IBM QRadar
7.4.3

Installation Guide

Note

Before you use this information and the product that it supports, read the information in “Notices” on page 135.

© Copyright International Business Machines Corporation 2004, 2021.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Introduction to QRadar installations

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

Thank you for ordering your appliance from IBM! It is strongly recommended that you apply the latest maintenance to you appliance for the best results. Please visit IBM Fix Central (http://www.ibm.com/support/fixcentral) to determine the latest recommended patch for your product.

To install or recover a high-availability (HA) system, see the *IBM QRadar High Availability Guide*.

Intended audience

Network administrators who are responsible for installing and configuring QRadar systems must be familiar with network security concepts and the Linux operating system.

Technical documentation

To find IBM QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM QRadar.

© Copyright IBM Corp. 2004, 2021

Chapter 1. QRadar deployment overview

You can install IBM QRadar on a single server for small enterprises, or across multiple servers for large enterprise environments.

For maximum performance and scalability, you must install a high-availability (HA) managed host appliance for each system that requires HA protection. For more information about installing or recovering an HA system, see the *IBM QRadar High Availability Guide*.

License keys

After you install IBM QRadar, you must apply your license keys.

Your system includes a temporary license key that provides you with access to QRadar software for five weeks. After you install the software and before the default license key expires, you must add your purchased licenses.

The following table describes the restrictions for the default license key:

Table 1. Restrictions for the default license key for QRadar SIEM installations

Usage	**Limit**
Events per second threshold **Important:** This restriction also applies to the default license key for IBM QRadar Log Manager.	5000
Flows per interval	200000

When you purchase a QRadar product, an email that contains your permanent license key is sent from IBM. These license keys extend the capabilities of your appliance type and define your system operating parameters. You must apply your license keys before your default license expires.

Related tasks

Installing a QRadar appliance

Installing RHEL on your system

You can install the Red Hat Enterprise Linux (RHEL) operating system on your system to use with IBM QRadar.

Installing QRadar on a virtual machine

After you create your virtual machine, you must install the IBM QRadar software on the virtual machine.

Integrated Management Module

Use Integrated Management Module, which is on the back panel of each M4 and M5 appliance, for remote management of the hardware and operating systems, independent of the status of the managed server. For information about the Lenovo M6 appliance management controller for systems-management functions, see “Management controller” on page 2.

You can configure Integrated Management Module to share an Ethernet port with the IBM QRadar product management interface. However, to reduce the risk of losing the connection when the appliance is restarted, configure Integrated Management Module in dedicated mode.

To configure Integrated Management Module, you must access the system BIOS settings by pressing F1 when the IBM splash screen is displayed. For more information about configuring Integrated Management Module, see *Integrated Management Module User's Guide* on the CD that is shipped with your appliance.

© Copyright IBM Corp. 2004, 2021

Related concepts

Prerequisite hardware accessories for QRadar installations
Before you install IBM QRadar products, ensure that you have access to the required hardware accessories and desktop software.

Management controller

The IBM QRadar appliances use a management controller for systems-management functions.

IBM QRadar appliances contain an integrated service processor, which provides advanced service-processor control, monitoring, and alerting functions and consolidates the service processor functionality, super I/O, video controller, and remote presence capabilities into a single chip on the server system board.

For more information about the Lenovo management controller, see Lenovo XClarity Controller(https://sysmgt.lenovofiles.com/help/index.jsp?topic=%2Fcom.lenovo.systems.management.xcc.doc%2Fdw1lm_c_ch1_introduction.html).

For more information about the Dell management controller, see Dell iDRAC Controller (https://www.delltechnologies.com/en-us/solutions/openmanage/idrac.htm).

For instructions on how to configure the Lenovo management controller, see XClarity Controller User Guide (https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/xcc_book.pdf.

For instructions on how to configure the Dell management controller, see iDRAC Controller User Guide (https://www.dell.com/support/article/en-ca/sln306877/dell-poweredge-how-to-configure-the-idrac9-and-the-lifecycle-controller-network-ip?lang=en).

Prerequisite hardware accessories for QRadar installations

Before you install IBM QRadar products, ensure that you have access to the required hardware accessories and desktop software.

Hardware accessories

Ensure that you have access to the following hardware components:

- Monitor and keyboard, or a serial console
- Uninterrupted Power Supply (UPS) for all systems that store data, such as QRadar Console, Event Processor components, or QRadar QFlow Collector components
- Null modem cable if you want to connect the system to a serial console

Important: QRadar products support hardware-based Redundant Array of Independent Disks (RAID) implementations, but do not support software-based RAID installations or hardware assisted RAID installations.

Related tasks

Installing a QRadar appliance

Installing RHEL on your system
You can install the Red Hat Enterprise Linux (RHEL) operating system on your system to use with IBM QRadar.

Installing QRadar on a virtual machine

After you create your virtual machine, you must install the IBM QRadar software on the virtual machine.

Environmental restrictions

QRadar performance can be affected by other devices in your deployment.

For any DNS server that you point a QRadar appliance to, you cannot have a DNS registry entry with the hostname set to `localhost`.

Supported web browsers

For the features in IBM QRadar products to work properly, you must use a supported web browser.

The following table lists the supported versions of web browsers.

Table 2. Supported web browsers for QRadar products

Web browser	Supported versions
64-bit Mozilla Firefox	60 Extended Support Release and later
64-bit Microsoft Edge	38.14393 and later
64-bit Google Chrome	Latest

The Microsoft Internet Explorer web browser is no longer supported on QRadar 7.4.0 or later.

Security exceptions and certificates

If you are using the Mozilla Firefox web browser, you must add an exception to Mozilla Firefox to log in to QRadar. For more information, see your Mozilla Firefox web browser documentation.

Navigate the web-based application

When you use QRadar, use the navigation options available in the QRadar Console instead of your web browser **Back** button.

Firmware update

Update the firmware on IBM QRadar appliances to take advantage of additional features and updates for the internal hardware components.

For more information about updating firmware, see Firmware update for QRadar (http://www-01.ibm.com/support/docview.wss?uid=swg27047121).

Bandwidth for managed hosts

To replicate state and configuration data, ensure that you have a minimum bandwidth of 100 Mbps between the IBM QRadar console and all managed hosts. Higher bandwidth is necessary when you search log and network activity, and you have over 10,000 events per second (EPS).

An Event Collector that is configured to store and forward data to an Event Processor forwards the data according to the schedule that you set. Ensure that you have sufficient bandwidth to cover the amount of data that is collected, otherwise the forwarding appliance cannot maintain the scheduled pace.

Use the following methods to mitigate bandwidth limitations between data centers:

Process and send data to hosts at the primary data center

Design your deployment to process and send data as it's collected to hosts at the primary data center where the console resides. In this design, all user-based searches query the data from the local data center rather than waiting for remote sites to send back data.

You can deploy a store and forward event collector, such as a QRadar 15XX physical or virtual appliance, in the remote locations to control bursts of data across the network. Bandwidth is used in the remote locations, and searches for data occur at the primary data center, rather than at a remote location.

Don't run data-intensive searches over limited bandwidth connections

Ensure that users don't run data-intensive searches over links that have limited bandwidth. Specifying precise filters on the search limits the amount of data that is retrieved from the remote locations, and reduces the bandwidth that is required to send the query result back.

For more information about deploying managed hosts and components after installation, see the *IBM QRadar Administration Guide*.

USB flash drive installations

You can install IBM QRadar software with a USB flash drive.

USB flash drive installations are full product installations. You cannot use a USB flash drive to upgrade or apply product patches. For information about applying fix packs, see the fix pack Release Notes.

Supported versions

The following appliances or operating systems can be used to create a bootable USB flash drive:

- A Linux system that is installed with Red Hat Enterprise Linux V7.7
- Apple Mac OS X
- Microsoft Windows

Installation overview

Follow this procedure to install QRadar software from a USB flash drive:

1. Create the bootable USB flash drive.
2. Install the software for your QRadar appliance.
3. Install any product maintenance releases or fix packs.

   See the Release Notes for installation instructions for fix packs and maintenance releases.

Creating a bootable USB flash drive with a Windows system

Use the Fedora® Media Writer app on a Windows system to create a bootable USB flash drive that you can use to install IBM QRadar software.

Before you begin

You must have access to an 8 GB or larger USB flash drive.

Important: Ensure that you load only the QRadar ISO image file on the bootable USB flash drive.

Procedure

1. On your Windows system, download and install the Fedora Media Writer app from the Fedora Media Writer GitHub repository (https://github.com/FedoraQt/MediaWriter/releases).

   Other media creation tools might work to create the bootable flash drive, but the QRadar ISO is a modified Red Hat ISO, and Red Hat suggests Fedora Media Writer. For more information, see Making

Installation USB Media (https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/installation_guide/sect-making-usb-media).

2. On your Windows system, download the QRadar ISO image file from Fix Central (www.ibm.com/support/fixcentral/) to a local drive.
3. Insert the USB flash drive into a USB port on your Windows system.

   Important: Any files stored on the USB flash drive are overwritten when creating the bootable flash drive.
4. Open Fedora Media Writer and in the main window, click **Custom Image**.
5. Browse to where you downloaded the QRadar ISO on your Windows system and select it.
6. Select the USB flash drive from the Fedora Media Writer menu, and then click **Write to disk**.
7. When the writing process is complete, click **Close** and remove the USB flash drive from your system.

What to do next

See Installing QRadar with a USB flash drive.

Creating a bootable USB flash drive on a Apple Mac OS X system

You can use an Apple Mac OS X computer to create a bootable USB flash drive that you can use to install QRadar software.

Before you begin

You must have access to the following items:

- An 8 GB or larger USB flash drive
- A QRadar V7.3.1 or later ISO image file

About this task

When you create a bootable USB flash drive, the contents of the flash drive are deleted.

Procedure

1. Download the QRadar ISO image file from Fix Central (www.ibm.com/support/fixcentral/).
2. Insert the USB flash drive into a USB port on your system.
3. Open a terminal and type the following command to unmount the USB flash drive:

   ```
   diskutil unmountDisk /dev/<name_of_the_connected_USB_flash_drive>
   ```
4. Type the following command to write the QRadar ISO to your USB flash drive:

   ```
   dd if=/<qradar>.iso of=/dev/r<name_of_the_connected_USB_flash_drive> bs=1m
   ```

   Note: The "r" before the name of the connected USB flash drive is for raw mode, which makes the transfer much faster. There is no space between the "r" and the name of the connected USB flash drive.
5. Remove the USB flash drive from your system.

What to do next

See Installing QRadar with a USB flash drive.

Creating a bootable USB flash drive with Red Hat Linux

You can use a desktop or notebook system with Red Hat Enterprise Linux V7 or higher to create a bootable USB flash drive that you can use to install QRadar software.

Before you begin

You must have access to the following items:

- An 8 GB or larger USB flash drive
- A QRadar 7.4.3 or later ISO image file

About this task

When you create a bootable USB flash drive, the contents of the flash drive are deleted.

Procedure

1. Download the QRadar ISO image file from Fix Central (www.ibm.com/support/fixcentral/).
2. Insert the USB flash drive into a USB port on your system.

   It might take up to 30 seconds for the system to recognize the USB flash drive.
3. Open a terminal and type the following command to determine the name of the USB flash drive:

   ```
   dmesg | grep SCSI
   ```

   The system outputs the messages produced by device drivers. The following example shows the name of the connected USB flash drive as *sdb*.

   ```
   [ 170.171135] sd 5:0:0:0: [sdb] Attached SCSI removable disk
   ```
4. Type the following commands to unmount the USB flash drive:

   ```
   df -h | grep <name_of_the_connected_USB_flash_drive>
   umount /dev/<name_of_the_connected_USB_flash_drive>
   ```

   Example:

   ```
   [root@m5qa04 ~]# dmesg | grep SCSI
   [93425.566934] sd 14:0:0:0: [sdb] Attached SCSI removable disk
   [root@m5qa04 ~]# df -h | grep sdb
   [root@m5qa04 ~]# umount /dev/sdb
   umount: /dev/sdb: not mounted
   ```
5. Type the following command to write the QRadar ISO to your USB flash drive:

   ```
   dd if=/<qradar>.iso of=/dev/<name_of_the_connected_USB_flash_drive> bs=512k
   ```

   Example:

   ```
   [root@m5qa04 ~]# dd if=Rhe764QRadar2021_2_0_20201215210530.iso of=/dev/sdb bs=512k
   11112+0 records in
   11112+0 records out
   5825888256 bytes (5.8 GB) copied, 1085.26 s, 5.4 MB/s
   ```
6. Remove the USB flash drive from your system.

What to do next

See "Installing QRadar with a USB flash drive" on page 6.

Installing QRadar with a USB flash drive

Follow this procedure to install QRadar from a bootable USB flash drive.

Before you begin

You must create the bootable USB flash drive before you can use it to install QRadar software.

About this task

This procedure provides general guidance on how to use a bootable USB flash drive to install QRadar software.

The complete installation process is documented in the product Installation Guide.

Procedure

1. Install all necessary hardware.
2. Choose one of the following options:
   - Connect a notebook to the serial port at the back of the appliance.
   - Connect a keyboard and monitor to their respective ports.
3. Insert the bootable USB flash drive into the USB port of your appliance.
4. Restart the appliance.

   Most appliances can boot from a USB flash drive by default. If you are installing QRadar software on your own hardware, you might have to set the device boot order to prioritize USB. However, if the boot order is set to USB and then hard drive, the USB drive must be removed when the first reboot starts to avoid a loop condition. Setting the boot order to hard drive then USB will avoid the loop condition.

   After the appliance starts, the USB flash drive prepares the appliance for installation. This process can take up to an hour to complete.
5. When the **Red Hat Enterprise Linux** menu is displayed, select one of the following options:

   For QRadar 7.4.1, 7.4.2, and 7.4.3.
   - If you connected a keyboard and monitor, select **Install Red Hat Enterprise Linux 7.7**.
   - If you connected a notebook with a serial connection, select **Install Red Hat Enterprise Linux 7.7 using Serial console without format prompt** or **Install Red Hat Enterprise Linux 7.7 using Serial console with format prompt**.

   For QRadar 7.4.0
   - If you connected a keyboard and monitor, select **Install Red Hat Enterprise Linux 7.6**.
   - If you connected a notebook with a serial connection, select **Install Red Hat Enterprise Linux 7.6 using Serial console without format prompt** or **Install Red Hat Enterprise Linux 7.6 using Serial console with format prompt**.
6. Type SETUP to begin the installation.
7. When the login prompt is displayed, type `root` to log in to the system as the root user.

   The user name is case-sensitive.
8. Press **Enter** and follow the prompts to install QRadar.

   The complete installation process is documented in the product Installation Guide. See "Installing QRadar after the RHEL installation" on page 18.

Standard Linux users

The tables describe the standard Linux user accounts that are created on the QRadar console SIEM server and other QRadar product components (All In One console, QRadar Risk Manager, QRadar Incident Forensics, QRadar Network Insights, App Host, and all other managed hosts).

The following tables show standard Linux user accounts for RedHat and QRadar.

Table 3. Standard Linux user accounts for RedHat

User account	Login to the Login Shell	Purpose
root (password required)	Yes	RedHat user

Table 3. Standard Linux user accounts for RedHat (continued)		
User account	**Login to the Login Shell**	**Purpose**
bin	No	Linux Standard Base
daemon	No	Linux Standard Base
adm	No	Linux Standard Base
lp	No	Linux Standard Base
sync	No	Linux Standard Base
shutdown	No	Linux Standard Base
halt	No	Linux Standard Base
mail	No	Linux Standard Base
operator	No	Linux Standard Base
games	No	RedHat user
ftp	No	RedHat user
nobody	No	Linux Standard Base
systemd-network	No	RedHat user
dbus	No	RedHat user
polkitd	No	RedHat user
sshd	No	RedHat user
rpc	No	RedHat user
rpcuser	No	RedHat user
nfsnobody	No	RedHat user
abrt	No	RedHat user
ntp	No	RedHat user
tcpdump	No	RedHat user
tss	No	RedHat user
saslauth	No	RedHat user
sssd	No	RedHat user

Table 4. Standard Linux user accounts for QRadar		
User Account	**Login to the Login Shell**	**Purpose**
ziptie	No	Ziptie service used by QRadar Risk Manager
vis	No	QRadar VIS service used by QRadar to process scan results
customactionuser	No	QRadar Custom Actions used to isolate custom actions into a chroot jail
mks	No	MKS QRadar component for handling secrets
qradar	No	General user for QRadar

Table 4. Standard Linux user accounts for QRadar (continued)		
User Account	**Login to the Login Shell**	**Purpose**
qvmuser	No	QRadar Vulnerability Manager used by QRadar Vulnerability Manager
postgres	No (account locked)	PostgreSQL database used by QRadar
tlsdated	No	Tlsdate legacy time sync tool that was previously used by QRadar
traefik	No	Traefik service proxies Docker Containers for QRadar App Framework
gluster	No	GlusterFS used by QRadar HA on event collectors
solr	No	Solr service used by QRadar Forensics
openvpn	No	OpenVPN optional VPN tool installed by QRadar
chrony	No	Chronyd service time sync tool used by QRadar
apache	No	Apache Web Server used by QRadar
postfix	No	Mail Service used by QRadar to send email
vsftpguest	No	FTP service used in QRadar Forensics

Third-party software on QRadar appliances

IBM QRadar is a security appliance that is built on Linux, and is designed to resist attacks. QRadar is not intended as a multi-user, general-purpose server. It is designed and developed specifically to support its intended functions. The operating system and the services are designed for secure operation. QRadar has a built-in firewall, and allows administrative access only through a secure connection that requires encrypted and authenticated access, and provides controlled upgrades and updates. QRadar does not require or support traditional anti-virus or malware agents, or support the installation of third-party packages or programs.

Chapter 2. QRadar installations

There are two ways to install QRadar on your hardware: a software installation, or an appliance installation.

Appliance installation
An appliance installation is a QRadar installation that uses the version of Red Hat Enterprise Linux (RHEL) included in the QRadar ISO. An appliance installation on your own hardware or in a virtual machine requires you to purchase a software node entitlement. Contact your QRadar sales representative for more information about purchasing a software node entitlement. You do not need to configure partitions or perform other RHEL preparation as part of an appliance installation. Choose this option, if RHEL is not already installed. Proceed to "Installing a QRadar appliance" on page 11. However, if the hardware/virtual instance configuration varies from our listed specifications, the version of RHEL included in the QRadar ISO may not install properly. In that case, you should attempt a software installation.

Software installation
A software installation is a QRadar installation that uses a RHEL operating system that you provide. The RHEL version required for your installment must be provided by a 3rd party. You must configure partitions and perform other RHEL preparations before a QRadar software installation. Aside from RHEL, all software installations requires you to purchase a software node entitlement. Contact your QRadar sales representative for more information about purchasing a software node entitlement. Proceed to "QRadar software installations" on page 13.

Installing a QRadar appliance

Install a IBM QRadar Console or a managed host on a QRadar appliance or on your own appliance.

Software versions for all QRadar appliances in a deployment must be same version and fix level. Deployments that use different versions of software are not supported.

Before you begin

Ensure that the following requirements are met:

- The required hardware is installed.
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection.
- If you want to configure bonded network interfaces, see Chapter 8, "Configuring bonded management interfaces," on page 113.
- If you are installing QRadar on a Unified Extensible Firmware Interface (UEFI) system, secure boot must be disabled.

Procedure

1. Type `root` at the login prompt to launch the installation wizard. Type `password` if you are prompted for a password.
2. Accept the **End User License Agreement**.
3. Select the appliance type:
   - **Appliance Install**
   - **High Availability Appliance**
4. If you selected **High Availability Appliance** complete the following steps:
   a) Select **HA appliance (All models) 500** as the functionality.

© Copyright IBM Corp. 2004, 2021

b) Select whether the high-availability (HA) appliance is a standby for a console or non-console appliance.

c) Select **Next**.

5. If you did not choose **High Availability Appliance**, select the appliance assignment, and then select **Next**.
6. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and set up the time.
7. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.
8. Select the Internet Protocol version:
   - **ipv4**
   - **ipv6**

   If you selected **ipv6**, select **manual** or **auto** for the **Configuration type**.

   manual
   You must use a static IP address with a CIDR range.

   auto
   A static IP address with a CIDR range is generated with the Neighbor Discovery Protocol.
9. Select the bonded interface setup, if required.
10. Select the management interface.
11. In the wizard, enter a fully qualified domain name in the **Hostname** field.

    Important:

    - The hostname must not contain only numbers.
    - The console and managed host (MH) cannot have the same hostname.
12. In the **IP address** field, enter a static IP address, or use the assigned IP address.
13. If you do not have an email server, enter `localhost` in the **Email server name** field.
14. Enter a `root` password that meets the following criteria:
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.
15. If you are installing a Console, enter an `admin` password that meets the following criteria:
    - Contains at least 8 characters
    - Contains at least one uppercase character
    - Contains at least one lowercase character
    - Contains at least one digit
    - Contains at least one special character: @, #, ^, or *
16. Click **Finish**.
17. Follow the instructions in the installation wizard to complete the installation.

    The installation process might take several minutes.
18. If you are installing a Console, apply your license key.

    a) Log in to QRadar as the `admin` user:

    `https://<IP_Address_QRadar>`

    b) Click **Login**.

    c) On the navigation menu (☰), click **Admin**.

    d) In the navigation pane, click **System Configuration**.

    e) Click the **System and License Management** icon.

    f) From the **Display** list box, select **Licenses**, and upload your license key.

g) Select the unallocated license and click **Allocate System to License**.

h) From the list of systems, select a system, and click **Allocate System to License**.

19. If you want to add managed hosts, see the *IBM QRadar Administration Guide*.

What to do next

Go to the (https://apps.xforce.ibmcloud.com/) to download *Security applications* for your installation. For more information, see the *Content Management* chapter in the *IBM QRadar Administration Guide*.

QRadar software installations

A software installation is a QRadar installation on your hardware that uses an RHEL operating system that you provide. You must configure partitions and perform other RHEL preparation before a QRadar software installation.

Important:

- Ensure that your hardware meets the system requirements for QRadar deployments. For more information about system requirements, see "Prerequisites for installing QRadar on your hardware" on page 13, and "System requirements for virtual appliances" on page 24.
- You must acquire entitlement to a QRadar Software Node for a QRadar software installation. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.
- Install no software other than QRadar and RHEL on your hardware. Unapproved RPM installations can cause dependency errors when you upgrade QRadar software and can also cause performance issues in your deployment.
- When you build a software appliance as an Event Processor and add it to your deployment, the appliance shows up in License management as an Event Processor/Flow Processor software appliance. However, the software appliance only functions as an Event Processor.
- Do not update your operating system or packages before or after QRadar installation.
- If you are installing QRadar on a Unified Extensible Firmware Interface (UEFI) system, secure boot must be disabled.

Warning: Software installations do not come with the recovery partition available, and also these instructions do not apply.

Complete the following tasks in order:

__ • "Installing RHEL on your system" on page 15

__ • "Installing QRadar after the RHEL installation" on page 18

Prerequisites for installing QRadar on your hardware

Before you install the Red Hat Enterprise Linux (RHEL) operating system on your hardware, ensure that your system meets the system requirements.

QRadar and RHEL version compatibility

The following table describes the version of Red Hat Enterprise Linux used with the IBM QRadar version.

Table 5. Red Hat version

IBM QRadar version	Red Hat Enterprise Linux version
IBM QRadar 7.4.0	Red Hat Enterprise Linux V7.6 64-bit
IBM QRadar 7.4.1	Red Hat Enterprise Linux V7.7 64-bit
IBM QRadar 7.4.2	Red Hat Enterprise Linux V7.7 64-bit
IBM QRadar 7.4.3	Red Hat Enterprise Linux V7.7 64-bit

The following table describes the system requirements:

Table 6. System requirements for RHEL installations on your own appliance

Requirement	Description
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.
Firewall configuration	WWW (http, https) enabled SSH-enabled
Hardware	See the tables below for memory, processor, and storage requirements.

Memory and CPU requirements

If you use hardware not provided by IBM QRadar, ensure that your appliance meets or exceeds the specifications for memory and CPU of the corresponding QRadar appliance. For information about the specifications of the QRadar appliances, see *IBM QRadar Hardware Guide*.

Important: You can change the memory or the CPU of your appliance by shutting down the appliance and making the changes. When you restart the appliance the system detects the changes and adjusts the performance related configuration. You must maintain the minimum requirements.

Storage requirements

Your appliance must have at least 256 GB of storage available.

The following table shows the storage requirements for installing QRadar on your hardware.

Note: The minimum required storage size will vary, based on factors such as event size, events per second (EPS), and retention requirements.

Table 7. Minimum storage requirements for appliances when you use the virtual or software installation option.

System classification	Appliance information	IOPS	Data transfer rate (MB/s)
Minimum performance	Supports XX05 licensing	800	500
Medium performance	Supports XX29 licensing	1200	1000
High Performance	Supports XX48 licensing	10,000	2000
Small All-in-One or 1600	Less than 500 EPS	300	300
Event/Flow Collectors	Events and flows	300	300

Installing RHEL on your system

You can install the Red Hat Enterprise Linux (RHEL) operating system on your system to use with IBM QRadar.

Before you begin

Download the Red Hat Enterprise Linux Server Binary DVD from https://access.redhat.com Refer to the Red Hat version table to choose the correct version.

Table 8. Red Hat version

IBM QRadar version	Red Hat Enterprise Linux version
7.4.0	Red Hat Enterprise Linux Server V7.6 Binary DVD
7.4.1	Red Hat Enterprise Linux Server V7.7 Binary DVD
7.4.2	Red Hat Enterprise Linux Server V7.7 Binary DVD
7.4.3	Red Hat Enterprise Linux Server V7.7 Binary DVD

About this task

You must acquire entitlement to a QRadar Software Node for a QRadar software installation. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

If there are circumstances where you need to install RHEL separately, proceed with the following instructions. Otherwise, proceed to "Installing a QRadar appliance" on page 11.

Procedure

1. Map the ISO to a device for your appliance by using the Integrated Management Module (IMM) or the Integrated Dell Remote Access Controller (iDRAC), or insert a bootable USB drive with the ISO.

   For information about creating a bootable USB flash drive, see:

   - "Creating a bootable USB flash drive with a Windows system" on page 4
   - "Creating a bootable USB flash drive on a Apple Mac OS X system" on page 5
   - "Creating a bootable USB flash drive with Red Hat Linux" on page 5
2. Insert the portable storage device into your appliance and restart your appliance.
3. From the starting menu, do one of the following options:
   - Select the device that you mapped the ISO to, or the USB drive, as the boot option.
   - To install on a system that supports Extensible Firmware Interface (EFI), you must start the system in `legacy` mode.
4. When prompted, log in to the system as the root user.
5. Follow the instructions in the installation wizard to complete the installation:
   a) Set the language to English (US).
   b) Click **Date & Time** and set the time for your deployment.
   c) Click **Software selection** and select **Minimal Install**.
   d) Click **Installation Destination** and select the **I will configure partitioning** option.
   e) To encrypt data, check the **Encrypt my data** checkbox.
   f) Select **LVM** from the list.
   g) Click the **Add** button to add the mount points and capacities for your partitions, and then click **Done**. For more information about RHEL7 partitions, see "Linux operating system partition properties for QRadar installations on your own system" on page 16.

      To encrypt data complete the following steps:

i) Select one of the LVM partitions created.

ii) Select **Modify** under the **Volume Group** section. A pop up console opens for further configuration options.

iii) Select **Encrypt.**

iv) Save the changes.

h) Click **Network & Host Name**.

i) Enter a fully qualified domain name for your appliance hostname.

Important: The console and managed host (MH) cannot have the same hostname.

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

k) On the **General** tab, select the **Automatically connect to this network when it is available** option.

l) On the **IPv4 Settings** or **IPv6 Settings** tab, select **Manual** in the **Method** list.

m) Click **Add**.

- For an IPv4 deployment, enter the IP address, Netmask, and Gateway for the appliance in the **Addresses** field.
- For an IPv6 deployment, enter the IP address, Prefix, and Gateway in the **Addresses** field.

n) Add two DNS servers.

o) Click **Save** > **Done** > **Begin Installation**.

6. Set the root password, and then click **Finish configuration**.
7. After the installation finishes, disable SELinux by modifying the `/etc/selinux/config` file, and restart the appliance.

What to do next

"Installing QRadar after the RHEL installation" on page 18

Linux operating system partition properties for QRadar installations on your own system

If you use your own appliance hardware, you can delete and re-create partitions on your Red Hat Enterprise Linux operating system rather than modify the default partitions.

