /var/log partition still selected, click **Modify** under the Volume Group button to create a varlogrhel volume group, and select **Size Policy** → **As large as possible**.

k. Create a /var/log/audit mount point that is 1651 MB in size, with XFS for a file system, and LVM for the device type. Ensure that varlogrhel is selected for the Volume Group.

l. Delete the /bootold partition in the Red Hat Enterprise Linux Server Linux.

m. For the V6.8 for x86_64 section, only three partitions are now listed for Red Hat Enterprise Linux V6.8:

- /store
- /storetmp
- /transient

5. Click **Done** on the Manual Partitioning window.

6. Follow the instructions in the wizard to complete the installation:

a. Click **Network & Host Name**.

b. Enter the host name for your appliance.

c. Select the interface in the list, move the switch to the ON position, and click **Configure**.

d. On the General tab, select the “Automatically connect to this network when it is available” option.

e. On the IPv4 Settings tab, in the Method list, select **Manual**.

f. Click **Add** to enter the IP address, netmask, and gateway for the appliance in the Addresses field.

g. Add two DNS servers.

h. Click **Save**, click **Done**, and then click **Begin Installation**.

7. Set the root password, and then click **Finish Configuration**.
8. Restart the host after the Red Hat Enterprise Linux V7.3 installation finishes.

4.4.5 Completing the QRadar installation

After you configure Red Hat Enterprise Linux V7.3, complete the IBM Security QRadar installation by preparing for the QRadar installation wizard:

1. Use SSH to log in to the system as a root user.
2. Modify the `SELINUX` value in the `/etc/sysconfig/selinux` file to `SELINUX=disabled`, and restart the host.
3. Use SSH to log back in to the system as the root user.
4. Confirm that the `/store` partition is not mounted by typing the following command:

   ```
   mount
   ```

   If the `/store` partition is mounted, unmount the partition by typing the following command:

   ```
   umount /store
   ```

5. Confirm that the `/storetmp` partition is mounted by typing the following command:

   ```
   mount /storetmp
   ```

6. Create the `/media/cdrom` directory by typing the following command:

   ```
   mkdir -p /media/cdrom
   ```

7. Mount the QRadar ISO by typing the following command:

   ```
   mount /storetmp/730/<QRadar_ISO_name> /media/cdrom
   ```

8. Type the following command to begin the QRadar upgrade:

   ```
   /media/cdrom/setup
   ```

9. After the installation finishes, clear your browser cache.

4.5 Health checks, monitoring tools

QRadar capabilities include monitoring features to view specific network activities. The next sections provide a brief description of these features that can be used by the administrator for a deeper understanding of network behavior.

4.5.1 QRadar basic procedures

Various controls on the QRadar user interface are common to most user interface tabs. Some information about these common procedures is described in the following sections.

Viewing messages

The Messages menu, which is on the upper, right corner of the user interface, provides access to a window in which you can read and manage your system notifications.

For system notifications to show on the Messages window, the administrator must create a rule that is based on each notification message type and select the Notify check box in the Custom Rules Wizard. The Messages menu indicates how many unread system notifications you have in your system.

Refreshing and pausing the user interface

The administrator can manually refresh, pause, and play the data that is displayed on tabs. Dashboard tab.

The Dashboard tab automatically refreshes every 60 seconds. The timer, which is on the upper, right corner of the interface, indicates the amount of time that remains until the tab is automatically refreshed. Click the title bar of any dashboard item to automatically pause the refresh time. The timer flashes red to indicate that the current display is paused.

Log Activity and Network Activity tabs

The Log Activity and Network Activity tabs automatically refresh every 60 seconds if the administrator is viewing the tab in Last Interval (auto refresh) mode. When the administrator view the Log Activity or Network Activity tab in Real Time (streaming) or Last Minute (auto refresh) mode, he can use the Pause icon to pause the current display.

Offenses tab

The Offenses tab must be refreshed manually. The timer, which is on the upper, right corner of the interface, indicates the amount of time since the data was last refreshed. The timer flashes red when the timer is paused.

4.5.2 Investigating IP addresses

You can use several methods to investigate information about IP addresses on the Dashboard, Log Activity, and Network Activity tabs. To investigate IP addresses:

1. Log in to QRadar.
2. Go to the tab that you want to view.
3. Move your mouse pointer over an IP address to view the location of the IP address.
4. Right-click the IP address or asset name and select one of the options shown in Table 4-2.

Table 4-2 Options for investigating IP addresses

Option	Description
Navigate → View by Network	Displays the networks that are associated with the selected IP address.
Navigate → View Source Summary	Displays the offenses that are associated with the selected source IP address.
Navigate → View Destination Summary	Displays the offenses that are associated with the selected destination IP address.
Information → DNS Lookup	Searches for DNS entries that are based on the IP address.
Information → WHOIS Lookup	Searches for the registered owner of a remote IP address. The default WHOIS server is whois.arin.net.