Use the values in following table as a guide when you re-create the partitioning on your Red Hat Enterprise Linux operating system. You must use these partition names. Using other partition names can cause the installation to fail and other issues.

The file system for each partition is XFS.

Table 9. Partitioning guide for RHEL

Mount Path	LVM supported?	Size
`/boot`	No	1 GB
`/boot/efi`	No	200 MB
`/var`	Yes	5 GB
`/var/log`	Yes	15 GB
`/var/log/audit`	Yes	3 GB
`/opt`	Yes	13 GB
`/home`	Yes	1 GB
`/storetmp`	Yes	15 GB
`/tmp`	Yes	3 GB

Table 9. Partitioning guide for RHEL (continued)		
Mount Path	**LVM supported?**	**Size**
`swap`	N/A	Swap formula: Configure the swap partition size to be 75 per cent of RAM, with a minimum value of 12 GiB and a maximum value of 24 GiB.
`/`	Yes	Up to 15 GB
`/store`	Yes	80% of remaining space
`/transient`	Yes	20% of remaining space

For more information about the swap partition, see https://www.ibm.com/support/pages/node/6348712 (https://www.ibm.com/support/pages/node/6348712).

Console partition configurations for multiple disk deployments

For systems with multiple disks, configure the following partitions for QRadar:

Disk 1
boot, swap, OS, QRadar temporary files, and log files

Remaining disks

- Use the default storage configurations for QRadar appliances as a guideline to determine what RAID type to use.
- Mounted as `/store`
- Store QRadar data

The following table shows the default storage configuration for QRadar appliances.

Table 10. Default storage configurations for QRadar appliances	
QRadar host role	**Storage configuration**
Flow collector QRadar Network Insights (QNI)	RAID1
Data node Event processor Flow processor Event and flow processor All-in-one console	RAID6
Event collector	RAID10

Installing QRadar after the RHEL installation

Install IBM QRadar on your own device after you install RHEL.

Before you begin

A fresh software install erases all data in `/store` as part of the installation process. If you want to preserve the contents of `/store` when performing a software install (such as when performing a manual retain), back up the data you want to preserve apart from the host where the software is to be installed.

Procedure

1. Copy the QRadar ISO to the `/root` or `/storetmp` directory of the device.
2. Create the `/media/cdrom` directory by typing the following command:

   ```
   mkdir /media/cdrom
   ```

3. Mount the QRadar ISO by using the following command:

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

4. Run the QRadar setup by using the following command:

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

   Note: A new kernel might be installed as part of the installation, which requires a system restart. Repeat the commands in steps 3 and 4 after the system restart to continue the installation.
5. Select the appliance type:
   - **Software Install**
   - **High Availability Appliance**
6. Select the appliance assignment, and then select **Next**.
7. If you selected an appliance for high-availability (HA), select whether the appliance is a console.
8. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and set up the time.
9. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.
10. Select the Internet Protocol version.
11. If you selected **ipv6**, select **manual** or **auto** for the **Configuration type**.
12. Select the bonded interface setup, if required.
13. Select the management interface.
14. In the wizard, enter a fully qualified domain name in the **Hostname** field.

    Important:
    - The hostname must not contain only numbers.
    - The console and managed host (MH) cannot share the have hostname.
15. In the **IP address** field, enter a static IP address, or use the assigned IP address.

    Important: If you are configuring this host as a primary host for a high availability (HA) cluster, and you selected **Yes** for auto-configure, you must record the automatically-generated IP address. The generated IP address is entered during HA configuration.

    For more information, see IBM Security QRadar High Availability Guide.
16. If you do not have an email server, enter `localhost` in the **Email server name** field.
17. Leave the `root` password as it is.
18. If you are installing a Console, enter an `admin` password that meets the following criteria:
    - Contains at least 5 characters
    - Contains no spaces

- Can include the following special characters: @, #, ^, and *.

19. Click **Finish**.
20. Follow the instructions in the installation wizard to complete the installation.

    The installation process might take several minutes.
21. If you are installing a Console, apply your license key.
    a) Log in to QRadar as the `admin` user:

       `https://<IP_Address_QRadar>`

    b) Click **Login**.
    c) On the navigation menu (☰), click **Admin**.
    d) In the navigation pane, click **System Configuration**.
    e) Click the **System and License Management** icon.
    f) From the **Display** list box, select **Licenses**, and upload your license key.
    g) Select the unallocated license and click **Allocate System to License**.
    h) From the list of systems, select a system, and click **Allocate System to License**.
22. If you want to add managed hosts, see Managed hosts.

Chapter 3. Virtual appliance installations

You can install IBM QRadar SIEM on a virtual appliance. Ensure that you use a supported virtual appliance that meets the minimum system requirements.

There are two ways to install QRadar on your virtual appliance: a software installation, or an appliance installation.

Appliance installation
An appliance installation is a QRadar installation that uses the version of Red Hat Enterprise Linux (RHEL) included in the QRadar ISO. An appliance installation on your own hardware or in a virtual machine requires you to purchase a software node entitlement. Contact your QRadar sales representative for more information about purchasing a software node entitlement. You do not need to configure partitions or perform other RHEL preparation as part of an appliance installation. Choose this option, if RHEL is not already installed. Proceed to Installing a QRadar appliance. However, if the hardware/virtual instance configuration varies from our listed specifications, the version of RHEL included in the QRadar ISO may not install properly. In that case, you should attempt a software installation.

Software installation
A software installation is a QRadar installation that uses a RHEL operating system that you provide. The RHEL version required for your installment must be provided by a 3rd party. You must configure partitions and perform other RHEL preparations before a QRadar software installation. Aside from RHEL, all software installations requires you to purchase a software node entitlement. Contact your QRadar sales representative for more information about purchasing a software node entitlement. Proceed to QRadar software installations.

Note: If the installer does not detect that RHEL is installed, an appliance installation is performed automatically. You still see both the **Appliance Install (purchased as an appliance)** or **Software Install (hardware was purchased separately)** options in the installer menu. If RHEL is installed, only the **Software Install (hardware was purchased separately)** option appears.

To install a virtual appliance, complete the following tasks in order:

- Create a virtual machine.
- Install QRadar software on the virtual machine.
- If your virtual appliance is a manged host, add your virtual appliance to your deployment.

Important: Install no software other than QRadar and RHEL on your virtual machine.

Overview of supported virtual appliances

A virtual appliance provides the same visibility and function in your virtual network infrastructure that QRadar appliances provide in your physical environment.

The following virtual appliances are available:

- QRadar SIEM All-in-One Virtual 3199
- QRadar SIEM Event and Flow Processor Virtual 1899
- QRadar SIEM Flow Processor Virtual 1799
- QRadar SIEM Event Processor Virtual 1699
- QRadar Event Collector Virtual 1599
- QRadar Data Node Virtual 1400
- QRadar QFlow Virtual 1299
- QRadar Risk Manager 700
- QRadar Vulnerability Manager Processor 600

© Copyright IBM Corp. 2004, 2021

- QRadar Vulnerability Manager Scanner 610
- QRadar App Host 4000
- QRadar Incident Forensics

QRadar SIEM All-in-One Virtual 3199

This virtual appliance is a QRadar SIEM system that profiles network behavior and identifies network security threats. The QRadar SIEM All-in-One Virtual 3199 virtual appliance includes an onboard Event Collector, a combined Event Processor and Flow Processor, and internal storage for events.

The QRadar SIEM All-in-One Virtual 3199 virtual appliance supports the following items:

- Up to 1,000 network objects
- 1,200,000 flows per interval, depending on your license
- 30,000 Events Per Second (EPS), depending on your license
- External flow data sources for NetFlow, sFlow, J-Flow, Packeteer, and Flowlog files
- QRadar QFlow Collector and Layer 7 network activity monitoring

To expand the capacity of the QRadar SIEM All-in-One Virtual 3199 beyond the license-based upgrade options, you can add one or more of the QRadar SIEM Event Processor Virtual 1699 or QRadar SIEM Flow Processor Virtual 1799 virtual appliances.

QRadar SIEM Event and Flow Processor Virtual 1899

This virtual appliance is deployed with any QRadar Console. The virtual appliance is used to increase storage and includes a combined Event Processor and Flow Processor and internal storage for events and flows.

QRadar SIEM Event and Flow Processor Virtual 1899 appliance supports the following items:

- 1,200,000 flows per interval, depending on traffic types
- 30,000 Events Per Second (EPS), depending on your license
- 2 TB or larger dedicated flow storage
- 1,000 network objects
- QRadar QFlow Collector and Layer 7 network activity monitoring

You can add QRadar SIEM Event and Flow Processor Virtual 1899 appliances to any QRadar Console to increase the storage and performance of your deployment.

QRadar SIEM Flow Processor Virtual 1799

This virtual appliance is a dedicated Flow Processor that you can use to scale your QRadar SIEM deployment to manage higher flows per interval rates. The QRadar SIEM Flow Processor Virtual 1799 includes an onboard Flow Processor and internal storage for flows.

The QRadar SIEM Flow Processor Virtual 1799 appliance supports the following items:

- 3,600,000 flows per interval, depending on traffic types
- 2 TB or larger dedicated flow storage
- 1,000 network objects
- QRadar QFlow Collector and Layer 7 network activity monitoring

The QRadar SIEM Flow Processor Virtual 1799 appliance is a distributed Flow Processor appliance and requires a connection to any QRadar SIEM 31XX series appliance.

QRadar SIEM Event Processor Virtual 1699

This virtual appliance is a dedicated Event Processor that you can use to scale your QRadar SIEM deployment to manage higher EPS rates. The QRadar SIEM Event Processor Virtual 1699 includes an onboard Event Collector, Event Processor, and internal storage for events.

The QRadar SIEM Event Processor Virtual 1699 appliance supports the following items:

- Up to 80,000 events per second
- 2 TB or larger dedicated event storage

The QRadar SIEM Event Processor Virtual 1699 virtual appliance is a distributed Event Processor appliance and requires a connection to any QRadar SIEM 31XX series appliance.

QRadar Event Collector Virtual 1599

This virtual appliance is a dedicated Event Collector that you can use to scale your QRadar SIEM deployment to manage higher EPS rates. The QRadar Event Collector Virtual 1599 includes an onboard Event Collector.

The QRadar Event Collector Virtual 1599 appliance supports the following items:

- Up to 30,000 events per second
- 2 TB or larger dedicated event storage

The QRadar Event Collector Virtual 1599 virtual appliance is a distributed Event Collector appliance and requires a connection to any QRadar SIEM 16XX, 18XX, or 31XX series appliance.

QRadar Data Node Virtual 1400

This virtual appliance provides retention and storage for events and flows. The virtual appliance expands the available data storage of Event Processors and Flow Processors, and also improves search performance.

Note: Encrypted data transmission between Data Nodes and Event Processors is not supported. The following firewall ports must be opened for Data Node communication with the Event Processor:

- Port 32006 between Data Nodes and the Event Processor appliance
- Port 32011 between Data Nodes and the Console's Event Processor

Size your QRadar Data Node Virtual 1400 appliance based on the EPS rate and data retention rules of the deployment.

Data retention policies are applied to a QRadar Data Node Virtual 1400 appliance in the same way that they are applied to stand-alone Event Processors and Flow Processors. The data retention policies are evaluated on a node-by-node basis. Criteria, such as free space, is based on the individual QRadar Data Node Virtual 1400 appliance and not the cluster as a whole.

Data Nodes can be added to the following appliances:

- Event Processor (16XX)
- Flow Processor (17XX)
- Event/Flow Processor (18XX)
- All-In-One (2100 and 31XX)

To enable all features included in the QRadar Data Node Virtual 1400 appliance, install it by using the Data Node 1400 appliance type.

QRadar QFlow Virtual 1299

This virtual appliance provides the same visibility and function in your virtual network infrastructure that a QRadar QFlow Collector offers in your physical environment. The QRadar QFlow Collector virtual

appliance analyzes network behavior and provides Layer 7 visibility within your virtual infrastructure. Network visibility is derived from a direct connection to the virtual switch.

The QRadar QFlow Virtual 1299 appliance supports the following capabilities:

- Maximum throughput of 1 Gbps

  When the hardware and software specifications are the same, virtual flow appliances can deliver throughput that is comparable to an IBM-supplied appliance. For more information about the specifications for IBM-supplied appliances, see the *IBM QRadar Hardware Guide*.
- Three virtual switches, with one more switch that is designated as the management interface.

QRadar Vulnerability Manager Processor

This appliance is used to process vulnerabilities within the applications, systems, and devices on your network or within your DMZ. The vulnerability processor provides a scanning component by default. If required, you can deploy more scanners, either on dedicated QRadar Vulnerability Manager managed host scanner appliances or QRadar managed hosts. For example, you can deploy a vulnerability scanner on an Event Collector or QRadar QFlow Collector.

QRadar Vulnerability Manager Scanner

This appliance is used to scan for vulnerabilities within the applications, systems, and devices on your network or within your DMZ.

QRadar Risk Manager

This appliance is used for monitoring device configurations, simulating changes to your network environment, and prioritizing risks and vulnerabilities in your network.

QRadar App Host 4000

This appliance is a managed host that is dedicated to running apps. App Hosts provide extra storage, memory, and CPU resources for your apps without impacting the processing capacity of your QRadar Console. Apps such as User Behavior Analytics with Machine Learning Analytics require more resources than are currently available on the Console.

QRadar Incident Forensics

QRadar Incident Forensics is installed from a separate ISO than other QRadar appliances. For more information about installing QRadar Incident Forensics as a virtual appliance, see "Virtual appliance installations for QRadar Incident Forensics" in *IBM QRadar Incident Forensics Installation Guide*.

System requirements for virtual appliances

To ensure that IBM QRadar works correctly, you must use virtual appliances that meet the minimum requirements.

For more information about supported hypervisors and virtual hardware versions, see Creating your virtual machine.

QRadar virtual appliances require x86 hardware.

QRadar appliances are certified to support certain maximum events per second (EPS) rates. Maximum EPS depends on the type of data that is processed, system configuration, and system load. For more information, see QRadar maximum EPS certification methodology.

Note: The minimum requirements support QRadar functionality with minimum data sets and performance. The minimum requirements support a QRadar system that uses only the default apps. For optimal performance, use the suggested requirements.

QRadar Incident Forensics is installed from a separate ISO than other QRadar appliances. For more information about installing QRadar Incident Forensics as a virtual appliance, see "Virtual appliance installations for QRadar Incident Forensics" in *IBM QRadar Incident Forensics Installation Guide*.

Important: You can change the memory or the CPU of your virtual appliance by shutting down the virtual appliance and making the changes. When you restart the virtual appliance the system detects the changes and adjusts the performance related configuration.

Memory requirements

The following table describes the memory requirements for virtual appliances.

Table 11. Minimum and suggested 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 appliance	24 GB	48 GB
QRadar Event Collector Virtual 1599	12 GB (up to 20,000 EPS) 64 GB (40,000 EPS) 128 GB (80,000 EPS)	16 GB (up to 20,000 EPS) 64 GB (40,000 EPS) 128 GB (80,000 EPS)
QRadar SIEM Event Processor Virtual 1699 up to 20,000 EPS	12 GB	48 GB
QRadar SIEM Event Processor Virtual 1699 20,000 EPS or higher	128 GB	128 GB
QRadar SIEM Flow Processor Virtual 1799 up to 1,200,000 FPM	12 GB	48 GB
QRadar SIEM Flow Processor Virtual 1799 1,200,000 FPM or higher	128 GB	128 GB
QRadar SIEM Event and Flow Processor Virtual 1899 5,000 EPS or less 200,000 FPM or less	12 GB	48 GB
QRadar SIEM Event and Flow Processor Virtual 1899 30,000 EPS or less 1,000,000 FPM or less	128 GB	128 GB

Table 11. Minimum and suggested memory requirements for QRadar virtual appliances (continued)		
Appliance	**Minimum memory requirement**	**Suggested memory requirement**
QRadar SIEM All-in-One Virtual 3199 5,000 EPS or less 200,000 FPM or less	32 GB	48 GB
QRadar SIEM All-in-One Virtual 3199 30,000 EPS or less 1,000,000 FPM or less	64 GB	128 GB
QRadar Log Manager Virtual 8099	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
QRadar App Host	12 GB	64 GB or more for a medium sized App Host 128 GB or more for a large sized App Host

Processor requirements

The following table describes the CPU requirements for virtual appliances.

Table 12. CPU requirements for QRadar virtual appliances			
QRadar appliance	**Threshold**	**Minimum number of CPU cores**	**Suggested number of CPU cores**
QRadar QFlow Virtual 1299	10,000 FPM or less	4	4
QRadar Event Collector Virtual 1599	5,000 EPS or less	8	16
	20,000 EPS or less	19	19
QRadar SIEM Event Processor Virtual 1699	5,000 EPS or less	8	24
	20,000 EPS or less	16	24
	40,000 EPS or less	40	40
	80,000 EPS or less	56	56

Table 12. CPU requirements for QRadar virtual appliances (continued)

QRadar appliance	Threshold	Minimum number of CPU cores	Suggested number of CPU cores
QRadar SIEM Flow Processor Virtual 1799	150,000 FPM or less	4	24
	300,000 FPM or less	8	24
	1,200,000 FPM or less	16	24
	2,400,000 FPM or less	48	48
	3,600,000 FPM or less	56	56
QRadar SIEM Event and Flow Processor Virtual 1899	200,000 FPM or less 5,000 EPS or less	16	24
	300,000 FPM or less 15,000 EPS or less	48	48
	1,200,000 FPM or less 30,000 EPS or less	56	56
QRadar SIEM All-in-One Virtual 3199	25,000 FPM or less 500 EPS or less	4	24
	50,000 FPM or less 1,000 EPS or less	8	24
	100,000 FPM or less 1,000 EPS or less	12	24
	200,000 FPM or less 5,000 EPS or less	16	24
	300,000 FPM or less 15,000 EPS or less	48	48
	1,200,000 FPM or less 30,000 EPS or less	56	56
QRadar Log Manager Virtual 8099	2,500 EPS or less	4	16
	5,000 EPS or less	8	16
QRadar Vulnerability Manager Processor		4	4
QRadar Vulnerability Manager Scanner		4	4
QRadar Risk Manager		8	8
QRadar Data Node Virtual 1400 appliance		4	16

Table 12. CPU requirements for QRadar virtual appliances (continued)			
QRadar appliance	**Threshold**	**Minimum number of CPU cores**	**Suggested number of CPU cores**
QRadar App Host		4	12 or more for a medium sized App Host 24 or more for a large sized App Host

Storage requirements

Your virtual appliance must have at least 256 GB of storage available.

The following table shows the storage requirements for installing QRadar by using the virtual or software only option.

Table 13. Minimum storage requirements for appliances when you use the virtual or software installation option.			
System classification	**Appliance information**	**IOPS**	**Data transfer rate (MB/s)**
Minimum performance	Supports XX05 licensing	800	500
Medium performance	Supports XX29 licensing	1200	1000
High Performance	Supports XX48 licensing	10,000	2000
Small All-in-One or 1600	Less than 500 EPS	300	300
Event/Flow Collectors	Events and flows	300	300

Related tasks

Creating your virtual machine
To install a IBM QRadar virtual appliance, you must first create a virtual machine.

Creating your virtual machine

To install a IBM QRadar virtual appliance, you must first create a virtual machine.

Before you begin

QRadar virtual appliances require x86 hardware.

Procedure

1. Create a virtual machine by using one of the following hypervisors:
   - VMWare ESXi with hardware version 13
   - KVM on CentOS or Red Hat Enterprise Linux V7.7 with QEMU KVM 1.5.3-141
   - The Hyper-V plugin on Windows Server 2016 with all Windows updates applied

   Notes:

   - If you are installing a QRadar appliance in Hyper-V, you must do a software installation, not an appliance installation. If you are using a version of Hyper-V that includes a secure boot option, secure boot must be disabled.
   - If you create a virtual machine by using KVM, you must do a software installation.

- If you are installing QRadar on a Unified Extensible Firmware Interface (UEFI) system, secure boot must be disabled.
- The listed hypervisor versions are tested by IBM, but other untested versions might also work. If you install QRadar on an unsupported version and encounter an issue that can be produced on the listed version of that hypervisor, IBM supports that issue.

For more information about VMWare ESXi and hardware versions, see ESXi/ESX hosts and compatible virtual machine hardware versions list (https://kb.vmware.com/s/article/2007240).

2. Configure your virtual machine to meet the requirements for CPUs, RAM, and storage parameters. See "System requirements for virtual appliances" on page 24.
3. Configure at least one network interface for your virtual machine.

What to do next

"Installing QRadar on a virtual machine" on page 29

Installing QRadar on a virtual machine

After you create your virtual machine, you must install the IBM QRadar software on the virtual machine.

Before you begin

Create a virtual machine. For more information, see "Creating your virtual machine" on page 28.

Determine if you need to do an appliance installation or a software installation. For more information about appliance installations and software installations, see Chapter 3, "Virtual appliance installations," on page 21.

For a software installation, you must install Red Hat Enterprise Linux (RHEL) before you install QRadar. For more information about installing RHEL for QRadar, see "Installing RHEL on your system" on page 15.

Procedure

1. Log in to the virtual machine by typing `root` for the user name.

   The user name is case-sensitive.
2. Accept the **End User License Agreement**.
3. Select the appliance type:
   - **Non-Software Appliance** for an appliance installation.
   - **Software Appliance** for a software installation.
4. Select the appliance assignment, and then select **Next**.
5. If you selected an appliance for high-availability (HA), select whether the appliance is a console.
6. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and set up the time.
7. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.
8. Select the Internet Protocol version:
   - Select **ipv4** or **ipv6**.
9. If you selected **ipv6**, select **manual** or **auto** for the **Configuration type**.
10. Select the bonded interface setup, if required.
11. Select the management interface.
12. In the wizard, enter a fully qualified domain name in the **Hostname** field.

    Important:
    - The hostname must not contain only numbers.
    - The console and managed host (MH) cannot have the same hostname.
13. In the **IP address** field, enter a static IP address, or use the assigned IP address.

Important: If you are configuring this host as a primary host for a high availability (HA) cluster, and you selected **Yes** for auto-configure, you must record the automatically generated IP address. The generated IP address is entered during HA configuration.

For more information, see the *IBM Security QRadar High Availability Guide*.

14. If you do not have an email server, enter `localhost` in the **Email server name** field.
15. Enter `root` and `admin` passwords that meet the following criteria:
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.
16. Click **Finish**.
17. Follow the instructions in the installation wizard to complete the installation.

    The installation process might take several minutes. When the installation is complete, if you are installing a QRadar Console, proceed to step 18. If you are installing a managed host, proceed to "Adding your virtual appliance to your deployment" on page 30.
18. Apply your license key.
    a) Log in to QRadar:

    `https://QRadar_IP_Address`

    b) Click **Login**.

    c) On the navigation menu (☰), click **Admin**.

    d) In the navigation pane, click **System Configuration**.

    e) Click the **System and License Management** icon.

    f) From the **Display** list box, select **Licenses**, and upload your license key.

    g) Select the unallocated license and click **Allocate System to License**.

    h) From the list of systems, select a system, and click **Allocate System to License**.

Adding your virtual appliance to your deployment

If your virtual appliance is a managed host, add your virtual appliance to your deployment.

Procedure

1. Log in to your QRadar Console.
2. On the navigation menu (☰), click **Admin**.
3. In the **Admin** settings, click the **System and License Management** icon.
4. On the **Deployment Actions** menu, click **Add Host**.
5. Configure the settings for the managed host by providing the fixed IP address, and the root password to access the operating system shell on the appliance.
6. Click **Add**.
7. In the **Admin** settings, click **Deploy Changes**.
8. If you are installing a Console, apply your license key.
    a) Log in to QRadar as the `admin` user:

    `https://<IP_Address_QRadar>`

    b) Click **Login**.

    c) On the navigation menu (☰), click **Admin**.

    d) In the navigation pane, click **System Configuration**.

    e) Click the **System and License Management** icon.

f) From the **Display** list box, select **Licenses**, and upload your license key.

g) Select the unallocated license and click **Allocate System to License**.

h) From the list of systems, select a system, and click **Allocate System to License**.

Chapter 4. QRadar cloud marketplace images

You can install instances of IBM QRadar software by using the marketplace images on supported cloud platform.

QRadar marketplace images are available on the following cloud platforms:

- Amazon Web Services
- Google Cloud Platform
- IBM Cloud
- IBM Cloud VPC
- Microsoft Azure
- Oracle Cloud

Marketplace images for a particular QRadar version might not be available right away. Earlier versions of the marketplace images can be upgraded to 7.4.3. For information about upgrading to 7.4.3, see Upgrading QRadar to 7.4.3.

Configuring a QRadar 7.4.3 virtual appliance on Amazon Web Services

Configure an IBM QRadar virtual appliance on an Amazon Web Services (AWS) instance by using the provided Amazon Machine Image (AMI).

Before you begin

You must acquire entitlement to a QRadar Software Node for any QRadar instance that is deployed from a third-party cloud marketplace. Entitlement to the software node should be in place before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with AWS infrastructure, refer to AWS documentation. If IBM Support determines that your issue is caused by the AWS infrastructure, you must contact AWS for support to resolve the underlying issue with the AWS infrastructure.

You must use static IP addresses.

If you are installing IBM QRadar Network Insights, you must ensure that the instance configuration can support the flow inspection rate that you want to achieve. To view examples of how the hardware configuration can impact the flow inspection rate, see Prerequisites for installing QRadar Network Insights on Amazon Web Services.

If you are installing a data gateway for QRadar on Cloud, go to Installing a QRadar data gateway in Amazon Web Services from the marketplace image (https://www.ibm.com/support/knowledgecenter/en/SSKMKU/com.ibm.qradar.doc_cloud/t_hosted_aws_image.html).

If you deploy a managed host and a Console in the same virtual network, use the private IP address of the managed host to add it to the Console.

If you deploy a managed host and a Console in different virtual networks, you must allow firewall rules for the communication between the Console and the managed host. For more information, see “QRadar port usage ” on page 122.

© Copyright IBM Corp. 2004, 2021

Procedure

1. Go to IBM Security QRadar SIEM 7.4.3 (BYOL) (https://aws.amazon.com/marketplace/pp/prodview-f6d7zsi6jtipa).

   Note: Go to the Amazon Web Services China marketplace (https://awsmarketplace.amazonaws.cn/marketplace/pp/prodview-ejtrfvtaya6k6) to obtain an image for use with your IBM QRadar SIEM in China.
2. Click **Continue to Subscribe**.
3. Click **Accept Terms**.
4. When the subscription is ready, click **Continue to Configuration**.
5. Select a region and click **Continue to launch**.
6. From the **Choose Action** list, select **Launch through EC2**.
7. Click **Launch**.
8. Give your instance a name.
9. Select an EC2 Instance from the following list that meets the system requirements for virtual appliances. (T3, T3A, M6i, M6a, M5, M5a, M5zn, C6i, C6a, C5, C5a, C5n, R6i, R5, R5a, R5b, R5n, X2iezn)
10. Configure or select a key pair. You use this key pair every time you connect to the appliance by using SSH.
11. Click **Edit** in the **Network settings** section.
    a) Select a virtual private cloud (VPC).
    b) Create or select a subnet for your VPC.
    c) Create or select a security group that allows ports 22, and 443 for a QRadar console, to create an allowlist of trusted IP addresses that can access your QRadar deployment.

       In a QRadar deployment with multiple appliances, other ports might also be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see Common ports and servers used by QRadar.
12. Navigate to the **Configure Storage** section
    a) Click **Add new volume**.

       For information about available disk options, see AWS Volume Types.
    b) Estimate your storage needs and then enter a size in GiB.

       The minimum size is 250 GiB. The added disk must be the second disk. It cannot be the third or greater disk. When the installation is complete, this disk contains the `/store` and `/transient` partitions.

       Warning: It is not possible to increase storage after installation.
    c) Select the volume type of the data disk.
13. Click **Launch Instance**
14. Add **Additional Network Interfaces** if installing a QRadar Network Insights 6500 appliance.
    a) When the instance is ready, click the **Network Interfaces** link in the left menu.
    b) Click **Create Network Interface**. Configure the interface as wanted and ensure it is in the same subnet as the instance you started.
    c) When the network interface is created, select it from the list of available interfaces.
    d) When selected, click **Actions -> Attach**, select the QRadar Network Insights instance that you created to attach to, then click **Attach**.
15. When the instance is ready, log in using your key pair by typing the following command:

```
ssh -i <key.pem> ec2-user@<public_IP_address>
```

16. Type the following command to install the virtual appliance:

    ```
    sudo /root/setup <appliance_id>
    ```

    For example, to deploy an Event Collector type the following command:

    ```
    sudo /root/setup 1599
    ```

    You can install the following virtual appliance types:

Appliance type ID	Appliance type
1299	Flow Collector
1400	Data Node
1599	Event Collector
1699	Event Processor
1799	Flow Processor
1899	Event and Flow Processor
3199	All-in-One Console
4000	App host appliance
6500	QRadar Network Insights
7000	Data Gateway appliance

17. Enter a password for the admin account for an All-in-One Console, or the root password for all other appliance types. Set a strong password that meets the following criteria.
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.

What to do next

For All-in-One Console installations, the QRadar instance uses Coordinated Universal Time (UTC). You can change the time zone of the instance. For more information about changing the time zone, see Configuring system time.

This image does not receive automatic software upgrades. You must manually upgrade your system to keep it up to date. To receive QRadar upgrade notifications, see: Receiving QRadar update notifications.

For all managed host (except data gateways) installations, see adding a managed host

For QRadar Network Insights installations, see QRadar Network Insights installations on Amazon Web Services for information about adding the virtual appliance as a managed host and configuring flow sources and traffic mirroring.

Configuring a QRadar Console on Google Cloud Platform

Configure an IBM QRadar SIEM Console on a Google Cloud Platform (GCP) instance by using the provided image.

Before you begin

Important:

The following procedure is for the configuration of an IBM QRadar 7.3.2 Console image, which has reached its End of Support. An IBM® QRadar® 7.4.3 Console image is not yet available. Once the image

is installed, it should be upgraded to ensure that support is available. For information about upgrading to 7.4.3, see Upgrading QRadar SIEM.

You must acquire entitlement to a QRadar Software Node for any QRadar instance that is deployed from a third-party cloud marketplace. Entitlement to the software node should be in place before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with GCP infrastructure, refer to GCP documentation. If IBM Support determines that your issue is caused by the GCP infrastructure, you must contact GCP for support to resolve the underlying issue with the GCP infrastructure.

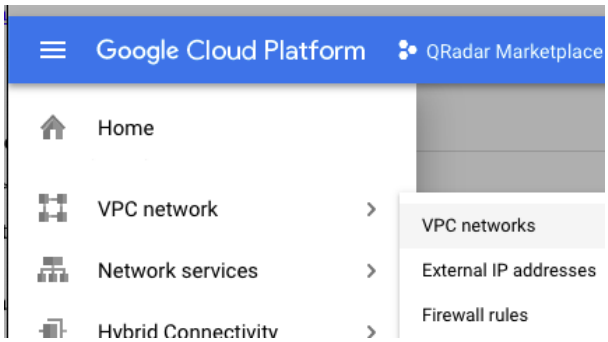
You must use static IP addresses.

You cannot have more than two DNS entries. QRadar installation fails if you have more than two DNS entries in the `/etc/resolv.conf` file.

If you are installing a data gateway for QRadar on Cloud, go to Installing a QRadar data gateway in Google Cloud Platform (https://www.ibm.com/support/knowledgecenter/en/SSKMKU/com.ibm.qradar.doc_cloud/t_hosted_gcp_image.html).

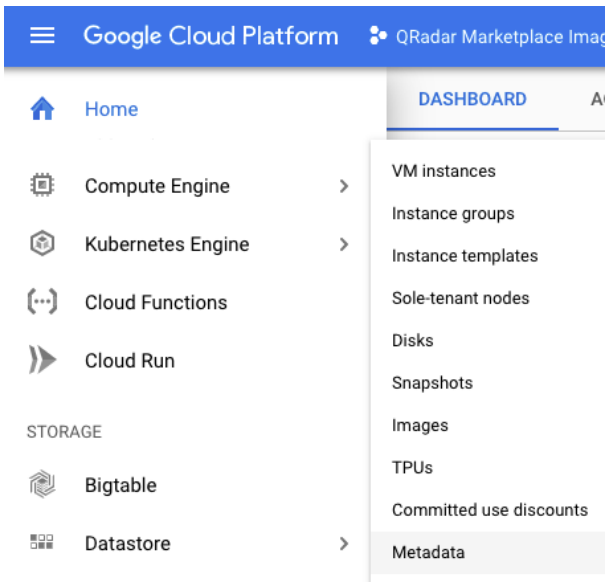
1. Create a project name that allows for a fully qualified domain name (FQDN) to be no more than 63 characters long. The FQDN consists of the deployment name followed by "-vm", the zone, the region, the project name, and ".internal".

   For example, if your project name is `abc-stq-xyz`, the appliance deployment name is `qr-con`, the zone is `us-east4-c`, and the region is `c`, the FQDN is `qr-con-vm.us-east4-c.c.abc-stq-xyz.internal`. The zone can be between 10 and 25 characters long. Depending on the zone, this leaves somewhere between 25 and 40 characters to be split between your project name and your deployment name.
2. In the project that you created in step 1, configure your network interface.
   a. Click **Google Cloud Platform** > **VPC network** > **VPC networks**.



©2019 Google LLC, used with permission. Google and the Google logo are registered trademarks of Google LLC.

   b. Click **CREATE VPC NETWORK**.
   c. Give your network a name, and configure the settings as needed. Set **DNS server policy** to **No server policy**.
   d. Click **Create**.
3. Add an SSH key to the project if you haven't already done so. The key must be created for a user called `cloud-user`.
   a. Click **Google Cloud Platform** > **Compute Engine** > **Metadata**.



©2019 Google LLC, used with permission. Google and the Google logo are registered trademarks of Google LLC.

b. Click **SSH Keys**.

c. Click **Edit**.

d. Click **Add item**.

e. Enter an SSH key, followed by `cloud-user`.

f. Click **Save**.

Procedure

1. Go to QRadar Security Intelligence Platform Console v7.3.2 P1 (https://console.cloud.google.com/marketplace/details/ibm-security-public/qradar-console?q=IBM%20qradar&id=34b7c045-edfa-485d-94d2-3b6ad1fe8ea9).
2. Click **LAUNCH**.
3. Set a deployment name for the appliance that allows for a fully qualified domain name (FQDN) to be no more than 63 characters long. The FQDN consists of the deployment name, the zone, the project name, and ".internal".

   For example, if your project name is `abc-stq-xyz`, the appliance deployment name is `qr-con`, the zone is `us-east4-c`, and the region is `c`, the FQDN is `qr-con-vm.us-east4-c.c.abc-stq-xyz.internal`. The zone can be between 10 and 25 characters long. Depending on the zone, this leaves somewhere between 25 and 40 characters to be split between your project name and your deployment name.
4. Select the zone that your project is in.
5. Select a **Machine Type** that meets the system requirements for virtual appliances.
6. Select the network interface that you created.
7. Set the firewall rules for your appliance that allow ports 22 and 443 only from trusted IP addresses to create an allowlist of IP addresses that can access your QRadar deployment.

   In a QRadar deployment with multiple appliances, other ports might also be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see “Common ports and servers used by QRadar” on page 122.
8. Check **I accept the GCP Marketplace Terms of Service**.
9. Click **Deploy**.
10. Set a static IP address for your appliance.

    a) Click **Google Cloud Platform** > **Compute Engine** > **VM instances**.

    b) Select your appliance from the list.

c) Click **Edit**.

d) Edit the network interface.

- Set the **Internal IP type** parameter to **Static** and reserve a new IP address.
- Select or create a static **External IP** address.

e) Click **Done**.

11. When the instance is ready, log in using **SSH** and your key pair by typing the following command:

```
ssh -i <key.pem> cloud-user@<public_IP_address>
```

12. Type the following command to check the length of your FQDN:

```
hostname -f | wc -c
```

If the command returns a value greater than 63 installation will fail. Restart this procedure with a shorter deployment name.

13. Ensure that there are no more than 2 DNS entries for the instance by typing the following command:

```
grep nameserver /etc/resolv.conf | wc -l
```

If the command returns 3 or higher, edit `/etc/resolv.conf` to remove all but two of the entries before you proceed to the next step. You will add the entries back after installation is complete.

14. To install the Console type the following command:

```
sudo /root/setup_console
```

15. Enter a password for the admin account. Set a strong password that meets the following criteria.

- Contains at least 5 characters
- Contains no spaces
- Can include the following special characters: @, #, ^, and *.

16. Type the following command to restart the host and complete the installation:

```
sudo reboot
```

17. Become the root user by typing the following command:

```
sudo -i
```

18. Update the license file to address the issue described in APAR IJ30161 (https://www.ibm.com/support/pages/apar/IJ30161) by typing the following command:

```
echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20"
| tee /opt/qradar/ecs/license.txt /opt/ibm/si/
services/ecs-ep/current/eventgnosis/license.txt /opt/ibm/si/services/ecs-ec-ingress/current/
eventgnosis/license.txt /opt/ibm/si/services/ecs-ec/current/eventgnosis/license.txt /usr/
eventgnosis/ecs/license.txt /opt/qradar/conf/templates/ecs_license.txt
```

It takes approximately 5 minutes for the changes to complete.

19. You can ensure automatic updates occur by typing the following command from a command line on the system:

```
$ sudo su -
$ pwck
$ systemctl start crond.service
```

To learn more, see APAR IJ21293 (https://www.ibm.com/support/pages/apar/IJ21293).

20. Exit the superuser shell by typing the following command:

```
exit
```

What to do next

If you removed any DNS entries in `/etc/resolv.conf`, restore them.

The QRadar instance uses Coordinated Universal Time (UTC). You can change the time zone of the instance. For more information about changing the time zone, see Configuring system time.

This image does not receive automatic software upgrades. You must manually upgrade your system to keep it up to date. To receive QRadar upgrade notifications, see: Receiving QRadar update notifications

The QRadar Autoupdate server has changed since the release of QRadar 7.3.2 to update the auto update settings, see QRadar: Important auto update server changes for administrators (https://www.ibm.com/support/pages/qradar-important-auto-update-server-changes-administrators).

Important: IBM QRadar 7.3.2 has reached End of Support. To ensure that support is available, an upgrade must be performed. For information about upgrading to 7.4.3, see Upgrading QRadar SIEM.

Related concepts

"System requirements for virtual appliances" on page 24
To ensure that IBM QRadar works correctly, you must use virtual appliances that meet the minimum requirements.

"Common ports and servers used by QRadar" on page 122
IBM QRadar requires that certain ports are ready to receive information from QRadar components and external infrastructure. To ensure that QRadar is using the most recent security information, it also requires access to public servers and RSS feeds.

Configuring a QRadar managed host on Google Cloud Platform

Configure an IBM QRadar managed host on a Google Cloud Platform (GCP) instance by using the provided image.

Before you begin

Important:

The following procedure is for the configuration of an IBM QRadar 7.3.2 managed host image, which has reached its End of Support. An IBM® QRadar® 7.4.3 managed host image is not yet available. Once the image is installed, it should be upgraded to ensure that support is available. For information about upgrading to 7.4.3, see Upgrading QRadar SIEM.

You must acquire entitlement to a QRadar Software Node for any QRadar instance that is deployed from a third-party cloud marketplace. Entitlement to the software node should be in place before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with GCP infrastructure, refer to GCP documentation. If IBM Support determines that your issue is caused by the GCP infrastructure, you must contact GCP for support to resolve the underlying issue with the GCP infrastructure.

You must use static IP addresses.

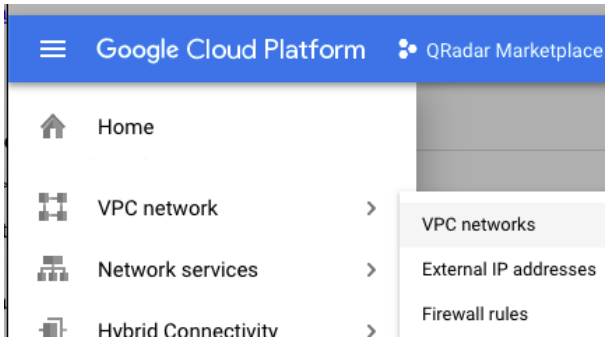
You cannot have more than two DNS entries. QRadar installation fails if you have more than two DNS entries in the `/etc/resolv.conf` file.

If you are installing a data gateway for QRadar on Cloud, go to Installing a QRadar data gateway in Google Cloud Platform (https://www.ibm.com/support/knowledgecenter/en/SSKMKU/com.ibm.qradar.doc_cloud/t_hosted_gcp_image.html).

1. Create a project name that allows for a fully qualified domain name (FQDN) to be no more than 63 characters long. The FQDN consists of the deployment name followed by "-vm", the zone, the region, the project name, and ".internal".

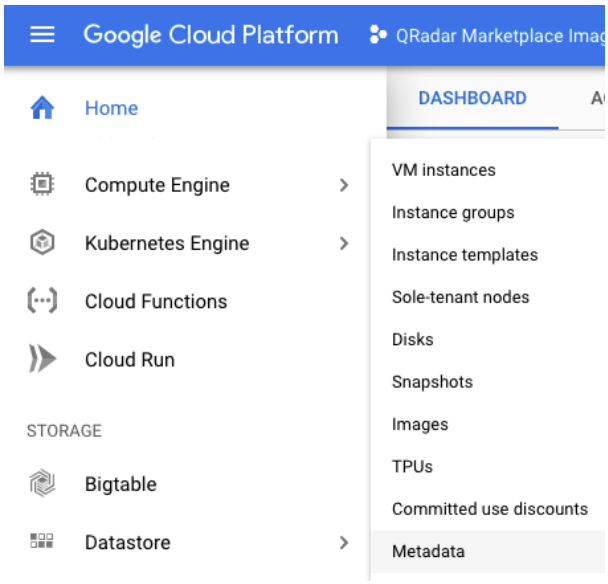
For example, if your project name is `abc-stq-xyz`, the appliance deployment name is `qr-con`, the zone is `us-east4-c`, and the region is `c`, the FQDN is `qr-con-vm.us-east4-c.c.abc-stq-xyz.internal`. The zone can be between 10 and 25 characters long. Depending on the zone, this leaves somewhere between 25 and 40 characters to be split between your project name and your deployment name.

2. In the project that you created in step 1, configure your network interface.
   a. Click **Google Cloud Platform** > **VPC network** > **VPC networks**.



©2019 Google LLC, used with permission. Google and the Google logo are registered trademarks of Google LLC.

   b. Click **CREATE VPC NETWORK**.
   c. Give your network a name, and configure the settings as needed. Set **DNS server policy** to **No server policy**.
   d. Click **Create**.
3. Add an SSH key to the project if you haven't already done so. The key must be created for a user called `cloud-user`.
   a. Click **Google Cloud Platform** > **Compute Engine** > **Metadata**.



©2019 Google LLC, used with permission. Google and the Google logo are registered trademarks of Google LLC.

   b. Click **SSH Keys**.
   c. Click **Edit**.
   d. Click **Add item**.
   e. Enter an SSH key, followed by `cloud-user`.
   f. Click **Save**.

Procedure

1. Go to QRadar Security Intelligence Platform Managed Host v7.3.2 P1 (https://console.cloud.google.com/marketplace/details/ibm-security-public/qradar-mh?q=IBM%20qradar&id=19dda1c2-9483-4ddc-a7bf-43e5e0d2fc01).
2. Click **LAUNCH**.
3. Set a deployment name for the appliance that allows for a fully qualified domain name (FQDN) to be no more than 63 characters long. The FQDN consists of the deployment name, the zone, the project name, and ".internal".

   For example, if your project name is `abc-stq-xyz`, the appliance deployment name is `qr-con`, the zone is `us-east4-c`, and the region is `c`, the FQDN is `qr-con-vm.us-east4-c.c.abc-stq-xyz.internal`. The zone can be between 10 and 25 characters long. Depending on the zone, this leaves somewhere between 25 and 40 characters to be split between your project name and your deployment name.
4. Select the zone that your project is in.
5. Select a **Machine Type** that meets the system requirements for virtual appliances.
6. Select the network interface that you created.
7. Set the firewall rules for your appliance that allow ports 22 and 443 only from trusted IP addresses to create an allowlist of IP addresses that can access your QRadar deployment.

   In a QRadar deployment with multiple appliances, other ports might also be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see “Common ports and servers used by QRadar” on page 122.
8. Check **I accept the GCP Marketplace Terms of Service**.
9. Click **Deploy**.
10. Set a static IP address for your appliance.
    a) Click **Google Cloud Platform** > **Compute Engine** > **VM instances**.
    b) Select your appliance from the list.
    c) Click **Edit**.
    d) Edit the network interface.
       - Set the **Internal IP type** parameter to **Static** and reserve a new IP address.
       - Select or create a static **External IP** address.
    e) Click **Done**.
11. When the instance is ready, log in using **SSH** and your key pair by typing the following command:

    ```
    ssh -i <key.pem> cloud-user@<public_IP_address>
    ```
12. Type the following command to check the length of your FQDN:

    ```
    hostname -f | wc -c
    ```

    If the command returns a value greater than 63 installation will fail. Restart this procedure with a shorter deployment name.
13. Type the following command for the virtual appliance that you're installing:

    ```
    sudo /root/setup_mh <appliance_type_id>
    ```

    For example, to deploy an Event Collector type the following command:

    ```
    sudo /root/setup_mh 1599
    ```

    You can install the following managed host appliance types:

Table 14. Appliance types	
Appliance type ID	**Appliance type**
1299	Flow Collector
1400	Data Node
1599	Event Collector
1699	Event Processor
1799	Flow Processor
1899	Event and Flow Processor

14. The system prompts you to set the root password. Set a strong password that meets the following criteria.
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.
15. Type the following command to restart the host and complete the installation:

    ```
    sudo reboot
    ```

16. Become the root user by typing the following command:

    ```
    sudo -i
    ```

17. Update the license file to address the issue described in APAR IJ30161 (https://www.ibm.com/support/pages/apar/IJ30161) by typing the following command:

    ```
    echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20"
    | tee /opt/qradar/ecs/license.txt /opt/ibm/si/
    services/ecs-ep/current/eventgnosis/license.txt /opt/ibm/si/services/ecs-ec-ingress/current/
    eventgnosis/license.txt /opt/ibm/si/services/ecs-ec/current/eventgnosis/license.txt /usr/
    eventgnosis/ecs/license.txt /opt/qradar/conf/templates/ecs_license.txt
    ```

18. Exit the superuser shell by typing the following command:

    ```
    exit
    ```

19. Add the host to your deployment in QRadar.
    a) On the navigation menu (☰), click **Admin**.
    b) In the **System Configuration** section, click **System and License Management**.
    c) In the **Display** list, select **Systems**.
    d) On the **Deployment Actions** menu, click **Add Host**.
    e) Configure the settings for the managed host by providing a static IP address, and the root password to access the operating system shell on the appliance.
    f) Click **Add**.
    g) Optional: Use the **Deployment actions** > **View Deployment** menu to see visualizations of your deployment. You can download a PNG image or a Microsoft Visio (2010) VDX file of your deployment visualization.
    h) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

    Important: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

What to do next

Important: IBM QRadar 7.3.2 has reached End of Support. To ensure that support is available, an upgrade must be performed. For information about upgrading to 7.4.3, see Upgrading QRadar SIEM.

Related concepts

"System requirements for virtual appliances" on page 24
To ensure that IBM QRadar works correctly, you must use virtual appliances that meet the minimum requirements.

"Common ports and servers used by QRadar" on page 122
IBM QRadar requires that certain ports are ready to receive information from QRadar components and external infrastructure. To ensure that QRadar is using the most recent security information, it also requires access to public servers and RSS feeds.

Configuring a QRadar App Host on Google Cloud Platform

Configure an IBM QRadar App Host on a Google Cloud Platform (GCP) instance by using the provided image.

Before you begin

Important:

The following procedure is for the configuration of an IBM QRadar 7.3.2 App Host image, which has reached its End of Support. An IBM® QRadar® 7.4.3 App Host image is not yet available. Once the image is installed, it should be upgraded to ensure that support is available. For information about upgrading to 7.4.3, see Upgrading QRadar SIEM.

You must acquire entitlement to a QRadar Software Node for any QRadar instance that is deployed from a third-party cloud marketplace. Entitlement to the software node should be in place before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with GCP infrastructure, refer to GCP documentation. If IBM Support determines that your issue is caused by the GCP infrastructure, you must contact GCP for support to resolve the underlying issue with the GCP infrastructure.

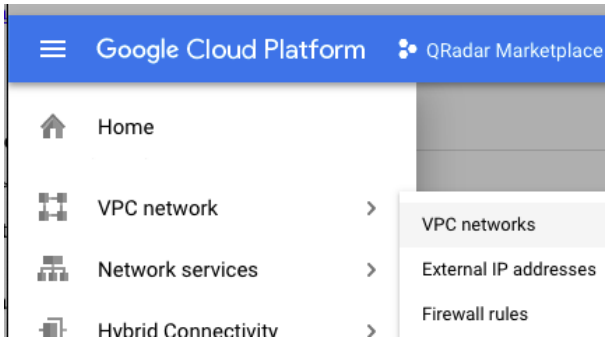
You must use static IP addresses.

You cannot have more than two DNS entries. QRadar installation fails if you have more than two DNS entries in the `/etc/resolv.conf` file.

If you are installing a data gateway for QRadar on Cloud, go to Installing a QRadar data gateway in Google Cloud Platform (https://www.ibm.com/support/knowledgecenter/en/SSKMKU/com.ibm.qradar.doc_cloud/t_hosted_gcp_image.html).

1. Create a project name that allows for a fully qualified domain name (FQDN) to be no more than 63 characters long. The FQDN consists of the deployment name followed by "-vm", the zone, the region, the project name, and ".internal".

   For example, if your project name is `abc-stq-xyz`, the appliance deployment name is `qr-con`, the zone is `us-east4-c`, and the region is `c`, the FQDN is `qr-con-vm.us-east4-c.c.abc-stq-xyz.internal`. The zone can be between 10 and 25 characters long. Depending on the zone, this leaves somewhere between 25 and 40 characters to be split between your project name and your deployment name.
2. In the project that you created in step 1, configure your network interface.
   a. Click **Google Cloud Platform** > **VPC network** > **VPC networks**.



©2019 Google LLC, used with permission. Google and the Google logo are registered trademarks of Google LLC.

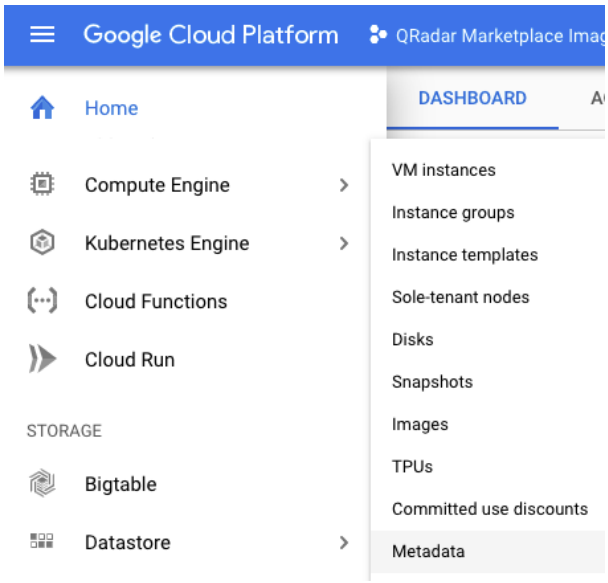
b. Click **CREATE VPC NETWORK**.

c. Give your network a name, and configure the settings as needed. Set **DNS server policy** to **No server policy**.

d. Click **Create**.

3. Add an SSH key to the project if you haven't already done so. The key must be created for a user called `cloud-user`.

a. Click **Google Cloud Platform** > **Compute Engine** > **Metadata**.



©2019 Google LLC, used with permission. Google and the Google logo are registered trademarks of Google LLC.

b. Click **SSH Keys**.

c. Click **Edit**.

d. Click **Add item**.

e. Enter an SSH key, followed by `cloud-user`.

f. Click **Save**.

Procedure

1. Go to QRadar Security Intelligence Platform App Host v7.3.2 P1 (https://console.cloud.google.com/marketplace/details/ibm-security-public/qradar-apphost?q=IBM%20qradar&id=181a7e9e-0ff5-483e-88d3-08c2cb353023).
2. Click **LAUNCH**.
3. Set a deployment name for the appliance that allows for a fully qualified domain name (FQDN) to be no more than 63 characters long. The FQDN consists of the deployment name, the zone, the project name, and ".internal".

For example, if your project name is `abc-stq-xyz`, the appliance deployment name is `qr-con`, the zone is `us-east4-c`, and the region is `c`, the FQDN is `qr-con-vm.us-east4-c.c.abc-stq-xyz.internal`. The zone can be between 10 and 25 characters long. Depending on the zone, this leaves somewhere between 25 and 40 characters to be split between your project name and your deployment name.

4. Select the zone that your project is in.
5. Select a **Machine Type** that meets the system requirements for virtual appliances.
6. Select the network interface that you created.
7. Set the firewall rules for your appliance that allow ports 22 and 443 only from trusted IP addresses to create an allowlist of IP addresses that can access your QRadar deployment.

   In a QRadar deployment with multiple appliances, other ports might also be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see "Common ports and servers used by QRadar" on page 122.
8. Check **I accept the GCP Marketplace Terms of Service**.
9. Click **Deploy**.
10. Set a static IP address for your appliance.
    a) Click **Google Cloud Platform** > **Compute Engine** > **VM instances**.
    b) Select your appliance from the list.
    c) Click **Edit**.
    d) Edit the network interface.
    - Set the **Internal IP type** parameter to **Static** and reserve a new IP address.
    - Select or create a static **External IP** address.

    e) Click **Done**.
11. When the instance is ready, log in using **SSH** and your key pair by typing the following command:

```
ssh -i <key.pem> cloud-user@<public_IP_address>
```

12. Type the following command to check the length of your FQDN:

```
hostname -f | wc -c
```

    If the command returns a value greater than 63 installation will fail. Restart this procedure with a shorter deployment name.
13. Ensure that there are no more than 2 DNS entries for the instance by typing the following command:

```
grep nameserver /etc/resolv.conf | wc -l
```

    If the command returns 3 or higher, edit `/etc/resolv.conf` to remove all but two of the entries before you proceed to the next step. You will add the entries back after installation is complete.
14. To install the App Host type the following command:

```
sudo /root/setup_apphost
```

15. The system prompts you to set the root password. Set a strong password that meets the following criteria.
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.
16. Type the following command to restart the host and complete the installation:

```
sudo reboot
```

17. Add the host to your deployment in QRadar.

a) On the navigation menu ( ), click **Admin**.

b) In the **System Configuration** section, click **System and License Management**.

c) In the **Display** list, select **Systems**.

d) On the **Deployment Actions** menu, click **Add Host**.

e) Configure the settings for the managed host by providing a static IP address, and the root password to access the operating system shell on the appliance.

f) Click **Add**.

g) Optional: Use the **Deployment actions** > **View Deployment** menu to see visualizations of your deployment. You can download a PNG image or a Microsoft Visio (2010) VDX file of your deployment visualization.

h) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

Important: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

18. Change where your apps are run in QRadar.

a) On the **System and License Management** screen, click the **Click to change where apps are run** link.

b) Click **App Host** to transfer apps to the App Host.

Note: The more apps and app data you have, the longer the transfer takes.

What to do next

If you removed any DNS entries in `/etc/resolv.conf`, restore them.

Important: IBM QRadar 7.3.2 has reached End of Support. To ensure that support is available, an upgrade must be performed. For information about upgrading to 7.4.3, see Upgrading QRadar SIEM.

Related concepts

"System requirements for virtual appliances" on page 24
To ensure that IBM QRadar works correctly, you must use virtual appliances that meet the minimum requirements.

"Common ports and servers used by QRadar" on page 122
IBM QRadar requires that certain ports are ready to receive information from QRadar components and external infrastructure. To ensure that QRadar is using the most recent security information, it also requires access to public servers and RSS feeds.

Configuring a Console on IBM Cloud

Configure an IBM QRadar SIEM Console on an IBM Cloud® instance by using the IBM Cloud image on Fix Central.

Before you begin

You must acquire entitlement to a QRadar Software Node before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with IBM Cloud infrastructure, refer to IBM Cloud documentation (https://cloud.ibm.com/docs). If IBM Support determines that your issue is caused by the IBM Cloud infrastructure, you must contact IBM Cloud for support to resolve the underlying issue.

About this task

You must use static IP addresses.

You cannot have more than two DNS entries. QRadar installation fails if you have more than two DNS entries in the `/etc/resolv.conf` file.

If you are installing a data gateway for QRadar on Cloud, go to Installing a QRadar data gateway in IBM Cloud (https://www.ibm.com/docs/en/SSKMKU/com.ibm.qradar.doc/t_hosted_IBM_Cloud.html).