Option	Description
Information → Port Scan	Performs a Network Mapper (NMAP) scan of the selected IP address. This option is only available if NMAP is installed on your system. For more information about installing NMAP, see your vendor documentation.
Information → Asset Profile	Displays asset profile information. This option is displayed if IBM Security QRadar Vulnerability Manager is purchased and licensed. This menu option is available if QRadar acquired profile data either actively through a scan or passively through flow sources.
Information → Search Events	Searches for events that are associated with this IP address.
Information → Search Flows	Searches for flows that are associated with this IP address.
Information → Search Connections	Searches for connections that are associated with this IP address. This option is only displayed if you purchased IBM Security QRadar Risk Manager and connected QRadar and the IBM Security QRadar Risk Manager appliance.
Information → Switch Port Lookup	Determines the switch port on a Cisco IOS device for this IP address. This option applies only to switches that are discovered by using the Discover Devices option on the Risks tab. Note: This menu option isn't available in QRadar Log Manager.
Information → View Topology	Displays the Risks tab, which depicts the layer 3 topology of your network. This option is available if you purchased IBM Security QRadar Risk Manager and connected QRadar and the IBM Security QRadar Risk Manager appliance.
Run Vulnerability Scan	Select the Run Vulnerability Scan option to scan an IBM Security QRadar Vulnerability Manager scan on this IP address. This option is only displayed when IBM Security QRadar Vulnerability Manager has been purchased and licensed.

4.5.3 Investigate user names

You can right-click a user name to access more menu options. Use these options to view more information about the user name or the IP address. Also, you can investigate user names when IBM Security QRadar Vulnerability Manager is purchased and licensed. When you right-click a user name, you can choose from the menu options shown in Table 4-3.

Table 4-3 Options for investigating user names

Option	Description
View Assets	Displays current assets that are associated to the selected user name.
View User History	Displays all assets that are associated to the selected user name over the previous 24 hours.
View Events	Displays the events that are associated to the selected user name.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

Other publications

These publications are also relevant as further information sources:

- Gartner. (2017). *IT Glossary*. Retrieved from Gartner:

  http://www.gartner.com/it-glossary/security-information-and-event-management-siem/

- Piggeé, J. (2016, Jan 10). *What is SIEM*. Retrieved from Tripwire:

  https://www.tripwire.com/state-of-security/incident-detection/log-management-siem/what-is-a-siem/

- Rouse, M. (2014). *security information and event management (SIEM)*. Retrieved from Tech Target:

  http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

- IBM. (2016, November 06). *QRadar: Reaching data storage limits*. Retrieved from IBM Support:

  http://www.ibm.com/support/docview.wss?uid=swg21993774

- IBM. (2017). *Data Nodes and data storage*. Retrieved from IBM Knowledge Center:

  https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_deployment_guide_DN_SANs_deployment.html

- IBM. (2017). *Offboard storage overview*. Retrieved from IBM knowledge Center:

  https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.5/com.ibm.qradar.doc_7.2.5/c_offboard_overview.html

- IBM. (2017, February 27). *QRadar: Storage Performance Requirements*. Retrieved from IBM Support:

  http://www.ibm.com/support/docview.wss?uid=swg21993402

- IBM. (2017, February 27). *QRadar: Techniques to Reduce Used Storage*. Retrieved from IBM Support:

  http://www.ibm.com/support/docview.wss?uid=swg21993401

- IBM. (2017, March 9). *QRadar: the Impacts of Storage Hardware Speed*. Retrieved from IBM Support:

  http://www.ibm.com/support/docview.wss?uid=swg21993400

- IBM. (2017). *Upgrading QRadar products*. Retrieved from IBM Knowledge Center:

  https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.7/com.ibm.qradar.doc/t_qradar_up_ugrad_sys.html

- IBM. (2017). *IBM Security QRadar SIEM V7.3.0 Product Documentation*. Retrieved from IBM Support:

  http://www.ibm.com/support/docview.wss?uid=swg27049537

- IBM. (2017). *Optimizing IBM QRadar Advisor with Watson*. Retrieved from IBM Support:

  http://www.ibm.com/support/docview.wss?uid=swg27049804&aid=1

- IBM. (2017). *IBM Security QRadar SIEM Fine-tuning for a Top 30 US Bank*. Retrieved from:

  https://www.scnsoft.com/case-studies/ibm-security-qradar-siem-fine-tuning-for-a-top-30-us-bank

- ScienceSoft. (2017). *Health Check Framework for IBM QRadar SIEM*. Retrieved from:

  https://www.scnsoft.com/services/security-intelligence-services/health-check-framework-for-ibm-qradar-siem#HCF-form

- IBM. (2015). *5 Ways to Get Even More from Your IBM Security QRadar Investment in 2016*. Retrieved from:

  https://www.slideshare.net/fgonza93/5-ways-to-get-even-more-from-your-ibm-security-qradar-investment-in-2016-57426851

- IBM. (2017). *Deployment Monitoring*. Retrieved from IBM Support:

  https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.7/com.ibm.qradar.doc/c_master_console_overview.html

- IBM. (2017). *Health Check Framework for IBM QRadar*. Retrieved from:

  https://exchange.xforce.ibmcloud.com/hub/extension/ScienceSoftCorporation:HealthCheckFrameworkManager

- IBM. (2017). *IBM QRadar Operations*. Retrieved from:

  https://exchange.xforce.ibmcloud.com/hub/extension/d35eae95160f59d79ca71683e2c72448

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Redbooks

IBM QRadar Version 7.3: Planning and Installation Guide

(0.2”spine)
0.17”<->0.473”
90<->249 pages

SG24-8412-00

ISBN 0738442879

Printed in U.S.A.