Procedure

1. Download the `.vhd` image file.
   a) Go to the CLOUD MARKET PLACE section of Fix Central (https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.4.0&platform=Linux&function=all).
   b) Click **7.4.1-CMP-IBMCloud-CONSOLE-QRADAR-20200716115107**.
   c) Download the `.vhd` and `.sig` files.
      The `.vhd` file download can take several hours.
2. Upload the `.vhd` image file.
   a) Go to IBM Cloud (https://cloud.ibm.com/) and create a new storage bucket.
      You need the location that is used by your storage bucket, and the IBM Cloud API Key for your storage bucket, in step 3.
   b) Upload the `.vhd` file.
      The upload can take up to an hour. Do not rename the `.vhd` file. Renaming the file causes the import to fail.
3. Import the `.vhd` image.
   a) In IBM Cloud, click **Navigation Menu (☰)** > **Classic Infrastructure** > **Manage** > **Images**.
   b) Click **Import custom image**.
   c) Enter a name for the image and the IBM Cloud API Key for your storage bucket.
   d) Select the Cloud Object Storage service instance, the location that is used by your storage bucket, your storage bucket, and the `.vhd` file that you uploaded.
   e) Select **RedHat EL 7.0 minimal (64-bit)**.
   f) From the **Boot mode** menu, select **Hardware Virtual Machine (HVM)**.
   g) Check **Your license** and **Cloud-init**.
   h) Click **Import image**.
      The import can take up to 15 minutes.
4. Configure network settings and create the instance.
   a) Click **Navigation Menu (☰)** > **Classic Infrastructure** > **Manage** > **Images**.
   b) In the **Visibility** menu, select **Private images** and find the image that you uploaded.
   c) Click **Actions menu (⋮)** > **Order Public VSI**.
   d) Select the **Public Multi-tenant** virtual server type.
   e) Enter a hostname and domain. The combined character count of the hostname and domain cannot exceed 64 characters.
   f) Select a data center location.
   g) Select a profile that meets the system requirements for virtual appliances.
      Important: Profiles from the **Balanced local storage** family are not supported.
   h) Select an SSH key if you have one. Otherwise, select **None**.

i) Choose an uplink port speed under **Public & Private** network uplinks.

You can choose to deploy either a public machine or a private machine.

- Public machines have a public IP address and a private IP address, and they are accessible from the internet.
- Private machines have only a private IP address, and can only be accessed within the same network, or through a routing solution of your own choosing.

j) Select **allow_all** and **allow_outbound** for a private security group. If you are deploying a public machine, select **allow_all** and **allow_outbound** for a public security group too.

In a QRadar deployment with multiple appliances, many ports must be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see "Common ports and servers used by QRadar" on page 122. Restrict ports that are not needed by using a firewall or other technology that allows you to restrict ports.

k) Accept the third-party service agreements and click **Create**.

The **Devices** screen loads. In a few minutes, a date appears in the **Start Date** field.

5. After the instance has a **Start Date**, configure storage for the instance.

a) Click **Navigation Menu (☰)** > **Classic Infrastructure** > **Block Storage**.

b) In the **Portable storage** section, click **Order Portable Storage**.

c) Select the same Region, Location, and Zone for your portable storage that your instance is in.

d) Enter a description for your portable storage.

e) Estimate your storage needs and enter a size for the second disk in GB.

The minimum size is 250 GB. The added disk must be the second disk. It cannot be the third or greater disk.

When the installation is complete, this disk contains the `/store` and `/transient` partitions.

Warning: You cannot increase storage after installation.

f) Accept the service agreement and click **Create**.

The second disk is added and the instance restarts. This process takes several minutes.

6. Attach storage to your instance.

a) Click **Navigation Menu (☰)** > **Classic Infrastructure** > **Block Storage**.

b) In the **Portable storage** section, find the disk that you created and click **Actions menu (⋮)** > **Attach**.

c) Find the instance that you created and click **Attach**.

d) Accept the warning that the virtual server will be shut off during disk attachment and click **Attach**.

The second disk is added and the instance restarts. This process takes several minutes.

7. Install the Console and set the admin password.

a) When the instance is ready, log in by typing the following command:

```
ssh root@<public_IP_address>
```

If you are not using an SSH key, you are prompted to enter the root password. This password is provided in your instance details.

If you deployed a private-only Console, you will not be able to SSH directly to the Console. You must first connect to a router that allows access to the Console.

b) To install the Console, type the following command:

```
sudo /root/setup_console
```

c) Enter a password for the admin account. Set a strong password that meets the following criteria.

- Contains at least 5 characters
- Contains no spaces
- Includes one or more of the following special characters: @, #, ^, and *.

d) Become the root user by typing the following command:

```
sudo -i
```

e) Update the license file to address the issue described in APAR IJ30161 (https://www.ibm.com/support/pages/apar/IJ30161) by typing the following command:

```
echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20"
| tee /opt/qradar/ecs/license.txt /opt/ibm/si/services/
ecs-ep/current/eventgnosis/license.txt /opt/ibm/si/services/ecs-ec-ingress/current/
eventgnosis/license.txt /opt/ibm/si/services/ecs-ec/current/eventgnosis/license.txt /usr/
eventgnosis/ecs/license.txt /opt/qradar/conf/templates/ecs_license.txt
```

It takes approximately 5 minutes for the changes to complete.

f) Restart your instance by typing the following command:

```
reboot
```

You can access your IBM QRadar SIEM Console by going to https://*<public_IP_address>* and logging in as the `admin` user.

For a private-only Console, you will need to use the public IP address configured in your routing solution in order to access the Console.

If you will be attaching any managed hosts to your Console that are not in the same network as the Console, you must configure a Network Address Translation (NAT) group .

a. On the **Admin** tab, click **System & License Management**.
b. Select your Console.
c. On the **Deployment Actions** menu, click **Edit Host**.
d. Select the **Network Address Translation** check box.
e. Select or create a NAT group for the Console. Provide the routed public IP address for the Console and click **Save**.
f. On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

What to do next

If you removed any DNS entries in `/etc/resolv.conf`, restore them.

The QRadar instance uses Coordinated Universal Time (UTC). You can change the time zone of the instance. For more information about changing the time zone, see Configuring system time.

This image does not receive automatic software upgrades. You must manually upgrade your system to keep it up to date. To receive QRadar upgrade notifications, see: Receiving QRadar update notifications

Configuring a managed host on IBM Cloud

Configure an IBM QRadar managed host on an IBM Cloud instance by using the provided IBM Cloud image.

Before you begin

You must acquire entitlement to a QRadar Software Node before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with IBM Cloud infrastructure, refer to IBM Cloud documentation (https://cloud.ibm.com/docs). If IBM Support

determines that your issue is caused by the IBM Cloud infrastructure, you must contact IBM Cloud for support to resolve the underlying issue.

About this task

You must use static IP addresses.

You cannot have more than two DNS entries. QRadar installation fails if you have more than two DNS entries in the `/etc/resolv.conf` file.

If you are installing a data gateway for QRadar on Cloud, go to Installing a QRadar data gateway in IBM Cloud (https://www.ibm.com/docs/en/SSKMKU/com.ibm.qradar.doc/t_hosted_IBM_Cloud.html).

Procedure

1. Download the `.vhd` image file.
   a) Go to the CLOUD MARKET PLACE section of Fix Central (https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.4.0&platform=Linux&function=all).
   b) Choose a public managed host or a private managed host.
      - For a public managed host, click **7.4.1-CMP-IBMCloud-MANAGEDHOST-QRADAR-20200716115107**. Public hosts have a public IP address and a private IP address. You must use the public IP address to attach this host to the Console in step 7 d.
      - For a private managed host, click **7.4.1-CMP-IBMCloud-MANAGEDHOST-PRIVATE-QRADAR-QRSIEM-20200716115107**. Private hosts have only a private IP address, and can only be accessed within the same network, or through a routing solution of your own choosing. You will need both the routed public IP address and the private IP address to attach this host to your Console in step 7 d.
   c) Download the `.vhd` and `.sig` files.
      The `.vhd` file download can take several hours.
2. Upload the `.vhd` image file.
   a) Go to IBM Cloud (https://cloud.ibm.com/) and create a new storage bucket.
      You need the location that is used by your storage bucket, and the IBM Cloud API Key for your storage bucket, in step 3.
   b) Upload the `.vhd` file.
      The upload can take up to an hour. Do not rename the `.vhd` file. Renaming the file causes the import to fail.
3. Import the `.vhd` image.
   a) In IBM Cloud, click **Navigation Menu (☰)** > **Classic Infrastructure** > **Manage** > **Images**.
   b) Click **Import custom image**.
   c) Enter a name for the image and the IBM Cloud API Key for your storage bucket.
   d) Select the Cloud Object Storage service instance, the location that is used by your storage bucket, your storage bucket, and the `.vhd` file that you uploaded.
   e) Select **RedHat EL 7.0 minimal (64-bit)**.
   f) From the **Boot mode** menu, select **Hardware Virtual Machine (HVM)**.
   g) Check **Your license** and **Cloud-init**.
   h) Click **Import image**.
      The import can take up to 15 minutes.
4. Configure network settings and create the instance.
   a) Click **Navigation Menu (☰)** > **Classic Infrastructure** > **Manage** > **Images**.

b) In the **Visibility** menu, select **Private images** and find the image that you uploaded.

For a public managed host, you must choose the public managed host image. For a private managed host, you must choose the private managed host image.

c) Click **Actions menu ( ) > Order Public VSI**.

d) Select the **Public Multi-tenant** virtual server type.

e) Enter a hostname and domain. The combined character count of the hostname and domain cannot exceed 64 characters.

f) Select a data center location.

g) Select a profile that meets the system requirements for virtual appliances.

Important: Profiles from the **Balanced local storage** family are not supported.

h) Select an SSH key if you have one. Otherwise, select **None**.

i) Choose an uplink port speed under **Public & Private** network uplinks.

You can choose to deploy either a public machine or a private machine. The network configuration of this host must match your Console. If your Console is public, this host must also be public. If your Console is private, this host must also be private.

- Public machines have a public IP address and a private IP address, and they are accessible from the internet. You must use the public IP address to attach this host to your Console.
- Private machines have only a private IP address, and can only be accessed within the same network, or through a routing solution of your own choosing.

j) Select **allow_all** and **allow_outbound** for a private security group. If you are deploying a public machine, select **allow_all** and **allow_outbound** for a public security group too.

In a QRadar deployment with multiple appliances, many ports must be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see "Common ports and servers used by QRadar" on page 122. Restrict ports that are not needed by using a firewall or other technology that allows you to restrict ports.

k) Accept the third-party service agreements and click **Create**.

The **Devices** screen loads. In a few minutes, a date appears in the **Start Date** field.

5. After the instance has a **Start Date**, configure storage for the instance.

a) Click **Navigation Menu ( ) > Classic Infrastructure > Block Storage**.

b) In the **Portable storage** section, click **Order Portable Storage**.

c) Select the same Region, Location, and Zone for your portable storage that your instance is in.

d) Enter a description for your portable storage.

e) Estimate your storage needs and enter a size for the second disk in GB.

The minimum size is 250 GB. The added disk must be the second disk. It cannot be the third or greater disk.

When the installation is complete, this disk contains the `/store` and `/transient` partitions.

Warning: You cannot increase storage after installation.

f) Accept the service agreement and click **Create**.

The second disk is added and the instance restarts. This process takes several minutes.

6. Attach storage to your instance.

a) Click **Navigation Menu ( ) > Classic Infrastructure > Block Storage**.

b) In the **Portable storage** section, find the disk that you created and click **Actions menu ( ) > Attach**.

c) Find the instance that you created and click **Attach**.

d) Accept the warning that the virtual server will be shut off during disk attachment and click **Attach**.

The second disk is added and the instance restarts. This process takes several minutes.

7. Install the managed host and set the admin password.
   a) When the instance is ready, log in by typing the following command:

   ```
   ssh root@<public_IP_address>
   ```

   If you are not using an SSH key, you are prompted to enter the root password. This password is provided in your instance details.

   If you deployed a private-only host, you will not be able to SSH directly to the host. You must first connect to a router that allows access to the host.

   b) Type the following command for the managed host that you're installing:

   ```
   sudo /root/setup_mh <appliance_type_id>
   ```

   For example, to deploy an Event Collector type the following command:

   ```
   sudo /root/setup_mh 1599
   ```

   You can install the following managed host appliance types:

   Table 15. Appliance types

Appliance type ID	Appliance type
1299	Flow Collector
1400	Data Node
1599	Event Collector
1699	Event Processor
1799	Flow Processor
1899	Event and Flow Processor

   c) The system prompts you to set the root password. Set a strong password that meets the following criteria.

   - Contains at least 5 characters
   - Contains no spaces
   - Includes one or more of the following special characters: @, #, ^, and *.

   d) Update the license file to address the issue described in APAR IJ30161 (https://www.ibm.com/support/pages/apar/IJ30161) by typing the following command:

   ```
   echo -n “QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20”
   | tee /opt/qradar/ecs/license.txt /opt/ibm/si/services/
   ecs-ep/current/eventgnosis/license.txt /opt/ibm/si/services/ecs-ec-ingress/current/
   eventgnosis/license.txt /opt/ibm/si/services/ecs-ec/current/eventgnosis/license.txt /usr/
   eventgnosis/ecs/license.txt /opt/qradar/conf/templates/ecs_license.txt
   ```

   It takes approximately 5 minutes for the changes to complete.

   e) Restart your instance by typing the following command:

   ```
   reboot
   ```

8. Add the host to your deployment in QRadar.
   a) On the navigation menu (☰), click **Admin**.
   b) In the **System Configuration** section, click **System and License Management**.
   c) In the **Display** list, select **Systems**.

d) On the **Deployment Actions** menu, click **Add Host**.

e) Configure the settings for the host by providing the public IP address, and the root password to access the operating system shell on the appliance.

- For a public host, provide the public IP address, and the root password to access the operating system shell on the appliance.
- For a private host, provide the private IP address and the root password. If your host is in a different network from your Console, select **NAT**. Select or create a NAT group for non-Consoles and provide the public IP address that you routed to the host.

f) Click **Add**.

g) Optional: Use the **Deployment actions** > **View Deployment** menu to see visualizations of your deployment. You can download a PNG image or a Microsoft Visio (2010) VDX file of your deployment visualization.

h) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

Important: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

What to do next

If you removed any DNS entries in `/etc/resolv.conf`, restore them.

The QRadar instance uses Coordinated Universal Time (UTC). You can change the time zone of the instance. For more information about changing the time zone, see Configuring system time.

This image does not receive automatic software upgrades. You must manually upgrade your system to keep it up to date. To receive QRadar upgrade notifications, see: Receiving QRadar update notifications

Configuring an App Host on IBM Cloud

Configure an IBM QRadar App Host on IBM Cloud instance by using the provided IBM Cloud image.

Before you begin

You must acquire entitlement to a QRadar Software Node before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with IBM Cloud infrastructure, refer to IBM Cloud documentation (https://cloud.ibm.com/docs). If IBM Support determines that your issue is caused by the IBM Cloud infrastructure, you must contact IBM Cloud for support to resolve the underlying issue.

About this task

You must use static IP addresses.

You cannot have more than two DNS entries. QRadar installation fails if you have more than two DNS entries in the `/etc/resolv.conf` file.

If you are installing a data gateway for QRadar on Cloud, go to Installing a QRadar data gateway in IBM Cloud (https://www.ibm.com/docs/en/SSKMKU/com.ibm.qradar.doc/t_hosted_IBM_Cloud.html).

Procedure

1. Download the `.vhd` image file.

a) Go to the CLOUD MARKET PLACE section of Fix Central (https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.4.0&platform=Linux&function=all).

b) Click **7.4.1-CMP-IBMCloud-APPHOST-QRADAR-20200716115107**.

c) Download the `.vhd` and `.sig` files.

The `.vhd` file download can take several hours.

2. Upload the `.vhd` image file.

a) Go to IBM Cloud (https://cloud.ibm.com/) and create a new storage bucket.

You need the location that is used by your storage bucket, and the IBM Cloud API Key for your storage bucket, in step 3.

b) Upload the `.vhd` file.

The upload can take up to an hour. Do not rename the `.vhd` file. Renaming the file causes the import to fail.

3. Import the `.vhd` image.

a) In IBM Cloud, click **Navigation Menu ( )** > **Classic Infrastructure** > **Manage** > **Images**.

b) Click **Import custom image**.

c) Enter a name for the image and the IBM Cloud API Key for your storage bucket.

d) Select the Cloud Object Storage service instance, the location that is used by your storage bucket, your storage bucket, and the `.vhd` file that you uploaded.

e) Select **RedHat EL 7.0 minimal (64-bit)**.

f) From the **Boot mode** menu, select **Hardware Virtual Machine (HVM)**.

g) Check **Your license** and **Cloud-init**.

h) Click **Import image**.

The import can take up to 15 minutes.

4. Configure network settings and create the instance.

a) Click **Navigation Menu ( )** > **Classic Infrastructure** > **Manage** > **Images**.

b) In the **Visibility** menu, select **Private images** and find the image that you uploaded.

c) Click **Actions menu ( )** > **Order Public VSI**.

d) Select the **Public Multi-tenant** virtual server type.

e) Enter a hostname and domain. The combined character count of the hostname and domain cannot exceed 64 characters.

f) Select a data center location.

g) Select a profile that meets the system requirements for virtual appliances.

Important: Profiles from the **Balanced local storage** family are not supported.

h) Select an SSH key if you have one. Otherwise, select **None**.

i) Choose an uplink port speed under **Public & Private** network uplinks.

You can choose to deploy either a public machine or a private machine. The network configuration of this host must match your Console. If your Console is public, this host must also be public. If your Console is private, this host must also be private.

- Public machines have a public IP address and a private IP address, and they are accessible from the internet. You must use the public IP address to attach this host to your Console in step 7 d.
- Private machines have only a private IP address, and can only be accessed within the same network, or through a routing solution of your own choosing. You will need both the routed public IP address and the private IP address to attach this host to your Console in step 7 d.

j) Select **allow_all** and **allow_outbound** for a private security group. If you are deploying a public machine, select **allow_all** and **allow_outbound** for a public security group too.

In a QRadar deployment with multiple appliances, many ports must be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see "Common ports and servers used by QRadar" on page 122. Restrict ports that are not needed by using a firewall or other technology that allows you to restrict ports.

k) Accept the third-party service agreements and click **Create**.

The **Devices** screen loads. In a few minutes, a date appears in the **Start Date** field.

5. After the instance has a **Start Date**, configure storage for the instance.

   a) Click **Navigation Menu (☰)** > **Classic Infrastructure** > **Block Storage**.

   b) In the **Portable storage** section, click **Order Portable Storage**.

   c) Select the same Region, Location, and Zone for your portable storage that your instance is in.

   d) Enter a description for your portable storage.

   e) Estimate your storage needs and enter a size for the second disk in GB.

   The minimum size is 250 GB. The added disk must be the second disk. It cannot be the third or greater disk.

   When the installation is complete, this disk contains the `/store` and `/transient` partitions.

   Warning: You cannot increase storage after installation.

   f) Accept the service agreement and click **Create**.

   The second disk is added and the instance restarts. This process takes several minutes.

6. Attach storage to your instance.

   a) Click **Navigation Menu (☰)** > **Classic Infrastructure** > **Block Storage**.

   b) In the **Portable storage** section, find the disk that you created and click **Actions menu ( )** > **Attach**.

   c) Find the instance that you created and click **Attach**.

   d) Accept the warning that the virtual server will be shut off during disk attachment and click **Attach**.

   The second disk is added and the instance restarts. This process takes several minutes.

7. Install the App Host and set the admin password.

   a) When the instance is ready, log in by typing the following command:

   ```
   ssh root@<public_IP_address>
   ```

   If you are not using an SSH key, you are prompted to enter the root password. This password is provided in your instance details.

   If you deployed a private-only host, you will not be able to SSH directly to the host. You must first connect to a router that allows access to the host.

   b) To install the App Host, type the following command:

   ```
   sudo /root/setup_apphost
   ```

   c) The system prompts you to set the root password. Set a strong password that meets the following criteria.

   - Contains at least 5 characters
   - Contains no spaces
   - Includes one or more of the following special characters: @, #, ^, and *.

   d) Update the license file to address the issue described in APAR IJ30161 (https://www.ibm.com/support/pages/apar/IJ30161) by typing the following command:

   ```
   echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20"
   | tee /opt/qradar/ecs/license.txt /opt/ibm/si/services/
   ```

```
ecs-ep/current/eventgnosis/license.txt /opt/ibm/si/services/ecs-ec-ingress/current/
eventgnosis/license.txt /opt/ibm/si/services/ecs-ec/current/eventgnosis/license.txt /usr/
eventgnosis/ecs/license.txt /opt/qradar/conf/templates/ecs_license.txt
```

It takes approximately 5 minutes for the changes to complete.

e) Restart your instance by typing the following command:

```
reboot
```

8. Add the host to your deployment in QRadar.

a) On the navigation menu (☰), click **Admin**.

b) In the **System Configuration** section, click **System and License Management**.

c) In the **Display** list, select **Systems**.

d) On the **Deployment Actions** menu, click **Add Host**.

e) Configure the settings for the App Host by providing the public IP address, and the root password to access the operating system shell on the appliance.

- For a public host, provide the public IP address, and the root password to access the operating system shell on the appliance.
- For a private host, provide the private IP address and the root password. If your host is in a different network from your Console, select **NAT**. Select or create a NAT group for non-Consoles and provide the public IP address that you routed to the host.

f) Click **Add**.

g) Optional: Use the **Deployment actions** > **View Deployment** menu to see visualizations of your deployment. You can download a PNG image or a Microsoft Visio (2010) VDX file of your deployment visualization.

h) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

Important: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

9. Change where your apps are run in QRadar.

a) On the **System and License Management** screen, click the **Click to change where apps are run** link.

b) Click **App Host** to transfer apps to the App Host.

Note: The more apps and app data you have, the longer the transfer takes.

Configuring a Console on IBM Cloud VPC

Configure an IBM QRadar SIEM Console on an IBM Cloud VPC Server instance by using the IBM Cloud VPC image on Fix Central.

Before you begin

You must acquire entitlement to a QRadar Software Node before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with IBM Cloud VPC infrastructure, refer to IBM Cloud VPC documentation (https://cloud.ibm.com/docs). If IBM Support determines that your issue is caused by the IBM Cloud VPC infrastructure, you must contact IBM Cloud for support to resolve the underlying issue.

About this task

If you are installing a data gateway for QRadar on Cloud, go to Installing a QRadar data gateway in IBM Cloud (https://www.ibm.com/docs/en/SSKMKU/com.ibm.qradar.doc/t_hosted_IBM_Cloud_VPC.html).

You must use static IP addresses.

If you deploy a managed host and a Console in the same virtual network, use the private IP address of the managed host to add it to the Console.

If you deploy a managed host and a Console in different virtual networks, you must allow firewall rules for the communication between the Console and the managed host. For more information, see "QRadar port usage " on page 122.

Procedure

1. Download the `.qcow2` image file.
   a) Go to the CLOUD MARKET PLACE section of Fix Central (https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.4.0&platform=Linux&function=all).
   b) Click **7.4.3-CMP-IBMCloudVPC-CONSOLE-QRADAR-20220329114452**.
   c) Download the `.qcow2` and `.sig` files.
      The `.qcow2` file download can take several hours.
   d) Use the `.sig` file to verify the integrity of the `.qcow2` file.
      For more information, see How to verify downloads from IBM Fix Central are trusted and code signed.
2. Upload the `.qcow2` image file.
   a) Go to IBM Cloud (https://cloud.ibm.com/) and create a new storage bucket.
      You need the location that is used by your storage bucket in step 3.
   b) Upload the `.qcow2` file.
      The upload can take up to an hour. Do not rename the `.qcow2` file. Renaming the file causes the import to fail.
3. Import the `.qcow2` file.
   a) In IBM Cloud, click ☰ > **VPC Infrastructure** > **Custom images**.
   b) Click **Create**.
   c) Enter a name for the image and select a **Resource group** for the image to belong to.
   d) Set the **Source** to **Cloud Object Storage**.
   e) Select the Cloud Object Storage service instance, the location that is used by your storage bucket, your storage bucket, and the `.qcow2` file that you uploaded.
      Note: If you want to import your image into multiple regions, you will have to repeat step 2 and create a new storage bucket in each desired region.
   f) Set the **Operating system** to **Red Hat Enterprise Linux**, and set the **Version** to **red-7-amd64-byol**.
   g) Click **Create custom image**.
      The import can take up to 10 minutes.
4. After the image status is `Available`, create the instance.
   a) Click ☰ > **VPC Infrastructure** > **Virtual Server Instances**.
   b) Click **Create +**.
   c) Set the **Architecture** to **Intel**.
   d) Set the **Hosting type** to **Public**.
   e) Set the location to the same region that you imported your image to in step 3.

f) Give your instance a name that doesn't exceed 57 characters.
The name can contain only alphanumeric characters and the - symbol.

g) Select a **Resource group** for the instance.

h) If you would like an easier way to identify your instance, enter a tag for your instance.

i) Set the **Operating system** to **Custom image**.
The **Select custom image** window appears.

j) Choose the image that you imported in step 3, then click **Select**.

k) Click **View all profiles**.
The **Select an instance profile** window appears.

l) Select a profile that meets the system requirements for virtual appliances, then click **Save**.

Important: Instances that use Instance storage are not supported.

m) Select or create an SSH key pair.
You need an SSH key pair to access the instance by using SSH.

n) In the **Data volumes** section, click **Create +**.

o) Enter a **Name** for the second disk.

p) Estimate your storage needs and enter a size for the second disk in GB.
The minimum size is 250 GB. The added disk must be the second disk. It cannot be the third or greater disk.

When the installation is complete, this disk contains the `/store` and `/transient` partitions.

Warning: You cannot increase storage after installation.

q) Select a profile, set the IOPS, and click **Create**.

r) Select a **Virtual private cloud**.

s) In the **Network interfaces** section, click the  icon next to **eth0**.

t) Leave the **interface** set to **eth0** and select a **Subnet**.

u) Set **Reserving method** to **Let me specify** and select a reserved private IP address from your subnet.
This IP address will be the private IP address associated with your instance.

v) Select a security group that allows ports 22 and 443 only from trusted IP addresses, then click **Save**.
In a QRadar deployment with multiple appliances, other ports might also be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see “Common ports and servers used by QRadar” on page 122.

w) Click **Create Virtual Server**.

5. When the instance status says `Running`, assign a floating IP address to your instance.

a) Click on the instance that you created.

b) In the **Network interfaces** section, click the  icon next to **eth0**.

c) Select an IP address or **Reserve a new floating IP** from the **Floating IP address** dropdown, then click **Save**.

6. Install the Console and set the admin password.

a) When the floating IP address is assigned, log in by typing the following command:

```
ssh -i <private_key> cloud-user@<public_IP_address>
```

b) To install the Console, type the following command:

```
sudo /root/setup_console
```

c) Enter a password for the admin account. Set a strong password that meets the following criteria.

- Contains at least 5 characters
- Contains no spaces
- Includes one or more of the following special characters: `@`, `#`, ^, and `*`.

You can access your IBM QRadar SIEM Console by going to https://*<fixed_IP_address>* and logging in as the `admin` user.

What to do next

The QRadar instance uses Coordinated Universal Time (UTC). You can change the time zone of the instance. For more information about changing the time zone, see Configuring system time.

This image does not receive automatic software upgrades. You must manually upgrade your system to keep it up to date. To receive QRadar upgrade notifications, see: Receiving QRadar update notifications

Configuring a managed host on IBM Cloud VPC

Configure an IBM QRadar managed host on an IBM Cloud VPC Server instance by using the IBM Cloud VPC image on Fix Central.

Before you begin

You must acquire entitlement to a QRadar Software Node before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with IBM Cloud VPC infrastructure, refer to IBM Cloud VPC documentation (https://cloud.ibm.com/docs). If IBM Support determines that your issue is caused by the IBM Cloud VPC infrastructure, you must contact IBM Cloud for support to resolve the underlying issue.

About this task

If you are installing a data gateway for QRadar on Cloud, go to Installing a QRadar data gateway in IBM Cloud (https://www.ibm.com/docs/en/SSKMKU/com.ibm.qradar.doc/t_hosted_IBM_Cloud_VPC.html).

You must use static IP addresses.

If you deploy a managed host and a Console in the same virtual network, use the private IP address of the managed host to add it to the Console.

If you deploy a managed host and a Console in different virtual networks, you must allow firewall rules for the communication between the Console and the managed host. For more information, see “QRadar port usage ” on page 122.

Procedure

1. Download the `.qcow2` image file.
   a) Go to the CLOUD MARKET PLACE section of Fix Central (https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.4.0&platform=Linux&function=all).
   b) Click **7.4.3-CMP-IBMCloudVPC-MH-QRADAR-20220329114452**.
   c) Download the `.qcow2` and `.sig` files.
      The `.qcow2` file download can take several hours.
   d) Use the `.sig` file to verify the integrity of the `.qcow2` file.
      For more information, see How to verify downloads from IBM Fix Central are trusted and code signed.
2. Upload the `.qcow2` image file.

a) Go to IBM Cloud (https://cloud.ibm.com/) and create a new storage bucket.

You need the location that is used by your storage bucket in step 3.

b) Upload the `.qcow2` file.

The upload can take up to an hour. Do not rename the `.qcow2` file. Renaming the file causes the import to fail.

3. Import the `.qcow2` file.

a) In IBM Cloud, click ☰ > **VPC Infrastructure** > **Custom images**.

b) Click **Create**.

c) Enter a name for the image and select a **Resource group** for the image to belong to.

d) Set the **Source** to **Cloud Object Storage**.

e) Select the Cloud Object Storage service instance, the location that is used by your storage bucket, your storage bucket, and the `.qcow2` file that you uploaded.

Note: If you want to import your image into multiple regions, you will have to repeat step 2 and create a new storage bucket in each desired region.

f) Set the **Operating system** to **Red Hat Enterprise Linux**, and set the **Version** to **red-7-amd64-byol**.

g) Click **Create custom image**.

The import can take up to 10 minutes.

4. After the image status is `Available`, create the instance.

a) Click ☰ > **VPC Infrastructure** > **Virtual Server Instances**.

b) Click **Create +**.

c) Set the **Architecture** to **Intel**.

d) Set the **Hosting type** to **Public**.

e) Set the location to the same region that you imported your image to in step 3.

f) Give your instance a name that doesn't exceed 57 characters.

The name can contain only alphanumeric characters and the - symbol.

g) Select a **Resource group** for the instance.

h) If you would like an easier way to identify your instance, enter a tag for your instance.

i) Set the **Operating system** to **Custom image**.

The **Select custom image** window appears.

j) Choose the image that you imported in step 3, then click **Select**.

k) Click **View all profiles**.

The **Select an instance profile** window appears.

l) Select a profile that meets the system requirements for virtual appliances, then click **Save**.

Important: Instances that use Instance storage are not supported.

m) Select or create an SSH key pair.

You need an SSH key pair to access the instance by using SSH.

n) In the **Data volumes** section, click **Create +**.

o) Enter a **Name** for the second disk.

p) Estimate your storage needs and enter a size for the second disk in GB.

The minimum size is 250 GB. The added disk must be the second disk. It cannot be the third or greater disk.

When the installation is complete, this disk contains the `/store` and `/transient` partitions.

Warning: You cannot increase storage after installation.

q) Select a profile, set the IOPS, and click **Create**.

r) Select a **Virtual private cloud**.

s) In the **Network interfaces** section, click the icon next to **eth0**.

t) Leave the **interface** set to **eth0** and select a **Subnet**.

u) Set **Reserving method** to **Let me specify** and select a reserved private IP address from your subnet.

This IP address will be the private IP address associated with your instance.

v) Select a security group that allows ports 22 and 443 only from trusted IP addresses, then click **Save**.

In a QRadar deployment with multiple appliances, other ports might also be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see "Common ports and servers used by QRadar" on page 122.

w) Click **Create Virtual Server**.

5. When the instance status says Running, assign a floating IP address to your instance.

a) Click on the instance that you created.

b) In the **Network interfaces** section, click the icon next to **eth0**.

c) Select an IP address or **Reserve a new floating IP** from the **Floating IP address** dropdown, then click **Save**.

6. Install the managed host and set the root password.

a) When the floating IP address is assigned, log in by typing the following command:

```
ssh -i <private_key> cloud-user@<public_IP_address>
```

b) Type the following command for the managed host that you're installing:

```
sudo /root/setup_mh <appliance_type_id>
```

For example, to deploy an Event Collector type the following command:

```
sudo /root/setup_mh 1599
```

You can install the following managed host appliance types:

Table 16. Appliance types

Appliance type ID	Appliance type
1299	Flow Collector
1400	Data Node
1599	Event Collector
1699	Event Processor
1799	Flow Processor
1899	Event and Flow Processor

c) The system prompts you to set the root password. Set a strong password that meets the following criteria.

- Contains at least 5 characters
- Contains no spaces
- Includes one or more of the following special characters: @, #, ^, and *.

7. Add the host to your deployment in QRadar.

a) On the navigation menu ( ), click **Admin**.

b) In the **System Configuration** section, click **System and License Management**.

c) In the **Display** list, select **Systems**.

d) On the **Deployment Actions** menu, click **Add Host**.

e) Configure the settings for the host by providing the fixed IP address, and the root password to access the operating system shell on the appliance.

f) Click **Add**.

g) Optional: Use the **Deployment actions** > **View Deployment** menu to see visualizations of your deployment. You can download a PNG image or a Microsoft Visio (2010) VDX file of your deployment visualization.

h) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

Important: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

Configuring an App Host on IBM Cloud VPC

Configure an IBM QRadar App Host on an IBM Cloud VPC Server instance by using the IBM Cloud VPC image on Fix Central.

Before you begin

You must acquire entitlement to a QRadar Software Node before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with IBM Cloud VPC infrastructure, refer to IBM Cloud VPC documentation (https://cloud.ibm.com/docs). If IBM Support determines that your issue is caused by the IBM Cloud VPC infrastructure, you must contact IBM Cloud for support to resolve the underlying issue.

About this task

If you are installing a data gateway for QRadar on Cloud, go to Installing a QRadar data gateway in IBM Cloud (https://www.ibm.com/docs/en/SSKMKU/com.ibm.qradar.doc/t_hosted_IBM_Cloud_VPC.html).

You must use static IP addresses.

If you deploy a managed host and a Console in the same virtual network, use the private IP address of the managed host to add it to the Console.

If you deploy a managed host and a Console in different virtual networks, you must allow firewall rules for the communication between the Console and the managed host. For more information, see “QRadar port usage ” on page 122.

Procedure

1. Download the `.qcow2` image file.
   a) Go to the CLOUD MARKET PLACE section of Fix Central (https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.4.0&platform=Linux&function=all).
   b) Click **7.4.3-CMP-IBMCloudVPC-APPHOST-QRADAR-20220329114452**.
   c) Download the `.qcow2` and `.sig` files.
   The `.qcow2` file download can take several hours.
   d) Use the `.sig` file to verify the integrity of the `.qcow2` file.

For more information, see How to verify downloads from IBM Fix Central are trusted and code signed.

2. Upload the `.qcow2` image file.
   a) Go to IBM Cloud (https://cloud.ibm.com/) and create a new storage bucket.
      You need the location that is used by your storage bucket in step 3.
   b) Upload the `.qcow2` file.
      The upload can take up to an hour. Do not rename the `.qcow2` file. Renaming the file causes the import to fail.
3. Import the `.qcow2` file.
   a) In IBM Cloud, click ☰ > **VPC Infrastructure** > **Custom images**.
   b) Click **Create**.
   c) Enter a name for the image and select a **Resource group** for the image to belong to.
   d) Set the **Source** to **Cloud Object Storage**.
   e) Select the Cloud Object Storage service instance, the location that is used by your storage bucket, your storage bucket, and the `.qcow2` file that you uploaded.
      Note: If you want to import your image into multiple regions, you will have to repeat step 2 and create a new storage bucket in each desired region.
   f) Set the **Operating system** to **Red Hat Enterprise Linux**, and set the **Version** to **red-7-amd64-byol**.
   g) Click **Create custom image**.
      The import can take up to 10 minutes.
4. After the image status is `Available`, create the instance.
   a) Click ☰ > **VPC Infrastructure** > **Virtual Server Instances**.
   b) Click **Create +**.
   c) Set the **Architecture** to **Intel**.
   d) Set the **Hosting type** to **Public**.
   e) Set the location to the same region that you imported your image to in step 3.
   f) Give your instance a name that doesn't exceed 57 characters.
      The name can contain only alphanumeric characters and the - symbol.
   g) Select a **Resource group** for the instance.
   h) If you would like an easier way to identify your instance, enter a tag for your instance.
   i) Set the **Operating system** to **Custom image**.
      The **Select custom image** window appears.
   j) Choose the image that you imported in step 3, then click **Select**.
   k) Click **View all profiles**.
      The **Select an instance profile** window appears.
   l) Select a profile that meets the system requirements for virtual appliances, then click **Save**.
      Important: Instances that use Instance storage are not supported.
   m) Select or create an SSH key pair.
      You need an SSH key pair to access the instance by using SSH.
   n) In the **Data volumes** section, click **Create +**.
   o) Enter a **Name** for the second disk.
   p) Estimate your storage needs and enter a size for the second disk in GB.
      The minimum size is 250 GB. The added disk must be the second disk. It cannot be the third or greater disk.

When the installation is complete, this disk contains the `/store` and `/transient` partitions.

Warning: You cannot increase storage after installation.

q) Select a profile, set the IOPS, and click **Create**.

r) Select a **Virtual private cloud**.

s) In the **Network interfaces** section, click the icon next to **eth0**.

t) Leave the **interface** set to **eth0** and select a **Subnet**.

u) Set **Reserving method** to **Let me specify** and select a reserved private IP address from your subnet.

This IP address will be the private IP address associated with your instance.

v) Select a security group that allows ports 22 and 443 only from trusted IP addresses, then click **Save**.

In a QRadar deployment with multiple appliances, other ports might also be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see "Common ports and servers used by QRadar" on page 122.

w) Click **Create Virtual Server**.

5. When the instance status says `Running`, assign a floating IP address to your instance.

a) Click on the instance that you created.

b) In the **Network interfaces** section, click the icon next to **eth0**.

c) Select an IP address or **Reserve a new floating IP** from the **Floating IP address** dropdown, then click **Save**.

6. Install the App Host and set the root password.

a) When the floating IP address is assigned, log in by typing the following command:

```
ssh -i <private_key> cloud-user@<public_IP_address>
```

b) To install the App Host, type the following command:

```
sudo /root/setup_apphost
```

c) The system prompts you to set the root password. Set a strong password that meets the following criteria.

- Contains at least 5 characters
- Contains no spaces
- Includes one or more of the following special characters: `@`, `#`, `^`, and `*`.

7. Add the host to your deployment in QRadar.

a) On the navigation menu ( ), click **Admin**.

b) In the **System Configuration** section, click **System and License Management**.

c) In the **Display** list, select **Systems**.

d) On the **Deployment Actions** menu, click **Add Host**.

e) Configure the settings for the host by providing the fixed IP address, and the root password to access the operating system shell on the appliance.

f) Click **Add**.

g) Optional: Use the **Deployment actions** > **View Deployment** menu to see visualizations of your deployment. You can download a PNG image or a Microsoft Visio (2010) VDX file of your deployment visualization.

h) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

Important: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

8. Change where your apps are run in QRadar.
   a) On the **System and License Management** screen, click the **Click to change where apps are run** link.
   b) Click **App Host** to transfer apps to the App Host.

      Note: The more apps and app data you have, the longer the transfer takes.

Configuring a Console on Microsoft Azure

Configure a Console in Microsoft Azure by using the provided image.

Before you begin

Important:

The following procedure is for the configuration of an IBM QRadar 7.3.3 Console image, which has reached its End of Support. An IBM® QRadar® 7.4.3 Console image is not yet available. Once the image is installed, it should be upgraded to ensure that support is available. For information about upgrading to 7.4.3, see Upgrading QRadar SIEM.

You must acquire entitlement to a QRadar Software Node for any QRadar instance that is deployed from a third-party cloud marketplace. Entitlement to the software node must be in place before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with Microsoft Azure infrastructure, refer to Microsoft Azure Support documentation. If IBM Support determines that your issue is caused by the Microsoft Azure infrastructure, you must contact Microsoft for support to resolve the underlying issue with the Microsoft Azure infrastructure.

You must use static IP addresses.

You cannot have more than two DNS entries. QRadar installation fails if you have more than two DNS entries in the `/etc/resolv.conf` file.

If you are installing a data gateway for QRadar on Cloud, go to Installing a QRadar data gateway in Microsoft Azure (https://www.ibm.com/support/knowledgecenter/en/SSKMKU/com.ibm.qradar.doc_cloud/t_hosted_azure.html).

If you deploy a managed host and a Console in the same virtual network, use the private IP address of the managed host to add it to the Console.

If you deploy a managed host and a Console in different virtual networks, you must allow firewall rules for the communication between the Console and the managed host. For more information, see “QRadar port usage ” on page 122.

You must complete all of the installation steps before you run QRadar commands such as **qchange_netsetup**.

For more information about configuring firewall rules between hosts, see Microsoft documentation.

Procedure

1. Go to the Microsoft Azure Marketplace (https://azuremarketplace.microsoft.com/en-us/marketplace/apps/ibm.qradar733?tab=Overview).

   Note: The **Plans + Pricing** tab can be used to estimate pricing for certain VM sizes, but you don't choose your VM size on this screen. Refer to the **Core** and **RAM** columns when you are estimating

pricing. Ignore the **Disk Space** column, as all QRadar marketplace images include a disk for the operating system, and a 1 TB disk for storage.

2. Click **Get It Now**.
3. Select **QRadar SIEM Console 7.3.3** from the **Software plan** menu list and click **Continue**.
4. Click **Create** to create an instance of the virtual appliance.
5. Configure VM settings.
   a) Select an existing **Resource Group** or create a new one.
   b) Enter a virtual machine name.

      Note: The VM name must be 10 characters or fewer.

   c) Select a **Region**.
   d) Click **Change size** and ensure that your VM meets the minimum system requirements.
      For more information, see "System requirements for virtual appliances" on page 24.
   e) Enter a username for the administrator account.
   f) Choose an **SSH public key** or **Password**.

      For more information about creating and using an SSH public-private key pair for Linux VMs in Microsoft Azure, see Microsoft documentation.

   g) Set **Public inbound ports** to **Allow selected ports**.
   h) Set **Select inbound ports** to **SSH (22)** and **HTTPS (443)**.
6. Click **Review + Create**.
7. Click **Create** to deploy the instance.
8. When your VM is deployed in Microsoft Azure, set the private and public IP addresses to static.
   a) Click **Go to resource**.
   b) Click the public IP address.
   c) Set the **Assignment** to **Static**.
   d) Click **Save**.
   e) Click **Overview**.
   f) Click the **Associated to** link.
   g) Click **IP configurations**.
   h) In the list of IP configurations, click the configuration row where the **Type** is set to Primary.
   i) Set the Private IP address assignment to **Static**.
   j) Click **Save**.
9. Create or select a security group that allows ports 22 and 443 only from trusted IP addresses to create an allowlist of IP addresses that can access your QRadar deployment.

   In a QRadar deployment with multiple appliances, other ports might also be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see "Common ports and servers used by QRadar" on page 122.

   a) Click **Home**.
   b) Click **Virtual Machines** .
   c) Click the name of your virtual machine.
   d) Click **Networking**.
   e) Click the SSH rule that is associated with port 22.
   f) In the edit pane, select **IP Addresses** from the **Source** list.
   g) In the **Source IP addresses/CIDR ranges** field, enter the address range of the IP addresses that are allowed to access the VM.
   h) Click **Save**.

i) Click the HTTPS rule that is associated with port 443.

j) In the edit pane, select **IP Addresses** from the **Source** list.

k) In the **Source IP addresses/CIDR ranges** field, enter the address range of the IP addresses that are allowed to access the VM.

l) Click **Save**.

10. To display the SSH connection information for the public IP address of the virtual appliance.
    a) Click **Virtual Machines** > **<virtual_machine_name>**.
    b) Click **Connect**.
11. Log in to your virtual machine.
    - To log in using SSH and your key pair, type the following command:

      ```
      ssh -i <key.pem> user@<public_IP_address>
      ```

    - To log in using SSH and your password, type the following command:

      ```
      ssh user@<public_IP_address>
      ```

12. To check that the hostname is a fully qualified domain name (FQDN), type the following command:

    ```
    hostname -f
    ```

    If the command returns a hostname that is not an FQDN, DNS is misconfigured and installation fails. Restart this procedure with proper DNS configuration. For more information about DNS configuration, see the Microsoft Azure Support documentation.
13. To check the length of your FQDN, type the following command:

    ```
    hostname -f | wc -c
    ```

    If the command returns a value greater than 63, installation fails. Restart this procedure with a shorter virtual machine name.
14. Ensure that there are no more than 2 DNS entries for the instance by typing the following command:

    ```
    grep nameserver /etc/resolv.conf | wc -l
    ```

    If the command returns 3 or higher, edit `/etc/resolv.conf` to remove all but two of the entries before you proceed to the next step. You will add the entries back after installation is complete.

What to do next

If you need to increase file system storage beyond the default 1 TB, follow the steps in "Increasing file system storage for a new Console by recreating the data disk at a larger size" on page 67. Increase the file system storage before you complete the installation if possible, as increasing file system storage on a running system is more risky than increasing it before installation is complete.

If you don't need more than 1 TB of storage, proceed to "Installing the Console" on page 73.

If you need to change your hostname or FQDN, run the **qchange_netsetup** command.

Increasing file system storage for a new Console by recreating the data disk at a larger size

Increase the size of the file system on the Console by re-creating the existing data disk at a larger size and by using the Red Hat LVM logical volume manager.

Before you begin

For more information about expanding the size of a disk, see Microsoft documentation.

About this task

Warning: This procedure is for new installations only, and must be complete before completing the steps in "Installing the Console" on page 73. Following these steps after installation is complete will result in errors and data loss.

Procedure

1. Stop your virtual machine (VM).
2. Click **Disks**.

   Warning: Do not add more disks.

   To increase storage to less than 4095 GiB:

   a) Click on the data disk link.

   b) Click **Size + performance**.

   c) Choose from the list, or enter the new disk size in GiB.

   d) Click **Save**.

   To increase storage to more than 4095 GiB:

   a) Click **Edit**.

   b) Click the **X** next to the data disk to detach the disk.

   c) Click **Save**.

   d) Click **Home**.

   e) Click **Disks**.

   f) Click the disk associated with the VM that you are editing.

   g) Click **Size + performance**.

   h) Enter the new disk size in GiB.

   i) Click **Save**.

   j) Go to the Home screen and click **Virtual machines**

   k) Click the name of your virtual machine.

   l) Click **Disks**.

   m) Click **+ Add data disk**.

   n) Select the disk that you modified.

   o) Click **Save**.
3. After the data disk is expanded, restart your VM.
4. Log in to your VM by using **ssh**.
5. Determine the device name and partition number for the `/store` and `/transient` file systems by typing the following command:

   ```
   lsblk
   ```

   In this example **lsblk** output, for the `/store` and `/transient` file systems the *<device_name>* is sdc, the *<partition_number>* is 1, and the *<volume_group>* is data.

   ```
   NAME                  MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
   fd0                     2:0    1     4K  0 disk
   sda                     8:0    0    98G  0 disk
   ├─sda1                  8:1    0     1G  0 part /boot
   ├─sda2                  8:2    0    20G  0 part /
   ├─sda3                  8:3    0   200M  0 part /boot/efi
   ├─sda4                  8:4    0     1K  0 part
   └─sda5                  8:5    0  76.8G  0 part
     ├─rhel-var          253:0    0     8G  0 lvm  /var
     ├─rhel-var_log      253:1    0    18G  0 lvm  /var/log
     ├─rhel-temp         253:2    0     8G  0 lvm  /temp
   ```

```
  ├─rhel-storetmp      253:3    0    15G  0 lvm  /storetmp
  ├─rhel-opt           253:4    0    14G  0 lvm  /opt
  ├─rhel-home          253:5    0     6G  0 lvm  /home
  └─rhel-var_log_audit 253:6    0   7.8G  0 lvm  /var/log/audit
sdb                      8:16   0    32G  0 disk
└─sdb1                   8:17   0    32G  0 part /mnt/resource
 sdc                       8:32   0     6T  0 disk
└─sdc 1                    8:33   0  1022G  0 part
  ├─ data -transient     253:7    0 204.4G  0 lvm  /transient
  └─ data -store         253:8    0 817.6G  0 lvm  /store
```

6. Become the super user by typing the following command and entering your password when promoted:

```
sudo -i
```

7. Open the **parted** prompt by typing the following command:

```
parted /dev/<device_name>
```

Example command:

```
parted /dev/sdc
```

8. Switch the units displayed to MiB by typing the following command:

```
unit mib
```

```
p
```

9. When prompted with "Error: The backup GPT table is not at the end of the disk...", enter `Fix`.
10. When prompted with "Warning: Not all of the space available ...", enter `Fix`.
11. Resize the partition to fill the disk by typing the following command:

```
resizepart <partition_number> 100%
```

Example command:

```
resizepart 1 100%
```

12. Exit parted by typing the following command:

```
quit
```

13. Ensure that the kernel recognizes the new partition information by typing the following command:

```
partprobe /dev/<device_name><partition_number>
```

Example command:

```
partprobe /dev/sdc1
```

There is no output for this step if it is successful.

- If there is no output, proceed directly to the next step.
- If there is output that indicates that **partprobe** didn't detect the new partitions, reboot the system before you continue to the next step.

14. Grow the physical volume to fill the extra disk space by typing the following command:

```
pvresize /dev/<device_name><partition_number>
```

Example command:

```
pvresize /dev/sdc1
```

Example successful output:

```
Physical volume "/dev/sdc1" changed
  1 physical volume(s) resized / 0 physical volume(s) not resized
```

15. Expand /transient by 20% of the extra disk space by typing the following command:

    ```
    lvextend -l +20%FREE /dev/<volume_group>/transient
    ```

    Example command:

    ```
    lvextend -l +20%FREE /dev/data/transient
    ```

    Example successful output:

    ```
    Size of logical volume data/transient changed from <204.40 GiB (52326 extents) to 1.20 TiB
    (314573 extents).
      Logical volume data/transient successfully resized.
    ```

16. Expand /store into the remaining extra disk space by typing the following command:

    ```
    lvextend -l +100%FREE /dev/<volume_group>/store
    ```

    Example command:

    ```
    lvextend -l +100%FREE /dev/data/store
    ```

    Example successful output:

    ```
    Size of logical volume data/store changed from <817.60 GiB (209305 extents) to 4.00 TiB
    (1048985 extents).
      Logical volume data/store successfully resized.
    ```

17. Reformat the /store file system:

    a) Unmount the /store file system by typing the following command:

    ```
    umount /dev/mapper/<volume_group>-store
    ```

    Example command:

    ```
    umount /dev/mapper/data-store
    ```

    b) Construct the XFS file system for /store by typing the following command:

    ```
    mkfs.xfs -f /dev/mapper/<volume_group>-store
    ```

    Example command:

    ```
    mkfs.xfs -f /dev/mapper/data-store
    ```

    Example successful output:

    ```
    meta-data=/dev/mapper/data-store isize=512    agcount=5, agsize=268435455 blks
             =                       sectsz=4096  attr=2, projid32bit=1
             =                       crc=1        finobt=0, sparse=0
    data     =                       bsize=4096   blocks=1074160640, imaxpct=5
             =                       sunit=0      swidth=0 blks
    naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
    log      =internal log           bsize=4096   blocks=521728, version=2
             =                       sectsz=4096  sunit=1 blks, lazy-count=1
    realtime =none                   extsz=4096   blocks=0, rtextents=0
    ```

    c) Verify that the XFS file system for /store is not damaged by typing the following command:

    ```
    xfs_repair /dev/mapper/<volume_group>-store
    ```

    Example command:

    ```
    xfs_repair /dev/mapper/data-store
    ```

    Example successful output:

    ```
    Phase 1 - find and verify superblock...
    Phase 2 - using internal log
    ```

```
        - zero log...
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan and clear agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - agno = 4
        - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
        - setting up duplicate extent list...
        - check for inodes claiming duplicate blocks...
        - agno = 0
        - agno = 1
        - agno = 3
        - agno = 4
        - agno = 2
Phase 5 - rebuild AG headers and trees...
        - reset superblock...
Phase 6 - check inode connectivity...
        - resetting contents of realtime bitmap and summary inodes
        - traversing filesystem ...
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
done
```

d) Mount the `/store` file system by typing the following command:

```
mount /dev/mapper/<volume_group>-store
```

Example command:

```
mount /dev/mapper/data-store
```

18. Reformat the `/transient` file system:

a) Unmount the `/transient` file system by typing the following command:

```
umount /dev/mapper/<volume_group>-transient
```

Example command:

```
umount /dev/mapper/data-transient
```

b) Construct the XFS file system for `/transient` by typing the following command:

```
mkfs.xfs -f /dev/mapper/<volume_group>-transient
```

Example command:

```
mkfs.xfs -f /dev/mapper/data-transient
```

Example successful output:

```
meta-data=/dev/mapper/data-transient isize=512    agcount=4, agsize=80530688 blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=0, sparse=0
data     =                       bsize=4096   blocks=322122752, imaxpct=5
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal log           bsize=4096   blocks=157286, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

c) Verify that the XFS file system for `/transient` is not damaged by typing the following command:

```
xfs_repair /dev/mapper/<volume_group>-transient
```

Example command:

```
xfs_repair /dev/mapper/data-transient
```

Example successful output:

```
Phase 1 - find and verify superblock...
Phase 2 - using internal log
        - zero log...
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan and clear agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
        - setting up duplicate extent list...
        - check for inodes claiming duplicate blocks...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
Phase 5 - rebuild AG headers and trees...
        - reset superblock...
Phase 6 - check inode connectivity...
        - resetting contents of realtime bitmap and summary inodes
        - traversing filesystem ...
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
done
```

d) Mount the `/transient` file system by typing the following command:

```
mount /dev/mapper/<volume_group>-transient
```

Example command:

```
mount /dev/mapper/data-transient
```

19. Verify that the new sizes of the expanded file systems are correct by typing the following command:

```
df -h
```

Example successful output:

```
Filesystem                      Size  Used Avail Use% Mounted on
/dev/sda2                        20G  1.2G   18G   7% /
devtmpfs                        7.9G     0  7.9G   0% /dev
tmpfs                           7.9G     0  7.9G   0% /dev/shm
tmpfs                           7.9G  9.1M  7.9G   1% /run
tmpfs                           7.9G     0  7.9G   0% /sys/fs/cgroup
/dev/sda1                       976M  127M  783M  14% /boot
/dev/sda3                       200M  8.0K  200M   1% /boot/efi
/dev/mapper/rhel-var            8.0G  178M  7.9G   3% /var
/dev/mapper/rhel-opt             14G  3.5G   11G  25% /opt
/dev/mapper/rhel-storetmp        15G   33M   15G   1% /storetmp
/dev/mapper/rhel-temp           8.0G   33M  8.0G   1% /temp
/dev/mapper/rhel-home           6.0G   33M  6.0G   1% /home
/dev/mapper/rhel-var_log         18G   44M   18G   1% /var/log
/dev/mapper/rhel-var_log_audit  7.8G   70M  7.8G   1% /var/log/audit
/dev/sdb1                        32G   13G   20G  38% /mnt/resource
tmpfs                           1.6G     0  1.6G   0% /run/user/1000
/dev/mapper/data-store          4.0T   33M  4.0T   1% /store
/dev/mapper/data-transient      1.2T   33M  1.2T   1% /transient
```

20. Reboot the VM.
21. Log in to your virtual machine.
    - To log in using SSH and your key pair, type the following command:

      ```
      ssh -i <key.pem> user@<public_IP_address>
      ```

    - To log in using SSH and your password, type the following command:

```
ssh user@<public_IP_address>
```

Results

If you increased the file system storage, you may see the following warning when you log in to the system:

```
WARNING:*****************************************************************
WARNING: QRadar requires 4092M of swap space but was only able to find
WARNING: 0M, please increase swap space by at least 4092M. Without this
WARNING: additional swap space, some components of QRadar will not function
WARNING: properly (such as complex queries or reports). Please contact
WARNING: Customer Support for further details and assistance in resolving
WARNING: this issue.
WARNING:*****************************************************************
```

This warning after increasing file system storage on a new VM in Microsoft Azure is benign. This warning is displayed because the swap space for the VM is being updated in the Microsoft Azure infrastructure. You can proceed with the installation.

What to do next

Follow the steps in "Installing the Console" on page 73.

Installing the Console

Procedure

1. Type the following command to install the Console:

   ```
   sudo /root/setup_console
   ```

2. Enter a password for the admin account. Set a strong password that meets the following criteria.
   - Contains at least 5 characters
   - Contains no spaces
   - Can include the following special characters, unless you are installing a data gateway: @, #, ^, and *.
3. Become the root user by typing the following command:

   ```
   sudo -i
   ```

4. Update the license file to address the issue described in APAR IJ30161 (https://www.ibm.com/support/pages/apar/IJ30161) by typing the following command:

   ```
   echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20"
   | tee /opt/qradar/ecs/license.txt /opt/ibm/si/services/ecs-ep/current/eventgnosis/
   license.txt /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/license.txt /opt/ibm/si/
   services/ecs-ec/current/eventgnosis/license.txt /usr/eventgnosis/ecs/license.txt /opt/qradar/
   conf/templates/ecs_license.txt
   ```

   It takes approximately 5 minutes for the changes to complete.
5. Exit the superuser shell by typing the following command:

   ```
   exit
   ```

What to do next

If you removed any DNS entries in `/etc/resolv.conf`, restore them.

Important: IBM QRadar 7.3.3 has reached End of Support. To ensure that support is available, an upgrade must be performed. For information about upgrading to 7.4.3, see Upgrading QRadar SIEM.

Configuring a managed host on Microsoft Azure

Configure a QRadar managed host in Microsoft Azure by using the provided image. You can specify which role the virtual appliance fulfills in your deployment. For example, you can configure the virtual appliance as a collector, or a processor.

Before you begin

Important:

The following procedure is for the configuration of an IBM QRadar 7.3.3 managed host image, which has reached its End of Support. An IBM® QRadar® 7.4.3 managed host image is not yet available. Once the image is installed, it should be upgraded to ensure that support is available. For information about upgrading to 7.4.3, see Upgrading QRadar SIEM.

You must acquire entitlement to a QRadar Software Node for any QRadar instance that is deployed from a third-party cloud marketplace. Entitlement to the software node should be in place before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with Microsoft Azure infrastructure, refer to Microsoft Azure Support documentation. If IBM Support determines that your issue is caused by the Microsoft Azure infrastructure, you must contact Microsoft for support to resolve the underlying issue with the Microsoft Azure infrastructure.

You must use static IP addresses.

You cannot have more than two DNS entries. QRadar installation fails if you have more than two DNS entries in the `/etc/resolv.conf` file.

The managed host must be the same version as your Console before you can add the managed host to your deployment. You can upgrade the managed host to a later version of QRadar after you complete the installation by downloading the fix pack from Fix Central (https://www.ibm.com/support/fixcentral) and following the normal upgrade procedure. For more information about upgrades, see *IBM QRadar Upgrade Guide*.

If you are installing a data gateway for QRadar on Cloud, go to Installing a QRadar data gateway in Microsoft Azure (https://www.ibm.com/support/knowledgecenter/en/SSKMKU/com.ibm.qradar.doc_cloud/t_hosted_azure.html).

If you deploy a managed host and a Console in the same virtual network, use the private IP address of the managed host to add it to the Console.

If you deploy a managed host and a Console in different virtual networks, you must allow firewall rules for the communication between the Console and the managed host. For more information, see “QRadar port usage ” on page 122.

You must complete all of the installation steps before you run QRadar commands such as **qchange_netsetup**.

For more information about configuring firewall rules between hosts, see Microsoft documentation.

Procedure

1. Go to the Microsoft Azure Marketplace (https://azuremarketplace.microsoft.com/en-us/marketplace/apps/ibm.qradar733?tab=Overview).

   Note: The **Plans + Pricing** tab can be used to estimate pricing for certain VM sizes, but you don't choose your VM size on this screen. Refer to the **Core** and **RAM** columns when you are estimating pricing. Ignore the **Disk Space** column, as all QRadar marketplace images include a disk for the operating system, and a 1 TB disk for storage.
2. Click **Get It Now**.
3. Select **QRadar SIEM MH 7.3.3** from the **Software plan** menu list and click **Continue**.

4. Click **Create** to create an instance of the virtual appliance.
5. Configure VM settings.
   a) Select an existing **Resource Group** or create a new one.
   b) Enter a virtual machine name.

      Note: The VM name must be 10 characters or fewer.
   c) Select a **Region**.
   d) Click **Change size** and ensure that your VM meets the minimum system requirements.
      For more information, see "System requirements for virtual appliances" on page 24.
   e) Enter a username for the administrator account.
   f) Choose an **SSH public key** or **Password**.

      For more information about creating and using an SSH public-private key pair for Linux VMs in Microsoft Azure, see Microsoft documentation.
   g) Set **Public inbound ports** to **Allow selected ports**.
   h) Set **Select inbound ports** to **SSH (22)** and **HTTPS (443)**.
6. Click **Review + Create**.
7. Click **Create** to deploy the instance.
8. When your VM is deployed in Microsoft Azure, set the private and public IP addresses to static.
   a) Click **Go to resource**.
   b) Click the public IP address.
   c) Set the **Assignment** to **Static**.
   d) Click **Save**.
   e) Click **Overview**.
   f) Click the **Associated to** link.
   g) Click **IP configurations**.
   h) In the list of IP configurations, click the configuration row where the **Type** is set to Primary.
   i) Set the Private IP address assignment to **Static**.
   j) Click **Save**.
9. Create or select a security group that allows ports 22 and 443 only from trusted IP addresses to create an allowlist of IP addresses that can access your QRadar deployment.

   In a QRadar deployment with multiple appliances, other ports might also be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see "Common ports and servers used by QRadar" on page 122.
   a) Click **Home**.
   b) Click **Virtual Machines** .
   c) Click the name of your virtual machine.
   d) Click **Networking**.
   e) Click the SSH rule that is associated with port 22.
   f) In the edit pane, select **IP Addresses** from the **Source** list.
   g) In the **Source IP addresses/CIDR ranges** field, enter the address range of the IP addresses that are allowed to access the VM.
   h) Click **Save**.
   i) Click the HTTPS rule that is associated with port 443.
   j) In the edit pane, select **IP Addresses** from the **Source** list.
   k) In the **Source IP addresses/CIDR ranges** field, enter the address range of the IP addresses that are allowed to access the VM.

l) Click **Save**.

10. To display the SSH connection information for the public IP address of the virtual appliance.
    a) Click **Virtual Machines** > **<virtual_machine_name>**.
    b) Click **Connect**.
11. Log in to your virtual machine.
    - To log in using SSH and your key pair, type the following command:

      ```
      ssh -i <key.pem> user@<public_IP_address>
      ```

    - To log in using SSH and your password, type the following command:

      ```
      ssh user@<public_IP_address>
      ```

12. To check that the hostname is a fully qualified domain name (FQDN), type the following command:

    ```
    hostname -f
    ```

    If the command returns a hostname that is not an FQDN, DNS is misconfigured and installation fails. Restart this procedure with proper DNS configuration. For more information about DNS configuration, see the Microsoft Azure Support documentation.
13. To check the length of your FQDN, type the following command:

    ```
    hostname -f | wc -c
    ```

    If the command returns a value greater than 63, installation fails. Restart this procedure with a shorter virtual machine name.

What to do next

If you need to increase file system storage beyond the default 1 TB, follow the steps in "Increasing file system storage for a new managed host by recreating the data disk at a larger size" on page 76. Increase the file system storage before you complete the installation if possible, as increasing file system storage on a running system is more risky than increasing it before installation is complete.

If you don't need more than 1 TB of storage, proceed to "Installing the managed host" on page 83.

If you need to change your hostname or FQDN, run the **qchange_netsetup** command.

Increasing file system storage for a new managed host by recreating the data disk at a larger size

Increase the size of the file system on the managed host by recreating the existing data disk at a larger size and by using the Red Hat LVM logical volume manager.

Before you begin

For more information about expanding the size of a disk, see Microsoft documentation.

About this task

Warning: This procedure is for new installations only, and must be complete before completing the steps in "Installing the managed host" on page 83. Following these steps after installation is complete will result in errors and data loss.

Procedure

1. Stop your virtual machine (VM).
2. Click **Disks**.

Warning: Do not add more disks.

To increase storage to less than 4095 GiB:

a) Click on the data disk link.

b) Click **Size + performance**.

c) Choose from the list, or enter the new disk size in GiB.

d) Click **Save**.

To increase storage to more than 4095 GiB:

a) Click **Edit**.

b) Click the **X** next to the data disk to detach the disk.

c) Click **Save**.

d) Click **Home**.

e) Click **Disks**.

f) Click the disk associated with the VM that you are editing.

g) Click **Size + performance**.

h) Enter the new disk size in GiB.

i) Click **Save**.

j) Go to the Home screen and click **Virtual machines**

k) Click the name of your virtual machine.

l) Click **Disks**.

m) Click **+ Add data disk**.

n) Select the disk that you modified.

o) Click **Save**.

3. After the data disk is expanded, restart your VM.
4. Log in to your VM by using **ssh**.
5. Determine the device name and partition number for the `/store` and `/transient` file systems by typing the following command:

```
lsblk
```

In this example **lsblk** output, for the `/store` and `/transient` file systems the *<device_name>* is sdc, the *<partition_number>* is 1, and the *<volume_group>* is data.

```
NAME                    MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
fd0                       2:0    1     4K  0 disk
sda                       8:0    0    98G  0 disk
├─sda1                    8:1    0     1G  0 part /boot
├─sda2                    8:2    0    20G  0 part /
├─sda3                    8:3    0   200M  0 part /boot/efi
├─sda4                    8:4    0     1K  0 part
└─sda5                    8:5    0  76.8G  0 part
  ├─rhel-var            253:0    0     8G  0 lvm  /var
  ├─rhel-var_log        253:1    0    18G  0 lvm  /var/log
  ├─rhel-temp           253:2    0     8G  0 lvm  /temp
  ├─rhel-storetmp       253:3    0    15G  0 lvm  /storetmp
  ├─rhel-opt            253:4    0    14G  0 lvm  /opt
  ├─rhel-home           253:5    0     6G  0 lvm  /home
  └─rhel-var_log_audit  253:6    0   7.8G  0 lvm  /var/log/audit
sdb                       8:16   0    32G  0 disk
└─sdb1                    8:17   0    32G  0 part /mnt/resource
sdc                       8:32   0     6T  0 disk
└─sdc1                    8:33   0  1022G  0 part
  ├─data-transient      253:7    0 204.4G  0 lvm  /transient
  └─data-store          253:8    0 817.6G  0 lvm  /store
```

6. Become the super user by typing the following command and entering your password when promoted:

```
sudo -i
```

7. Stop services by typing the following commands:

```
systemctl stop ecs-ec-ingress
```

```
systemctl stop ecs-ep
```

```
systemctl stop hostservices
```

```
systemctl stop systemStabMon
```

```
systemctl stop crond
```

8. Go to the root directory by typing the following command:

```
cd /
```

9. Create a backup of the `/store` file system by typing the following command:

```
tar -czpf storetmp/storebackup.tgz store
```

The output may include something like "tar: store/tmp/storebackup.tgz: file is the archive; not dumped". This message is benign. If you encounter this message, ignore it and proceed with the next step.

10. Create a backup of the `/transient` file system by typing the following command:

```
tar -czpf storetmp/transientbackup.tgz transient
```

11. Open the **parted** prompt by typing the following command:

```
parted /dev/<device_name>
```

Example command:

```
parted /dev/sdc
```

12. Switch the units displayed to MiB by typing the following command:

```
unit mib
```

```
p
```

13. When prompted with "Error: The backup GPT table is not at the end of the disk...", enter `Fix`.
14. When prompted with "Warning: Not all of the space available ...", enter `Fix`.
15. Resize the partition to fill the disk by typing the following command:

```
resizepart <partition_number> 100%
```

Example command:

```
resizepart 1 100%
```

16. Exit parted by typing the following command:

```
quit
```

17. Ensure that the kernel recognizes the new partition information by typing the following command:

```
partprobe /dev/<device_name><partition_number>
```

Example command:

```
partprobe /dev/sdc1
```

There is no output for this step if it is successful.

- If there is no output, proceed directly to the next step.
- If there is output that indicates that **partprobe** didn't detect the new partitions, reboot the system and repeat step 7 before you continue to the next step.

18. Grow the physical volume to fill the extra disk space by typing the following command:

```
pvresize /dev/<device_name><partition_number>
```

Example command:

```
pvresize /dev/sdc1
```

Example successful output:

```
Physical volume "/dev/sdc1" changed
  1 physical volume(s) resized / 0 physical volume(s) not resized
```

The output may include something like "File descriptor 63 (pipe:[102103]) leaked on pvresize invocation. Parent PID 6636: -bash". This message is benign. If you encounter this message, ignore it and proceed with the next step.

19. Expand `/transient` by 20% of the extra disk space by typing the following command:

```
lvextend -l +20%FREE /dev/<volume_group>/transient
```

Example command:

```
lvextend -l +20%FREE /dev/data/transient
```

Example successful output:

```
Size of logical volume data/transient changed from <204.40 GiB (52326 extents) to 1.20 TiB
(314573 extents).
  Logical volume data/transient successfully resized.
```

20. Expand `/store` into the remaining extra disk space by typing the following command:

```
lvextend -l +100%FREE /dev/<volume_group>/store
```

Example command:

```
lvextend -l +100%FREE /dev/data/store
```

Example successful output:

```
Size of logical volume data/store changed from <817.60 GiB (209305 extents) to 4.00 TiB
(1048985 extents).
  Logical volume data/store successfully resized.
```

21. Reformat the `/store` file system:
    a) Unmount the `/store` file system by typing the following command:

```
umount /dev/mapper/<volume_group>-store
```

Example command:

```
umount /dev/mapper/data-store
```

    b) Construct the XFS file system for `/store` by typing the following command:

```
mkfs.xfs -f /dev/mapper/<volume_group>-store
```

Example command:

```
mkfs.xfs -f /dev/mapper/data-store
```

Example successful output:

```
meta-data=/dev/mapper/data-store isize=512    agcount=5, agsize=268435455 blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=0, sparse=0
data     =                       bsize=4096   blocks=1074160640, imaxpct=5
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal log           bsize=4096   blocks=521728, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

c) Verify that the XFS file system for `/store` is not damaged by typing the following command:

```
xfs_repair /dev/mapper/<volume_group>-store
```

Example command:

```
xfs_repair /dev/mapper/data-store
```

Example successful output:

```
Phase 1 - find and verify superblock...
Phase 2 - using internal log
        - zero log...
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan and clear agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - agno = 4
        - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
        - setting up duplicate extent list...
        - check for inodes claiming duplicate blocks...
        - agno = 0
        - agno = 1
        - agno = 3
        - agno = 4
        - agno = 2
Phase 5 - rebuild AG headers and trees...
        - reset superblock...
Phase 6 - check inode connectivity...
        - resetting contents of realtime bitmap and summary inodes
        - traversing filesystem ...
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
done
```

d) Mount the `/store` file system by typing the following command:

```
mount /dev/mapper/<volume_group>-store
```

Example command:

```
mount /dev/mapper/data-store
```

22. Reformat the `/transient` file system:

a) Unmount the `/transient` file system by typing the following command:

```
umount /dev/mapper/<volume_group>-transient
```

Example command:

```
umount /dev/mapper/data-transient
```

b) Construct the XFS file system for `/transient` by typing the following command:

```
mkfs.xfs -f /dev/mapper/<volume_group>-transient
```

Example command:

```
mkfs.xfs -f /dev/mapper/data-transient
```

Example successful output:

```
meta-data=/dev/mapper/data-transient isize=512    agcount=4, agsize=80530688 blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=0, sparse=0
data     =                       bsize=4096   blocks=322122752, imaxpct=5
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal log           bsize=4096   blocks=157286, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

c) Verify that the XFS file system for `/transient` is not damaged by typing the following command:

```
xfs_repair /dev/mapper/<volume_group>-transient
```

Example command:

```
xfs_repair /dev/mapper/data-transient
```

Example successful output:

```
Phase 1 - find and verify superblock...
Phase 2 - using internal log
        - zero log...
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan and clear agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
        - setting up duplicate extent list...
        - check for inodes claiming duplicate blocks...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
Phase 5 - rebuild AG headers and trees...
        - reset superblock...
Phase 6 - check inode connectivity...
        - resetting contents of realtime bitmap and summary inodes
        - traversing filesystem ...
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
done
```

d) Mount the `/transient` file system by typing the following command:

```
mount /dev/mapper/<volume_group>-transient
```

Example command:

```
mount /dev/mapper/data-transient
```

23. Verify that the new sizes of the expanded file systems are correct by typing the following command:

```
df -h
```

Example successful output:

```
Filesystem                    Size  Used Avail Use% Mounted on
/dev/sda2                      20G  1.2G   18G   7% /
devtmpfs                      7.9G     0  7.9G   0% /dev
```

```
tmpfs                           7.9G     0  7.9G   0% /dev/shm
tmpfs                           7.9G  9.1M  7.9G   1% /run
tmpfs                           7.9G     0  7.9G   0% /sys/fs/cgroup
/dev/sda1                       976M  127M  783M  14% /boot
/dev/sda3                       200M  8.0K  200M   1% /boot/efi
/dev/mapper/rhel-var            8.0G  178M  7.9G   3% /var
/dev/mapper/rhel-opt             14G  3.5G   11G  25% /opt
/dev/mapper/rhel-storetmp        15G   33M   15G   1% /storetmp
/dev/mapper/rhel-temp           8.0G   33M  8.0G   1% /temp
/dev/mapper/rhel-home           6.0G   33M  6.0G   1% /home
/dev/mapper/rhel-var_log         18G   44M   18G   1% /var/log
/dev/mapper/rhel-var_log_audit  7.8G   70M  7.8G   1% /var/log/audit
/dev/sdb1                        32G   13G   20G  38% /mnt/resource
tmpfs                           1.6G     0  1.6G   0% /run/user/1000
/dev/mapper/data-store          4.0T   33M  4.0T   1% /store
/dev/mapper/data-transient      1.2T   33M  1.2T   1% /transient
```

24. Restore your backup of the `/store` file system by typing the following command:

    ```
    tar -xphf storetmp/storebackup.tgz store
    ```

25. Restore your backup of the `/transient` file system by typing the following command:

    ```
    tar -xphf storetmp/transientbackup.tgz transient
    ```

26. Start services by typing the following commands:

    ```
    systemctl start crond
    ```

    ```
    systemctl start systemStabMon
    ```

    ```
    systemctl start ecs-ep
    ```

    ```
    systemctl start ecs-ec-ingress
    ```

    ```
    systemctl start hostservices
    ```

27. Reboot the VM.
28. Log in to your virtual machine.
    - To log in using SSH and your key pair, type the following command:

      ```
      ssh -i <key.pem> user@<public_IP_address>
      ```

    - To log in using SSH and your password, type the following command:

      ```
      ssh user@<public_IP_address>
      ```

Results

If you increased the file system storage, you may see the following warning when you log in to the system:

```
WARNING:********************************************************************
WARNING: QRadar requires 4092M of swap space but was only able to find
WARNING: 0M, please increase swap space by at least 4092M. Without this
WARNING: additional swap space, some components of QRadar will not function
WARNING: properly (such as complex queries or reports). Please contact
WARNING: Customer Support for further details and assistance in resolving
WARNING: this issue.
WARNING:********************************************************************
```

This warning after increasing file system storage on a new VM in Microsoft Azure is benign. This warning is displayed because the swap space for the VM is being updated in the Microsoft Azure infrastructure. You can proceed with the installation.

What to do next

Follow the steps in “Installing the managed host” on page 83.

Installing the managed host

Procedure

1. Type the following command for the virtual appliance that you're installing:

   ```
   sudo /root/setup_mh <appliance_type_id>
   ```

   For example, to deploy an Event Collector type the following command:

   ```
   sudo /root/setup_mh 1599
   ```

   You can install the following managed host appliance types:

   Table 17. Appliance types

Appliance type ID	Appliance type
1299	Flow Collector
1400	Data Node
1599	Event Collector
1699	Event Processor
1799	Flow Processor
1899	Event and Flow Processor

2. The system prompts you to set a root password. Set a strong root password that meets the following criteria.
   - Contains at least 5 characters
   - Contains no spaces
   - Can include the following special characters, unless you are installing a data gateway: @, #, ^, and *.
3. Become the root user by typing the following command:

   ```
   sudo -i
   ```

4. Update the license file to address the issue described in APAR IJ30161 (https://www.ibm.com/support/pages/apar/IJ30161) by typing the following command:

   ```
   echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20"
   | tee /opt/qradar/ecs/license.txt /opt/ibm/si/services/ecs-ep/current/eventgnosis/
   license.txt /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/license.txt /opt/ibm/si/
   services/ecs-ec/current/eventgnosis/license.txt /usr/eventgnosis/ecs/license.txt /opt/qradar/
   conf/templates/ecs_license.txt
   ```

5. Exit the superuser shell by typing the following command:

   ```
   exit
   ```

6. Ensure that the managed host is the same version as your Console, then add the host to your deployment in QRadar.
   a) On the navigation menu (☰), click **Admin**.
   b) In the **System Configuration** section, click **System and License Management**.
   c) In the **Display** list, select **Systems**.
   d) On the **Deployment Actions** menu, click **Add Host**.
   e) Configure the settings for the managed host by providing a static IP address, and the root password to access the operating system shell on the appliance.
   f) Click **Add**.

g) Optional: Use the **Deployment actions** > **View Deployment** menu to see visualizations of your deployment. You can download a PNG image or a Microsoft Visio (2010) VDX file of your deployment visualization.

h) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

Important: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

What to do next

If you increased file system storage, delete the backup archive.

1. Log in using your key pair by typing the following command:

```
ssh -i <key.pem> ec2-user@<public_IP_address>
```

2. Delete the backup archive by typing the following command:

```
sudo rm /storetmp/storebackup.tgz
```

3. Delete the `/transient` backup archive by typing the following command:

```
sudo rm /storetmp/transientbackup.tgz
```

Important: IBM QRadar 7.3.3 has reached End of Support. To ensure that support is available, an upgrade must be performed. For information about upgrading to 7.4.3, see Upgrading QRadar SIEM.

Configuring an App Host on Microsoft Azure

Configure an App host in Microsoft Azure by using the provided image.

Before you begin

Important:

The following procedure is for the configuration of an IBM QRadar 7.3.3 App Host image, which has reached its End of Support. An IBM® QRadar® 7.4.3 App Host image is not yet available. Once the image is installed, it should be upgraded to ensure that support is available. For information about upgrading to 7.4.3, see Upgrading QRadar SIEM.

You must acquire entitlement to a QRadar Software Node for any QRadar instance that is deployed from a third-party cloud marketplace. Entitlement to the software node should be in place before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with Microsoft Azure infrastructure, refer to Microsoft Azure Support documentation. If IBM Support determines that your issue is caused by the Microsoft Azure infrastructure, you must contact Microsoft for support to resolve the underlying issue with the Microsoft Azure infrastructure.

You must use static IP addresses.

You cannot have more than two DNS entries. QRadar installation fails if you have more than two DNS entries in the `/etc/resolv.conf` file.

The App Host must be the same version as your Console before you can add the App Host to your deployment. You can upgrade the App Host to a later version of QRadar after you complete the installation by downloading the fix pack from Fix Central (https://www.ibm.com/support/fixcentral) and following the normal upgrade procedure. For more information about upgrades, see *IBM QRadar Upgrade Guide*.

If you are installing a data gateway for QRadar on Cloud, go to Installing a QRadar data gateway in Microsoft Azure (https://www.ibm.com/support/knowledgecenter/en/SSKMKU/com.ibm.qradar.doc_cloud/t_hosted_azure.html).

If you deploy a managed host and a Console in the same virtual network, use the private IP address of the managed host to add it to the Console.

If you deploy a managed host and a Console in different virtual networks, you must allow firewall rules for the communication between the Console and the managed host. For more information, see "QRadar port usage " on page 122.

You must complete all of the installation steps before you run QRadar commands such as **qchange_netsetup**.

For more information about configuring firewall rules between hosts, see Microsoft documentation.

Procedure

1. Go to the Microsoft Azure Marketplace (https://azuremarketplace.microsoft.com/en-us/marketplace/apps/ibm.qradar733?tab=Overview).

   Note: The **Plans + Pricing** tab can be used to estimate pricing for certain VM sizes, but you don't choose your VM size on this screen. Refer to the **Core** and **RAM** columns when you are estimating pricing. Ignore the **Disk Space** column, as all QRadar marketplace images include a disk for the operating system, and a 1 TB disk for storage.
2. Click **Get It Now**.
3. Select **QRadar SIEM AH 7.3.3** from the **Software plan** menu list and click **Continue**.
4. Click **Create** to create an instance of the virtual appliance.
5. Configure VM settings.
   a) Select an existing **Resource Group** or create a new one.
   b) Enter a virtual machine name.

      Note: The VM name must be 10 characters or fewer.
   c) Select a **Region**.
   d) Click **Change size** and ensure that your VM meets the minimum system requirements.
      For more information, see "System requirements for virtual appliances" on page 24.
   e) Enter a username for the administrator account.
   f) Choose an **SSH public key** or **Password**.

      For more information about creating and using an SSH public-private key pair for Linux VMs in Microsoft Azure, see Microsoft documentation.
   g) Set **Public inbound ports** to **Allow selected ports**.
   h) Set **Select inbound ports** to **SSH (22)** and **HTTPS (443)**.
6. Click **Review + Create**.
7. Click **Create** to deploy the instance.
8. When your VM is deployed in Microsoft Azure, set the private and public IP addresses to static.
   a) Click **Go to resource**.
   b) Click the public IP address.
   c) Set the **Assignment** to **Static**.
   d) Click **Save**.
   e) Click **Overview**.
   f) Click the **Associated to** link.
   g) Click **IP configurations**.
   h) In the list of IP configurations, click the configuration row where the **Type** is set to Primary.

i) Set the Private IP address assignment to **Static**.

j) Click **Save**.

9. Create or select a security group that allows ports 22 and 443 only from trusted IP addresses to create an allowlist of IP addresses that can access your QRadar deployment.

   In a QRadar deployment with multiple appliances, other ports might also be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see "Common ports and servers used by QRadar" on page 122.

   a) Click **Home**.

   b) Click **Virtual Machines** .

   c) Click the name of your virtual machine.

   d) Click **Networking**.

   e) Click the SSH rule that is associated with port 22.

   f) In the edit pane, select **IP Addresses** from the **Source** list.

   g) In the **Source IP addresses/CIDR ranges** field, enter the address range of the IP addresses that are allowed to access the VM.

   h) Click **Save**.

   i) Click the HTTPS rule that is associated with port 443.

   j) In the edit pane, select **IP Addresses** from the **Source** list.

   k) In the **Source IP addresses/CIDR ranges** field, enter the address range of the IP addresses that are allowed to access the VM.

   l) Click **Save**.

10. To display the SSH connection information for the public IP address of the virtual appliance.

    a) Click **Virtual Machines** > **<virtual_machine_name>**.

    b) Click **Connect**.

11. Log in to your virtual machine.

    - To log in using SSH and your key pair, type the following command:

      ```
      ssh -i <key.pem> user@<public_IP_address>
      ```

    - To log in using SSH and your password, type the following command:

      ```
      ssh user@<public_IP_address>
      ```

12. To check that the hostname is a fully qualified domain name (FQDN), type the following command:

    ```
    hostname -f
    ```

    If the command returns a hostname that is not an FQDN, DNS is misconfigured and installation fails. Restart this procedure with proper DNS configuration. For more information about DNS configuration, see the Microsoft Azure Support documentation.

13. To check the length of your FQDN, type the following command:

    ```
    hostname -f | wc -c
    ```

    If the command returns a value greater than 63, installation fails. Restart this procedure with a shorter virtual machine name.

14. Ensure that there are no more than 2 DNS entries for the instance by typing the following command:

    ```
    grep nameserver /etc/resolv.conf | wc -l
    ```

    If the command returns 3 or higher, edit `/etc/resolv.conf` to remove all but two of the entries before you proceed to the next step. You will add the entries back after installation is complete.

What to do next

If you need to increase file system storage beyond the default 1 TB, follow the steps in "Increasing file system storage for a new App Host by recreating the data disk at a larger size" on page 87. Increase the file system storage before you complete the installation if possible, as increasing file system storage on a running system is more risky than increasing it before installation is complete.

If you don't need more than 1 TB of storage, proceed to "Installing the App Host" on page 92.

If you need to change your hostname or FQDN, run the **qchange_netsetup** command.

Increasing file system storage for a new App Host by recreating the data disk at a larger size

Increase the size of the file system on the App Host by recreating the existing data disk at a larger size and by using the Red Hat LVM logical volume manager.

Before you begin

For more information about expanding the size of a disk, see Microsoft documentation.

About this task

Warning: This procedure is for new installations only, and must be complete before completing the steps in "Installing the App Host" on page 92. Following these steps after installation is complete will result in errors and data loss.

Procedure

1. Stop your virtual machine (VM).
2. Click **Disks**.

   Warning: Do not add more disks.

   To increase storage to less than 4095 GiB:

   a) Click on the data disk link.
   b) Click **Size + performance**.
   c) Choose from the list, or enter the new disk size in GiB.
   d) Click **Save**.

   To increase storage to more than 4095 GiB:

   a) Click **Edit**.
   b) Click the **X** next to the data disk to detach the disk.
   c) Click **Save**.
   d) Click **Home**.
   e) Click **Disks**.
   f) Click the disk associated with the VM that you are editing.
   g) Click **Size + performance**.
   h) Enter the new disk size in GiB.
   i) Click **Save**.
   j) Go to the Home screen and click **Virtual machines**
   k) Click the name of your virtual machine.
   l) Click **Disks**.
   m) Click **+ Add data disk**.

n) Select the disk that you modified.

o) Click **Save**.

3. After the data disk is expanded, restart your VM.
4. Log in to your VM by using **ssh**.
5. Determine the device name and partition number for the `/store` and `/transient` file systems by typing the following command:

```
lsblk
```

In this example **lsblk** output, for the `/store` and `/transient` file systems the *<device_name>* is sdc, the *<partition_number>* is 1, and the *<volume_group>* is data.

```
NAME                    MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
fd0                       2:0    1     4K  0 disk
sda                       8:0    0    98G  0 disk
├─sda1                    8:1    0     1G  0 part /boot
├─sda2                    8:2    0    20G  0 part /
├─sda3                    8:3    0   200M  0 part /boot/efi
├─sda4                    8:4    0     1K  0 part
└─sda5                    8:5    0  76.8G  0 part
  ├─rhel-var            253:0    0     8G  0 lvm  /var
  ├─rhel-var_log        253:1    0    18G  0 lvm  /var/log
  ├─rhel-temp           253:2    0     8G  0 lvm  /temp
  ├─rhel-storetmp       253:3    0    15G  0 lvm  /storetmp
  ├─rhel-opt            253:4    0    14G  0 lvm  /opt
  ├─rhel-home           253:5    0     6G  0 lvm  /home
  └─rhel-var_log_audit  253:6    0   7.8G  0 lvm  /var/log/audit
sdb                       8:16   0    32G  0 disk
└─sdb1                    8:17   0    32G  0 part /mnt/resource
sdc                       8:32   0     6T  0 disk
└─sdc1                    8:33   0  1022G  0 part
  ├─data-transient      253:7    0 204.4G  0 lvm  /transient
  └─data-store          253:8    0 817.6G  0 lvm  /store
```

6. Become the super user by typing the following command and entering your password when promoted:

```
sudo -i
```

7. Open the **parted** prompt by typing the following command:

```
parted /dev/<device_name>
```

Example command:

```
parted /dev/sdc
```

8. Switch the units displayed to MiB by typing the following command:

```
unit mib
```

```
p
```

9. When prompted with "Error: The backup GPT table is not at the end of the disk...", enter `Fix`.
10. When prompted with "Warning: Not all of the space available ...", enter `Fix`.
11. Resize the partition to fill the disk by typing the following command:

```
resizepart <partition_number> 100%
```

Example command:

```
resizepart 1 100%
```

12. Exit parted by typing the following command:

```
quit
```

13. Ensure that the kernel recognizes the new partition information by typing the following command:

    ```
    partprobe /dev/<device_name><partition_number>
    ```

    Example command:

    ```
    partprobe /dev/sdc1
    ```

    There is no output for this step if it is successful.

    - If there is no output, proceed directly to the next step.
    - If there is output that indicates that **partprobe** didn't detect the new partitions, reboot the system before you continue to the next step.
14. Grow the physical volume to fill the extra disk space by typing the following command:

    ```
    pvresize /dev/<device_name><partition_number>
    ```

    Example command:

    ```
    pvresize /dev/sdc1
    ```

    Example successful output:

    ```
    Physical volume "/dev/sdc1" changed
      1 physical volume(s) resized / 0 physical volume(s) not resized
    ```
15. Expand /transient by 20% of the extra disk space by typing the following command:

    ```
    lvextend -l +20%FREE /dev/<volume_group>/transient
    ```

    Example command:

    ```
    lvextend -l +20%FREE /dev/data/transient
    ```

    Example successful output:

    ```
    Size of logical volume data/transient changed from <204.40 GiB (52326 extents) to 1.20 TiB
    (314573 extents).
      Logical volume data/transient successfully resized.
    ```
16. Expand /store into the remaining extra disk space by typing the following command:

    ```
    lvextend -l +100%FREE /dev/<volume_group>/store
    ```

    Example command:

    ```
    lvextend -l +100%FREE /dev/data/store
    ```

    Example successful output:

    ```
    Size of logical volume data/store changed from <817.60 GiB (209305 extents) to 4.00 TiB
    (1048985 extents).
      Logical volume data/store successfully resized.
    ```
17. Reformat the /store file system:
    a) Unmount the /store file system by typing the following command:

       ```
       umount /dev/mapper/<volume_group>-store
       ```

       Example command:

       ```
       umount /dev/mapper/data-store
       ```

    b) Construct the XFS file system for /store by typing the following command:

       ```
       mkfs.xfs -f /dev/mapper/<volume_group>-store
       ```

       Example command:

```
mkfs.xfs -f /dev/mapper/data-store
```

Example successful output:

```
meta-data=/dev/mapper/data-store isize=512    agcount=5, agsize=268435455 blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=0, sparse=0
data     =                       bsize=4096   blocks=1074160640, imaxpct=5
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal log           bsize=4096   blocks=521728, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

c) Verify that the XFS file system for `/store` is not damaged by typing the following command:

```
xfs_repair /dev/mapper/<volume_group>-store
```

Example command:

```
xfs_repair /dev/mapper/data-store
```

Example successful output:

```
Phase 1 - find and verify superblock...
Phase 2 - using internal log
        - zero log...
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan and clear agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - agno = 4
        - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
        - setting up duplicate extent list...
        - check for inodes claiming duplicate blocks...
        - agno = 0
        - agno = 1
        - agno = 3
        - agno = 4
        - agno = 2
Phase 5 - rebuild AG headers and trees...
        - reset superblock...
Phase 6 - check inode connectivity...
        - resetting contents of realtime bitmap and summary inodes
        - traversing filesystem ...
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
done
```

d) Mount the `/store` file system by typing the following command:

```
mount /dev/mapper/<volume_group>-store
```

Example command:

```
mount /dev/mapper/data-store
```

18. Reformat the `/transient` file system:

a) Unmount the `/transient` file system by typing the following command:

```
umount /dev/mapper/<volume_group>-transient
```

Example command:

```
umount /dev/mapper/data-transient
```

b) Construct the XFS file system for `/transient` by typing the following command:

```
mkfs.xfs -f /dev/mapper/<volume_group>-transient
```

Example command:

```
mkfs.xfs -f /dev/mapper/data-transient
```

Example successful output:

```
meta-data=/dev/mapper/data-transient isize=512    agcount=4, agsize=80530688 blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=0, sparse=0
data     =                       bsize=4096   blocks=322122752, imaxpct=5
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal log           bsize=4096   blocks=157286, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

c) Verify that the XFS file system for `/transient` is not damaged by typing the following command:

```
xfs_repair /dev/mapper/<volume_group>-transient
```

Example command:

```
xfs_repair /dev/mapper/data-transient
```

Example successful output:

```
Phase 1 - find and verify superblock...
Phase 2 - using internal log
        - zero log...
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan and clear agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
        - setting up duplicate extent list...
        - check for inodes claiming duplicate blocks...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
Phase 5 - rebuild AG headers and trees...
        - reset superblock...
Phase 6 - check inode connectivity...
        - resetting contents of realtime bitmap and summary inodes
        - traversing filesystem ...
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
done
```

d) Mount the `/transient` file system by typing the following command:

```
mount /dev/mapper/<volume_group>-transient
```

Example command:

```
mount /dev/mapper/data-transient
```

19. Verify that the new sizes of the expanded file systems are correct by typing the following command:

```
df -h
```

Example successful output:

```
Filesystem                    Size  Used Avail Use% Mounted on
/dev/sda2                      20G  1.2G   18G   7% /
devtmpfs                      7.9G     0  7.9G   0% /dev
```

```
tmpfs                           7.9G     0  7.9G   0% /dev/shm
tmpfs                           7.9G  9.1M  7.9G   1% /run
tmpfs                           7.9G     0  7.9G   0% /sys/fs/cgroup
/dev/sda1                       976M  127M  783M  14% /boot
/dev/sda3                       200M  8.0K  200M   1% /boot/efi
/dev/mapper/rhel-var            8.0G  178M  7.9G   3% /var
/dev/mapper/rhel-opt             14G  3.5G   11G  25% /opt
/dev/mapper/rhel-storetmp        15G   33M   15G   1% /storetmp
/dev/mapper/rhel-temp           8.0G   33M  8.0G   1% /temp
/dev/mapper/rhel-home           6.0G   33M  6.0G   1% /home
/dev/mapper/rhel-var_log         18G   44M   18G   1% /var/log
/dev/mapper/rhel-var_log_audit  7.8G   70M  7.8G   1% /var/log/audit
/dev/sdb1                        32G   13G   20G  38% /mnt/resource
tmpfs                           1.6G     0  1.6G   0% /run/user/1000
/dev/mapper/data-store          4.0T   33M  4.0T   1% /store
/dev/mapper/data-transient      1.2T   33M  1.2T   1% /transient
```

20. Reboot the VM.
21. Log in to your virtual machine.
    - To log in using SSH and your key pair, type the following command:

      ```
      ssh -i <key.pem> user@<public_IP_address>
      ```

    - To log in using SSH and your password, type the following command:

      ```
      ssh user@<public_IP_address>
      ```

Results

If you increased the file system storage, you may see the following warning when you log in to the system:

```
WARNING:********************************************************************
WARNING: QRadar requires 4092M of swap space but was only able to find
WARNING: 0M, please increase swap space by at least 4092M. Without this
WARNING: additional swap space, some components of QRadar will not function
WARNING: properly (such as complex queries or reports). Please contact
WARNING: Customer Support for further details and assistance in resolving
WARNING: this issue.
WARNING:********************************************************************
```

This warning after increasing file system storage on a new VM in Microsoft Azure is benign. This warning is displayed because the swap space for the VM is being updated in the Microsoft Azure infrastructure. You can proceed with the installation.

What to do next

Follow the steps in “Installing the App Host” on page 92.

Installing the App Host

Procedure

1. Type the following command to install the App Host:

   ```
   sudo /root/setup_apphost
   ```

2. The system prompts you to set a root password. Set a strong root password that meets the following criteria.
   - Contains at least 5 characters
   - Contains no spaces
   - Can include the following special characters, unless you are installing a data gateway: @, #, ^, and *.
3. Ensure that the App Host is the same version as your Console, then add the host to your deployment in QRadar.

   a) On the navigation menu (☰), click **Admin**.

b) In the **System Configuration** section, click **System and License Management**.

c) In the **Display** list, select **Systems**.

d) On the **Deployment Actions** menu, click **Add Host**.

e) Configure the settings for the managed host by providing a static IP address, and the root password to access the operating system shell on the appliance.

f) Click **Add**.

g) Optional: Use the **Deployment actions** > **View Deployment** menu to see visualizations of your deployment. You can download a PNG image or a Microsoft Visio (2010) VDX file of your deployment visualization.

h) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

Important: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

What to do next

If you removed any DNS entries in `/etc/resolv.conf`, restore them.

Important: IBM QRadar 7.3.3 has reached End of Support. To ensure that support is available, an upgrade must be performed. For information about upgrading to 7.4.3, see Upgrading QRadar SIEM.

Configuring a Console in Oracle Cloud

Configure an IBM QRadar SIEM Console on an Oracle Cloud instance by using the Oracle Cloud image on Fix Central.

Before you begin

You must acquire entitlement to a QRadar Software Node before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with Oracle Cloud infrastructure, refer to Oracle Cloud documentation. If IBM Support determines that your issue is caused by the Oracle Cloud infrastructure, you must contact Oracle Cloud for support to resolve the underlying issue with the Oracle Cloud infrastructure.

About this task

If you are installing a data gateway for QRadar on Cloud, go to installing a QRadar data gateway in Oracle Cloud.

You must use static IP addresses.

You cannot have more than two DNS entries. QRadar installation fails if you have more than two DNS entries in the /etc/resolv.conf file.

Do not make any configuration changes, such as adding extra DNS entries, until after QRadar installation is complete.

If you deploy a managed host and a Console in the same virtual network, use the private IP address of the managed host to add it to the Console.

If you deploy a managed host and a Console in different virtual networks, you must allow firewall rules for the communication between the Console and the managed host. For more information, see QRadar port usage.

Procedure

1. Download the image file.
   a) Go to the CLOUD MARKET PLACE section of Fix Central (https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.4.0&platform=Linux&function=all).
   b) Click **7.4.1-CMP-OracleCloud-CONSOLE-QRADAR-20220811114721**.
   c) Download the image and `.sig` files.

      The image file download can take several hours.
   d) Use the `.sig` file to verify the integrity of the image file.

      For more information, see how to verify downloads from IBM Fix Central are trusted and code signed.
2. Upload the image file.
   a) Go to Oracle Cloud (https://www.oracle.com/ca-en/cloud/) and create a new storage bucket.
   b) Upload the file.

      The upload can take up to an hour. Do not rename the image file. Renaming the file causes the import to fail.
3. Import the image.
   a) In Oracle Cloud, click **Navigation Menu** > **Compute** > **Custom images**.
   b) Select a **Compartment**.
   c) Click **Import Image**.
   d) Enter a name for the image.
   e) Select **Linux** as the Operating system.
   f) Select **Import from an Object Storage Bucket**.
   g) Select the bucket that you uploaded the image file to from step 2.
   h) Select the image file that you uploaded from step 2.
   i) Select **OCI** for the image type.
   j) Click **Import Image**.
4. When the image is created, click **Create Instance**.
5. Give your instance a name that is no longer than 58 characters. The name can contain only alphanumeric characters and the - symbol.
6. Select a compartment for the instance.
7. Select an availability domain for the instance.
8. Select a shape that meets the minimum system requirements.
   a) Click **Change Shape**.
   b) Click **Virtual machine** as the Instance type.
   c) Select any shape from the AMD, Intel, or Specialty and previous generation shape series that meets the system requirements for virtual appliances.

      Important: Instances that contain extra storage drives are not supported.

      For more information, see the IBM QRadar Installation Guide.
9. Configure networking for the instance.
   a) Select a virtual cloud network compartment.
   b) Select a virtual cloud network.
   c) Select a subnet.
   d) Select **Assign a public IPv4 address**.
   e) Under Show Advanced Options check **Use network security groups to control traffic**.

f) Select a security group that allows port 22, and port 443 for a QRadar Console, to create an allowlist of trusted IP addresses that can access your QRadar deployment. In a QRadar deployment with multiple appliances, other ports might also be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see Common ports and servers that are used by QRadar.

10. Add or generate an SSH key pair.

    You need an SSH key pair to access the instance by using SSH. For more information, see connecting to your instance.

11. Click **Create**.
12. Add a second disk to your instance for storage.
    a) Go to **Navigation Menu** > **Storage** > **Block Volumes** and click **Create Block Volume**.
    b) Name the volume and enter a size in GB.

    The minimum size is 250 GiB. The added disk must be the second disk. It cannot be the third or greater disk. When the installation is complete, this disk contains the `/store` and `/transient` partitions.

    Warning: It is not possible to increase storage after installation.

    c) Select the same compartment that your instance was created in.
    d) Click **Create Block Volume**.
    e) Go to **Navigation Menu** > **Compute** > **Instances** and select your instance.
    f) Click **Attached Block Volumes**.
    g) Click **Attach Block Volume**.
    h) Select your block volume from the drop-down menu, then select **Paravirtualized** as the attachment type.
    i) Click **Attach**.
13. When the instance is ready, log in using the private key from your key pair.

```
ssh -i <private_key_file> cloud-user@<public_IP_address>
```

14. Type the following command to install the console:

```
sudo /root/setup_console
```

15. Enter a password for the admin account. Set a strong password that meets the following criteria:
    - Contains at least 5 characters.
    - Contains no spaces.
    - Includes one or more of the following special characters: @, #, ^, and *.

What to do next

If you removed any DNS entries in `/etc/resolv.conf`, restore them.

The QRadar instance uses Coordinated Universal Time (UTC). You can change the time zone of the instance. For more information about changing the time zone, see IBM QRadar Administration Guide.

This image does not receive automatic software upgrades. You must manually upgrade your system to keep it up to date. To receive QRadar upgrade notifications, see IBM QRadar Upgrade Guide.

Configuring an App Host in Oracle Cloud

Configure an IBM QRadar SIEM App Host on an Oracle Cloud instance by using the Oracle Cloud image on Fix Central.

Before you begin

You must acquire entitlement to a QRadar Software Node before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with Oracle Cloud infrastructure, refer to Oracle Cloud documentation. If IBM Support determines that your issue is caused by the Oracle Cloud infrastructure, you must contact Oracle Cloud for support to resolve the underlying issue with the Oracle Cloud infrastructure.

About this task

If you are installing a data gateway for QRadar on Cloud, go to installing a QRadar data gateway in Oracle Cloud.

You must use static IP addresses.

You cannot have more than two DNS entries. QRadar installation fails if you have more than two DNS entries in the /etc/resolv.conf file.

Do not make any configuration changes, such as adding extra DNS entries, until after QRadar installation is complete.

If you deploy a managed host and a Console in the same virtual network, use the private IP address of the managed host to add it to the Console.

If you deploy a managed host and a Console in different virtual networks, you must allow firewall rules for the communication between the Console and the managed host. For more information, see QRadar port usage.

Procedure

1. Download the image file.
   a) Go to the CLOUD MARKET PLACE section of Fix Central (https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.4.0&platform=Linux&function=all).
   b) Click **7.4.1-CMP-OracleCloud-APPHOST-QRADAR-20220811114721**.
   c) Download the image and `.sig` files.
      The image file download can take several hours.
   d) Use the `.sig` file to verify the integrity of the image file.
      For more information, see how to verify downloads from IBM Fix Central are trusted and code signed.
2. Upload the image file.
   a) Go to Oracle Cloud (https://www.oracle.com/ca-en/cloud/) and create a new storage bucket.
   b) Upload the file.
      The upload can take up to an hour. Do not rename the image file. Renaming the file causes the import to fail.
3. Import the image.
   a) In Oracle Cloud, click **Navigation Menu** > **Compute** > **Custom images**.
   b) Select a **Compartment**.
   c) Click **Import Image**.

d) Enter a name for the image.

e) Select **Linux** as the Operating system.

f) Select **Import from an Object Storage Bucket**.

g) Select the bucket that the image file was uploaded to in step 2.

h) Select the image file that was uploaded in step 2.

i) Select **OCI** for the image type.

j) Click **Import Image**.

4. When the image is created, click **Create Instance**.
5. Give your instance a name that is no longer than 58 characters. The name can contain only alphanumeric characters and the - symbol.
6. Select a compartment for the instance.
7. Select an availability domain for the instance.
8. Select a shape that meets the minimum system requirements.

   a) Click **Change Shape**.

   b) Click **Virtual machine** as the Instance type.

   c) Select any shape from the AMD, Intel, or Specialty and previous generation shape series that meets the system requirements for virtual appliances.

   Important: Instances that contain extra storage drives are not supported.

   For more information, see the IBM QRadar Installation Guide.
9. Configure networking for the instance.

   a) Select a virtual cloud network compartment.

   b) Select a virtual cloud network.

   c) Select a subnet.

   d) Select **Assign a public IPv4 address**.

   e) Under Show Advanced Options check **Use network security groups to control traffic**.

   f) Select a security group that allows port 22, and port 443 for a QRadar Console, to create an allowlist of trusted IP addresses that can access your QRadar deployment. In a QRadar deployment with multiple appliances, other ports might also be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see Common ports and servers that are used by QRadar.
10. Add or generate an SSH key pair.

    You need an SSH key pair to access the instance by using SSH. For more information, see connecting to your instance.
11. Click **Create**.
12. Add a second disk to your instance for storage.

    a) Go to **Navigation Menu** > **Storage** > **Block Volumes** and click **Create Block Volume**.

    b) Name the volume and enter a size in GB.

    The minimum size is 250 GiB. The added disk must be the second disk. It cannot be the third or greater disk. When the installation is complete, this disk contains the `/store` and `/transient` partitions.

    Warning: It is not possible to increase storage after installation.

    c) Select the same compartment that your instance was created in.

    d) Click **Create Block Volume**.

    e) Go to **Navigation Menu** > **Compute** > **Instances** and select your instance.

    f) Click **Attached Block Volumes**.

g) Click **Attach Block Volume**.

h) Select your block volume from the drop-down menu, then select **Paravirtualized** as the attachment type.

i) Click **Attach**.

13. When the instance is ready, log in using the private key from your key pair.

```
ssh -i <private_key_file> cloud-user@<public_IP_address>
```

14. Type the following command to install the app host:

```
sudo /root/setup_apphost
```

15. When prompted to set the root password, set a strong password that meets the following criteria:

- Contains at least 5 characters.
- Contains no spaces.
- Includes one or more of the following special characters: @, #, ^, and *.

16. Add the host to your deployment in QRadar.

a) On the navigation menu, click **Admin**.

b) In the **System Configuration** section, click **System and License Management**.

c) In the **Display** list, select **Systems**.

d) On the **Deployment Actions** menu, click **Add Host**.

e) Configure the settings for the host by providing the private IP address, and the root password to access the operating system shell on the appliance.

f) Click **Add**.

g) Optional: Use the **Deployment actions** > **View Deployment** menu to see visualizations of your deployment. You can download a PNG image or a Microsoft Visio (2010) VDX file of your deployment visualization.

h) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

Important: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

17. Change where your apps are run in QRadar.

a) On the System and License Management screen, click the **Click to change where apps run** link.

b) Click **App Host** to transfer apps to the App Host.

Note: The more apps and app data you have, the longer the transfer takes.

What to do next

If you removed any DNS entries in `/etc/resolv.conf`, restore them.

Configuring a managed host in Oracle Cloud

Configure an IBM QRadar SIEM managed host on an Oracle Cloud instance by using the Oracle Cloud image on Fix Central.

Before you begin

You must acquire entitlement to a QRadar Software Node before you deploy the QRadar instance. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

For any issues with QRadar software, engage IBM Support. If you experience any problems with Oracle Cloud infrastructure, refer to Oracle Cloud documentation. If IBM Support determines that your issue

is caused by the Oracle Cloud infrastructure, you must contact Oracle Cloud for support to resolve the underlying issue with the Oracle Cloud infrastructure.

About this task

If you are installing a data gateway for QRadar on Cloud, go to installing a QRadar data gateway in Oracle Cloud.

You must use static IP addresses.

You cannot have more than two DNS entries. QRadar installation fails if you have more than two DNS entries in the /etc/resolv.conf file.

Do not make any configuration changes, such as adding extra DNS entries, until after QRadar installation is complete.

If you deploy a managed host and a Console in the same virtual network, use the private IP address of the managed host to add it to the Console.

If you deploy a managed host and a Console in different virtual networks, you must allow firewall rules for the communication between the Console and the managed host. For more information, see QRadar port usage.

Procedure

1. Download the image file.
   a) Go to the CLOUD MARKET PLACE section of Fix Central (https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.4.0&platform=Linux&function=all).
   b) Click **7.4.1-CMP-OracleCloud-MANAGEDHOST-QRADAR-20220811114721**.
   c) Download the image and `.sig` files.
      The image file download can take several hours.
   d) Use the `.sig` file to verify the integrity of the image file.
      For more information, see how to verify downloads from IBM Fix Central are trusted and code signed.
2. Upload the image file.
   a) Go to Oracle Cloud (https://www.oracle.com/ca-en/cloud/) and create a new storage bucket.
   b) Upload the file.
      The upload can take up to an hour. Do not rename the image file. Renaming the file causes the import to fail.
3. Import the image.
   a) In Oracle Cloud, click **Navigation Menu** > **Compute** > **Custom images**.
   b) Select a **Compartment**.
   c) Click **Import Image**.
   d) Enter a name for the image.
   e) Select **Linux** as the Operating system.
   f) Select **Import from an Object Storage Bucket**.
   g) Select the bucket that the image file was uploaded to in step 2.
   h) Select the image file that was uploaded in step 2.
   i) Select **OCI** for the image type.
   j) Click **Import Image**.
4. When the image is created, click **Create Instance**.

5. Give your instance a name that is no longer than 58 characters. The name can contain only alphanumeric characters and the - symbol.
6. Select a compartment for the instance.
7. Select an availability domain for the instance.
8. Select a shape that meets the minimum system requirements.
   a) Click **Change Shape**.
   b) Click **Virtual machine** as the Instance type.
   c) Select any shape from the AMD, Intel, or Specialty and previous generation shape series that meets the system requirements for virtual appliances.

      Important: Instances that contain extra storage drives are not supported.

      For more information, see the IBM QRadar Installation Guide.
9. Configure networking for the instance.
   a) Select a virtual cloud network compartment.
   b) Select a virtual cloud network.
   c) Select a subnet.
   d) Select **Assign a public IPv4 address**.
   e) Under Show Advanced Options check **Use network security groups to control traffic**.
   f) Select a security group that allows port 22, and port 443 for a QRadar Console, to create an allowlist of trusted IP addresses that can access your QRadar deployment. In a QRadar deployment with multiple appliances, other ports might also be allowed between managed hosts. For more information about what ports might need to be allowed in your deployment, see Common ports and servers that are used by QRadar.
10. Add or generate an SSH key pair.

    You need an SSH key pair to access the instance by using SSH. For more information, see connecting to your instance.
11. Click **Create**.
12. Add a second disk to your instance for storage.
    a) Go to **Navigation Menu** > **Storage** > **Block Volumes** and click **Create Block Volume**.
    b) Name the volume and enter a size in GB.

       The minimum size is 250 GiB. The added disk must be the second disk. It cannot be the third or greater disk. When the installation is complete, this disk contains the `/store` and `/transient` partitions.

       Warning: It is not possible to increase storage after installation.
    c) Select the same compartment that your instance was created in.
    d) Click **Create Block Volume**.
    e) Go to **Navigation Menu** > **Compute** > **Instances** and select your instance.
    f) Click **Attached Block Volumes**.
    g) Click **Attach Block Volume**.
    h) Select your block volume from the drop-down menu, then select **Paravirtualized** as the attachment type.
    i) Click **Attach**.
13. When the instance is ready, log in using the private key from your key pair.

    ```
    ssh -i <private_key_file> cloud-user@<public_IP_address>
    ```
14. Type the following command to install the managed host:

```
sudo /root/setup_mh <appliance_id>
```

For example, to deploy an Event Collector type the following command:

```
sudo /root/setup_mh 1599
```

You can install the following managed host appliance types:

Appliance Type ID	Appliance Type
1299	Flow Collector
1400	Data Node
1599	Event Collector
1699	Event Processor
1799	Flow Processor
1899	Event and Flow Processor

15. When prompted to set the root password, set a strong password that meets the following criteria:
    - Contains at least 5 characters.
    - Contains no spaces.
    - Includes one or more of the following special characters: @, #, ^, and *.
16. Add the host to your deployment in QRadar.
    a) On the navigation menu, click **Admin**.
    b) In the **System Configuration** section, click **System and License Management**.
    c) In the **Display** list, select **Systems**.
    d) On the **Deployment Actions** menu, click **Add Host**.
    e) Configure the settings for the host by providing the private IP address, and the root password to access the operating system shell on the appliance.
    f) Click **Add**.
    g) Optional: Use the **Deployment actions** > **View Deployment** menu to see visualizations of your deployment. You can download a PNG image or a Microsoft Visio (2010) VDX file of your deployment visualization.
    h) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

    Important: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

What to do next

If you removed any DNS entries in `/etc/resolv.conf`, restore them.

Chapter 5. Installations from the recovery partition

When you install IBM QRadar products, the installer (ISO image) is copied to the recovery partition. From this partition, you can reinstall QRadar products. Your system is restored back to the default configuration. Your current configuration and data files are overwritten

When you restart your QRadar appliance, an option to reinstall the software is displayed. If you do not respond to the prompt within 5 seconds, the system continues to start as normal. Your configuration and data files are maintained. If you choose the reinstall option, a warning message is displayed and you must confirm that you want to reinstall.

The warning message states that you can retain the data on the appliance. This data includes events and flows. Selecting the retain option backs up the data before the reinstallation, and restores the data after installation completes. If the retain option is not available, the partition where the data resides may not be available, and it is not possible to back up and restore the data. The absence of the retain option can indicate a hard disk failure. Contact Customer Support if the retain option is not available.

Important: The retain option is not available on High-Availability systems. See the *IBM QRadar High Availability Guide* for information on recovering High-Availability appliances.

Reinstalling from the recovery partition

You can reinstall IBM QRadar products from the recovery partition.

Before you begin

If your deployment includes offboard storage solutions, you must disconnect your offboard storage before you reinstall QRadar. After you reinstall, you can remount your external storage solutions. For more information about configuring offboard storage, see the *Offboard Storage Guide*.

Warning: Software installations do not come with the recovery partition available, and also these instructions do not apply.

Procedure

1. Restart your QRadar appliance and select **Factory re-install**.
2. Type `flatten` or `retain`.

   The installer partitions and reformats the hard disk, installs the OS, and then reinstalls the QRadar product. You must wait for the flatten `or retain` process to complete. This process can take up to several minutes. When the process is complete, a confirmation is displayed.
3. Log in as the root user.
4. Ensure that the **End User License Agreement** (EULA) is displayed.

   Tip: Press the Spacebar key to advance through the document.
5. For QRadar Console installations, select the **Enterprise** tuning template.
6. Follow the instructions in the installation wizard to complete the installation.
7. If you are installing a Console, apply your license key.
   a) Log in to QRadar as the `admin` user:

      `https://<IP_Address_QRadar>`
   b) Click **Login**.
   c) On the navigation menu (☰), click **Admin**.
   d) In the navigation pane, click **System Configuration**.
   e) Click the **System and License Management** icon.

© Copyright IBM Corp. 2004, 2021

f) From the **Display** list box, select **Licenses**, and upload your license key.

g) Select the unallocated license and click **Allocate System to License**.

h) From the list of systems, select a system, and click **Allocate System to License**.

Chapter 6. Reinstalling QRadar from media

You can reinstall QRadar from a USB flash drive.

Before you begin

__ • Back up your data.

__ • On a Unified Extensible Firmware Interface (UEFI) system, remove the Grand Unified Bootloader (GRUB) entries for the existing QRadar installation from the UEFI boot loader before you reinstall QRadar.

1. At boot time, press F1 to enter **System Configuration and Boot Management**.
2. Select **Boot Manager**.
3. Select **Delete Boot Option**.
4. Check **grub**, then select **Commit Changes and Exit**.

Procedure

1. At boot time, press F12 to enter **Boot Devices Manager**.
2. Select your installation media from the list.
3. At the prompt, type `flatten`.
4. To reinstall QRadar, follow the instructions in “Installing a QRadar appliance” on page 11.

© Copyright IBM Corp. 2004, 2021

Chapter 7. Setting up a QRadar silent installation

Install IBM QRadar "silently," or perform an unattended installation.

Before you begin

- You must have the QRadar ISO for the release that you want to install.
- Modify the SELINUX value in the `/etc/sysconfig/selinux` file to `SELINUX=disabled`, and restart the system.
- You must install Red Hat Enterprise Linux (RHEL) on the system where you want to install QRadar. For more information, see Installing RHEL on your own appliance. The following table describes the version of Red Hat Enterprise Linux used with the IBM QRadar version.

Table 18. Red Hat version

IBM QRadar version	Red Hat Enterprise Linux version
IBM QRadar 7.4.0	Red Hat Enterprise Linux V7.6 64-bit
IBM QRadar 7.4.1	Red Hat Enterprise Linux V7.7 64-bit
IBM QRadar 7.4.2	Red Hat Enterprise Linux V7.7 64-bit
IBM QRadar 7.4.3	Red Hat Enterprise Linux V7.7 64-bit

Procedure

1. As the root user, use SSH to log on to the host where you want to install QRadar.
2. In the root directory of the host where you want to install QRadar, create a file that is named `AUTO_INSTALL_INSTRUCTIONS` and contains the following content:

Table 19. Silent Install File parameters. Parameters that are listed as "Optional" are required in the `AUTO_INSTALL_INSTRUCTIONS` file, but can have no value.

Parameter	Value Required?	Description	Permitted values
`force`	Required	Forces the installation of the appliance despite any hardware issues.	`true` or `false`
`api_auth_token`	Optional	An authorization token. For more information about managing authorized services, see the *IBM Security QRadar Administration Guide*.	Authorization token
`appliance_number`	Optional	The identifier for the appliance	`0`, `3105`, `1201`, and so on.
`appliance_oem`	Required	Identifies the appliance provider.	`qradar`, `forensics`, and so on.
`appliance_filter`	Required	The appliance name or identifier.	`vmware`, `na`
`bonding enabled`	Required.	Specifies whether you are using bonded interfaces.	`true` or `false`

© Copyright IBM Corp. 2004, 2021

Table 19. Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO_INSTALL_INSTRUCTIONS file, but can have no value. *(continued)*

Parameter	Value Required?	Description	Permitted values
bonding_interface	If using bonded interfaces, then required.	The MAC addresses for the interfaces that you are bonding, separated by commas.	*<interface_name=mac_address>*,*<secondary_interface_name=mac_address>*
bonding_interface_name	If using bonded interfaces, then required.	Identifies the bonding interface.	bond0
bonding_options	If using bonded interfaces, then required.	The Linux options for bonded interfaces. For more information about NIC bonding, see the *IBM Security QRadar Administration Guide*.	**Example:** miimon=100 mode=4 lacp_rate=1
ha_cluster_virtual_ip	Optional	Specifies the IP address for the HA cluster.	ip_address
hostname	Required	The fully qualified host name for your QRadar system.	
ip_protocol	Required	The IP protocol for this host.	ipv4, ipv6
ip_dns_primary	If ip_protocol is set to IPv4, then required	The primary DNS server.	A valid IPv4 address.
ip_dns_secondary	If ip_protocol is set to IPv4, then required	The secondary DNS server.	A valid IPv4 address.
ip_management_interface	Required	The interface name, and the MAC address of the management interface. You can use either, or both separated by "=".	
ipv4_address	If ip_protocol is set to IPv4, then required	The IP address of the host that you are installing the software on.	A valid IPv4 address

Table 19. Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO_INSTALL_INSTRUCTIONS file, but can have no value. *(continued)*

Parameter	Value Required?	Description	Permitted values
ipv4_address_public	If ip_protocol is set to IPv4, and NATed, then required	The public IP address of the host that you are installing the software on.	A valid IPv4 address
ipv4_gateway	If ip_protocol is set to IPv4, then required	The network gateway for this host	A valid IPv4 address
ipv4_nework_mask	If ip_protocol is set to IPv4, then required	The netmask for this host	
ip_v6_address	If ip_protocol is set to IPv6, then required	The IPv6 address of the QRadar installation if required.	A valid IPv6 address
ip_v6_address_public	If ip_protocol is set to IPv6, and NATed, then required	The public IP address of the host that you are installing the software on.	A valid IPv6 address
ip_v6_autoconf	Required	Specifies whether IPv6 is autoconfigured.	true or false
ip_v6_gateway	Not required	Leave empty.	
is_console	Required	Specifies whether this host is the console within the deployment	true - This host is the console in the deployment false - This is not the console and is another type of managed host (Event or Flow Processor, and so on)
is_console_standby	Required.	Specifies whether this host is an HA console standby	true or false

Table 19. Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO_INSTALL_INSTRUCTIONS file, but can have no value. *(continued)*

Parameter	Value Required?	Description	Permitted values
admin_password	Optional.	The password for the administrator account. You can encrypt the password if required. If you leave this parameter blank, the password is not updated.	<*password*> **Important:** Your company's security policies can prevent you from entering a password in a static file on the appliance. Defined, or leaving the value empty to use a previously entered password on an upgrade.
root_password	Required	The password for the root account. You can encrypt the password, if required. If you leave this parameter blank, the password is not updated.	<*password*> **Important:** Your company's security policies can prevent you from entering a password in a static file on the appliance. Defined, or leaving the value empty uses a previously entered password on an upgrade.
security _template	If isconsole is set to Y, then required	The security template This value must be consistent with the value entered in appliance_number.	Enterprise - for all SIEM-based hosts Logger - for Log Manager
time_current _date	Required	The current date for this host. Use the following format: YYYY/MM/DD format	
time_current _time	Required	The time for the host in the 24 hour format HH:MM:SS.	
time_ntp_server	Optional	The FQHN or IP address of the network time protocol (NTP) server.	
timezone	Required	The time zone from the TZ database. For more information, see http://timezonedb.com/.	Europe/London GMT America/Montreal America/New_York America/Los_Angeles Asia/Tokyo, and so on.

Table 19. Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO_INSTALL_INSTRUCTIONS file, but can have no value. *(continued)*

Parameter	Value Required?	Description	Permitted values
type_of_setup	Required	Specifies the type of installation for this host	normal- A standard QRadar managed host or console deployment. recovery - A High Availability (HA) recovery installation on this host.
console_host	Required for SIOC	The name for your IBM QRadar on Cloud system.	IP address
Gateway setup choice	Required for SIOC	Type True if this appliance is an IBM QRadar on Cloud gateway. Type False if the appliance is not a gateway appliance.	true or false
http_proxy_host	Optional	The host name of the proxy host for the IBM QRadar on Cloud appliance.	
http_proxy_password	Optional	The password for the proxy host for the IBM QRadar on Cloud appliance.	
http_proxy_port	Optional	The identifier for the port you connect to on the proxy host for the IBM QRadar on Cloud appliance.	
http_proxy_user	Optional	The user name for the proxy host for the IBM QRadar on Cloud appliance.	
internet_access_mode	Required for SIOC	The mode that you use to access the IBM QRadar on Cloud appliance	direct or proxy

Example:

```
#0.0.1
ai_force=<true_false>
ai_api_auth_token= <certificate>
ai_appliance_number= <####>
ai_appliance_oem= <qradar_forensics_or_oem>
ai_appliance_filter= <appliance_number_or_identifier>
ai_bonding_enabled= <true_or_false>
ai_bonding_interfaces= <mac_address>
ai_bonding_interface_name= <interface_identifier>
ai_bonding_options= <bonding_option_identifiers>
ai_gateway_setup_choice= <true_or_false>
ai_ha_cluster_virtual_ip= <IP_address>
ai_hostname= <hostname_with_FQDN>
ai_ip_dns_primary= <IP_address_of _primary_DNS>
ai_ip_dns_secondary= <IP_address_of_secondary DNS>
ai_ip_management_interface= <MAC_address>
ai_ip_protocol= <ipv4_or_ipv6>
ai_ip_v4_address= <IP_address>
ai_ip_v4_address_public= <public_IP_address>
ai_ip_v4_gateway= <IP_address_of_gateway>
ai_ip_v4_network_mask= <network_mask>
ai_ip_v6_address= <IPv6_address>
ai_ip_v6_address_public= <IPv6_public_address>
ai_ip_v6_autoconf= <true_false>
ai_ip_v6_gateway= <IP_address>
ai_is_console= <true_or_false>
```

```
ai_is_console_standby= <true_or_false>
ai_root_password= <password_for_root_account>
ai_security_template= <enterprise_or_logger>
ai_time_current_date= <yyyy-mm-dd>
ai_time_current_time= <hh:mm:ss>
ai_time_ntp_server= <ntpserver_hostserver>
ai_timezone= <EST_or_PST_or_timezone>
ai_type_of_setup= <normal_or_recovery>
ai_console_host= <IP_address_or_identifier_for_SIOC_7000_host>
ai_http_proxy_host= <SIOC_7000_proxy_hostname>
ai_http_proxy_password= <SIOC_7000_proxy_password>
ai_http_proxy_port= <SIOC_7000_proxy_port>
ai_http_proxy_user= <SIOC_7000_proxy_user_name>
ai_internet_access_mode= <SIOC_7000_direct_or_proxy>
```

Replace the configuration settings in the file with ones that are suitable for your environment.

Important: Ensure that the AUTO_INSTALL_INSTRUCTIONS file has no extension, such as .txt, or .doc. The installation does not succeed if the file has an extension.

3. Using an SFTP program copy the QRadar ISO to the host where you want to install QRadar.
4. On the host where you are installing, create a `/media/cdrom` directory on the host by using the following command:

```
mkdir /media/cdrom
```

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

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

6. Run the QRadar setup by using the following command:

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

7. Open the End User License Agreement (EULA) at `/media/cdrom/EULA.txt` and review.
8. To agree to the EULA, add `--accept-eula` to the `/media/cdrom/setup` command.

   When you add `--accept-eula`, you bypass the EULA prompt.

Chapter 8. Configuring bonded management interfaces

You can bond the management interface on QRadar hardware.

About this task

You can bond the management interfaces during the QRadar installation process, or after installation by following these steps.

You can bond non-management interfaces in the QRadar user interface after installation. See "Configuring network interfaces" in *IBM QRadar Administration Guide* for more information about configuring non-management interfaces.

Bonding modes 1 and 4 are supported. Mode 4 is the default.

Note: You must be physically logged in to your appliance, for example through IMM or iDRAC, for these steps. Do not use `ssh` for these steps.

Procedure

1. Change your network setup by typing the command `qchange_netsetup`.

   Note: If you attempt to run `qchange_netsetup` over a serial connection, the connection can be misidentified as a network connection. To run over a serial connection use `qchange_netsetup -y`. This command allows you to bypass the validation check that detects a network connection.

   Note: Verify all external storage which is not /store/ariel or /store is not mounted.
2. Select the protocol version that is used for the appliance.
3. Select **Yes** to continue with bonded network interface configuration.
4. Select interfaces to configure as bonded interfaces. The interfaces that you select must not already be configured.
5. Enter the bonding options.

   For more information about configuring specific bonding options, see your vendor-specific operating system documentation.
6. Update any network information settings as needed.

   Your appliance restarts automatically.
7. Log in to the appliance and verify the configuration.

© Copyright IBM Corp. 2004, 2021

Chapter 9. Network settings management

Use the `qchange_netsetup script` to change the network settings of your IBM QRadar system. Configurable network settings include host name, IP address, network mask, gateway, DNS addresses, public IP address, and email server.

Changing the network settings in an all-in-one system

You can change the network settings in your all-in-one system. An all-in-one system has all IBM QRadar components that are installed on one system.

Before you begin

- You must have a local connection to your QRadar Console
- Confirm that there are no undeployed changes.
- If you are changing the IP address host name of a box in the deployment you must remove it from the deployment.
- If this system is part of an HA pair you must disable HA first before you change any network settings.
- If the system that you want to change is the console, you must remove all hosts in the deployment before proceeding.

Important: You cannot change the IP address of any host to the IP address of a previously deleted Managed Host.

Procedure

1. Log in to as the root user.
2. Type the following command:

   `qchange_netsetup`

   Important:

   - If you attempt to run `qchange_netsetup` over a serial connection, the connection can be misidentified as a network connection. To run over a serial connection use `qchange_netsetup -y`. This command allows you to bypass the validation check that detects a network connection.
   - Verify all external storage which is not /store/ariel or /store is not mounted.
3. Follow the instructions in the wizard to complete the configuration.

   The following table contains descriptions and notes to help you configure the network settings.

Table 20. Description of network settings for an all-in-one QRadar Console

Network Setting	Description
Internet Protocol	IPv4 or IPv6
Host name	Fully qualified domain name
Secondary DNS server address	Optional

© Copyright IBM Corp. 2004, 2021

Table 20. Description of network settings for an all-in-one QRadar Console (continued)	
Network Setting	**Description**
Public IP address for networks that use Network Address Translation (NAT)	Optional Used to access the server, usually from a different network or the Internet. Configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. (NAT translates an IP address in one network to a different IP address in another network).
Email server name	If you do not have an email server, use `localhost`.

A series of messages are displayed as QRadar processes the requested changes. After the requested changes are processed, the QRadar system is automatically shutdown and restarted.

Changing the network settings of a QRadar Console in a multi-system deployment

To change the network settings in a multi-system IBM QRadar deployment, remove all managed hosts, change the network settings, add the managed hosts again, and then reassign the component.

Before you begin

- You must have a local connection to your QRadar Console
- If you are adding a network adapter to either physical appliance or a virtual machine, you must shut down the appliance before you add the network adapter. Power on the appliance before you follow this procedure.

Important: You cannot change the IP address of any host to the IP address of a previously deleted Managed Host.

Procedure

1. To remove managed hosts, log in to QRadar:

   `https://`*`IP_Address_QRadar`*

   The **Username** is `admin`.

   a) On the navigation menu (☰), click **Admin**.

   b) Click the **System and License Management** icon.

   c) Select the managed host that you want to remove.

   d) Select **Deployment Actions** > **Remove Host**.

   e) in the **Admin** settings, click **Deploy Changes**.
2. Type the following command: `qchange_netsetup`.

   Important:

   - If you attempt to run `qchange_netsetup` over a serial connection, the connection can be misidentified as a network connection. To run over a serial connection use `qchange_netsetup -y`. This command allows you to bypass the validation check that detects a network connection.
   - Verify all external storage which is not /store/ariel or /store is not mounted.

3. Follow the instructions in the wizard to complete the configuration.

   The following table contains descriptions and notes to help you configure the network settings.

Table 21. Description of network settings for a multi-system QRadar Console deployment	
Network Setting	**Description**
Internet Protocol	IPv4 or IPv6
Host name	Fully qualified domain name
Secondary DNS server address	Optional
Public IP address for networks that use Network Address Translation (NAT)	Optional Used to access the server, usually from a different network or the Internet. Configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. (NAT translates an IP address in one network to a different IP address in another network).
Email server name	If you do not have an email server, use `localhost`.

   After you configure the installation parameters, a series of messages are displayed. The installation process might take several minutes.

4. To re-add and reassign the managed hosts, log in to QRadar.

   `https://`*`IP_Address_QRadar`*

   The **Username** is `admin`.

   a) On the navigation menu (☰), click **Admin**.

   b) Click the **System and License Management** icon.

   c) Click **Deployment Actions** > **Add Host**.

   d) Follow the instructions in the wizard to add a host.

      Select the **Network Address Translation** option to configure a public IP address for the server. This IP address is a secondary IP address that is used to access the server, usually from a different network or the Internet. The Public IP address is often configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. NAT translates an IP address in one network to a different IP address in another network

5. Reassign all components that are not your QRadar Console to your managed hosts .

   a) On the navigation menu (☰), click **Admin**.

   b) Click the **System and License Management** icon.

   c) Select the host that you want to reassign.

   d) Click **Deployment Actions** > **Edit Host Connection**.

   e) Enter the IP address of the source host in the **Modify Connection** window.

Chapter 10. Troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

Review the following table to help you or customer support resolve a problem.

Table 22. Troubleshooting actions to prevent problems

Action	Description
Apply all known fix packs, service levels, or program temporary fixes (PTF).	A product fix might be available to fix the problem.
Ensure that the configuration is supported.	Review the software and hardware requirements.
Look up error message codes by selecting the product from the IBM Support Portal (http://www.ibm.com/support/entry/portal) and then typing the error message code into the **Search support** box.	Error messages give important information to help you identify the component that is causing the problem.
Reproduce the problem to ensure that it is not just a simple error.	If samples are available with the product, you might try to reproduce the problem by using the sample data.
Check the installation directory structure and file permissions.	The installation location must contain the appropriate file structure and the file permissions. For example, if the product requires write access to log files, ensure that the directory has the correct permission.
Review relevant documentation, such as release notes, tech notes, and proven practices documentation.	Search the IBM knowledge bases to determine whether your problem is known, has a workaround, or if it is already resolved and documented.
Review recent changes in your computing environment.	Sometimes installing new software might cause compatibility issues.

If you still need to resolve problems, you must collect diagnostic data. This data is necessary for an IBM technical-support representative to effectively troubleshoot and assist you in resolving the problem. You can also collect diagnostic data and analyze it yourself.

Troubleshooting resources

Troubleshooting resources are sources of information that can help you resolve a problem that you have with a product. Many of the resource links provided can also be viewed in a short video demonstration.

To view the video version, search for "troubleshooting" through either Google search engine or YouTube video community.

Related concepts

QRadar log files

© Copyright IBM Corp. 2004, 2021

Use the IBM QRadar log files to help you troubleshoot problems.

Support Portal

The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services.

Use IBM Support Portal to access all the IBM support resources from one place. You can adjust the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos).

Find the IBM QRadar content that you need by selecting your products from the IBM Support Portal (http://www.ibm.com/support/entry/portal).

Related concepts

Service requests
Service requests are also known as Problem Management Records (PMRs). Several methods exist to submit diagnostic information to IBM Software Technical Support.

Fix Central
Fix Central provides fixes and updates for your system software, hardware, and operating system.

Knowledge bases
You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods

Service requests

Service requests are also known as Problem Management Records (PMRs). Several methods exist to submit diagnostic information to IBM Software Technical Support.

To open a service request, or to exchange information with technical support, view the IBM Software Support Exchanging information with Technical Support page (http://www.ibm.com/software/support/exchangeinfo.html). Service requests can also be submitted directly by using the Service requests (PMRs) tool (http://www.ibm.com/support/entry/portal/Open_service_request) or one of the other supported methods that are detailed on the exchanging information page.

Related concepts

Support Portal
The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services.

Fix Central
Fix Central provides fixes and updates for your system software, hardware, and operating system.

Knowledge bases
You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods

Fix Central

Fix Central provides fixes and updates for your system software, hardware, and operating system.

Use the pull-down menu to go to your product fixes on Fix Central (http://www.ibm.com/support/fixcentral). You might also want to view Getting started with Fix Central (http://www.ibm.com/systems/support/fixes/en/fixcentral/help/getstarted.html).

Related concepts

Support Portal
The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services.

Service requests

Service requests are also known as Problem Management Records (PMRs). Several methods exist to submit diagnostic information to IBM Software Technical Support.

Knowledge bases
You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods

Related information

Ordering PTFs Using IBM Fix Central Web Site

Knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods

Use the following knowledge bases to find useful information.

Tech notes and APARs

From the IBM Support Portal (http://www.ibm.com/support/entry/portal), you can search tech notes and APARs (problem reports).

IBM masthead search

Use the IBM masthead search by typing your search string into the **Search** field at the top of any ibm.com page.

External search engines

Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to include information that is outside the ibm.com® domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

Related concepts

Support Portal
The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services.

Service requests
Service requests are also known as Problem Management Records (PMRs). Several methods exist to submit diagnostic information to IBM Software Technical Support.

Fix Central
Fix Central provides fixes and updates for your system software, hardware, and operating system.

QRadar log files

Use the IBM QRadar log files to help you troubleshoot problems.

You can review the log files for the current session individually or you can collect them to review later.

Follow these steps to review the QRadar log files.

1. To help you troubleshoot errors or exceptions, review the following log files.
   - `/var/log/qradar.log`
   - `/var/log/qradar.error`
2. If you require more information, review the following log files:
   - /var/log/qradar-sql.log
   - /opt/tomcat6/logs/catalina.out

- /var/log/qflow.debug

3. Review all logs by selecting **Admin** > **System & License Mgmt** > **Actions** > **Collect Log Files**.

Related concepts

Troubleshooting resources

Troubleshooting resources are sources of information that can help you resolve a problem that you have with a product. Many of the resource links provided can also be viewed in a short video demonstration.

Common ports and servers used by QRadar

IBM QRadar requires that certain ports are ready to receive information from QRadar components and external infrastructure. To ensure that QRadar is using the most recent security information, it also requires access to public servers and RSS feeds.

Warning: If you change any common ports, your QRadar deployment might break.

SSH communication on port 22

All the ports that are used by the QRadar console to communicate with managed hosts can be tunneled, by encryption, through port 22 over SSH.

The console connects to the managed hosts by using an encrypted SSH session to communicate securely. These SSH sessions are initiated from the console to provide data to the managed host. For example, the QRadar Console can initiate multiple SSH sessions to the Event Processor appliances for secure communication. This communication can include tunneled ports over SSH, such as HTTPS data for port 443 and Ariel query data for port 32006. IBM QRadar QFlow Collector that use encryption can initiate SSH sessions to Flow Processor appliances that require data.

Open ports that are not required by QRadar

You might find additional open ports in the following situations:

- When you install QRadar on your own hardware, you may see open ports that are used by services, daemons, and programs included in Red Hat Enterprise Linux.
- When you mount or export a network file share, you might see dynamically assigned ports that are required for RPC services, such as `rpc.mountd` and `rpc.rquotad`.

QRadar port usage

Review the list of common ports that IBM QRadar services and components use to communicate across the network. You can use the port list to determine which ports must be open in your network. For example, you can determine which ports must be open for the QRadar Console to communicate with remote event processors.

Warning: If you change any common ports, your QRadar deployment might break.

WinCollect remote polling

WinCollect agents that remotely poll other Microsoft Windows operating systems might require additional port assignments.

For more information, see the IBM QRadar WinCollect *User Guide*.

QRadar listening ports

The following table shows the QRadar ports that are open in a `LISTEN` state. The `LISTEN` ports are valid only when iptables is enabled on your system. Unless otherwise noted, information about the assigned port number applies to all QRadar products.

Table 23. Listening ports that are used by QRadar services and components

Port	Description	Protocol	Direction	Requirement
22	SSH	TCP	Bidirectional from the QRadar Console to all other components.	Remote management access. Adding a remote system as a managed host. Log source protocols to retrieve files from external devices, for example the log file protocol. Users who use the command-line interface to communicate from desktops to the Console. High-availability (HA).
25	SMTP	TCP	From all managed hosts to the SMTP gateway.	Emails from QRadar to an SMTP gateway. Delivery of error and warning email messages to an administrative email contact.
111 and random generated port	Port mapper	TCP/UDP	Managed hosts (MH) that communicate with the QRadar Console. Users that connect to the QRadar Console.	Remote Procedure Calls (RPC) for required services, such as Network File System (NFS).
123	Network Time Protocol (NTP)	UDP	Outbound from the QRadar Console to the NTP Server Outbound from the MH to the QRadar Console	Time synchronization via Chrony between: • QRadar Console and NTP server • QRadar Managed Hosts and QRadar Console
135 and dynamically allocated ports above 1024 for RPC calls.	DCOM	TCP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. Bidirectional traffic between QRadar Console components or IBM QRadar event collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter. **Note:** DCOM typically allocates a random port range for communication. You can configure Microsoft Windows products to use a specific port. For more information, see your Microsoft Windows documentation.
137	Windows NetBIOS name service	UDP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.

Table 23. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
138	Windows NetBIOS datagram service	UDP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
139	Windows NetBIOS session service	TCP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
162	NetSNMP	UDP	QRadar managed hosts that connect to the QRadar Console. External log sources to QRadar Event Collectors.	UDP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources. The port is open only when the SNMP agent is enabled.
199	NetSNMP	TCP	QRadar managed hosts that connect to the QRadar Console. External log sources to QRadar Event Collectors.	TCP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources. The port is open only when the SNMP agent is enabled.
427	Service Location Protocol (SLP)	UDP/TCP		The Integrated Management Module uses the port to find services on a LAN.
443	Apache/HTTPS	TCP	Bidirectional traffic for secure communications from all products to the QRadar Console. Unidirectional traffic from the App Host to the QRadar Console.	Configuration downloads to managed hosts from the QRadar Console. QRadar managed hosts that connect to the QRadar Console. Users to have log in access to QRadar. QRadar Console that manage and provide configuration updates for WinCollect agents. Apps that require access to the QRadar API.

Table 23. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
445	Microsoft Directory Service	TCP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
514	Syslog	UDP/TCP	External network appliances that provide TCP syslog events use bidirectional traffic. External network appliances that provide UDP syslog events use uni-directional traffic. Internal syslog traffic from QRadar hosts to the QRadar Console.	External log sources to send event data to QRadar components. Syslog traffic includes WinCollect agents, event collectors, and Adaptive Log Exporter agents capable of sending either UDP or TCP events to QRadar.
762	Network File System (NFS) mount daemon (mountd)	TCP/UDP	Connections between the QRadar Console and NFS server.	The Network File System (NFS) mount daemon, which processes requests to mount a file system at a specified location.
1514	Syslog-ng	TCP/UDP	Connection between the local Event Collector component and local Event Processor component to the syslog-ng daemon for logging.	Internal logging port for syslog-ng.
2049	NFS	TCP	Connections between the QRadar Console and NFS server.	The Network File System (NFS) protocol to share files or data between components.
2055	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the IBM QRadar QFlow Collector.	NetFlow datagram from components, such as routers.
2376	Docker command port	TCP	Internal communications. This port is not available externally.	Used to manage QRadar application framework resources.
3389	Remote Desktop Protocol (RDP) and Ethernet over USB is enabled	TCP/UDP		If the Microsoft Windows operating system is configured to support RDP and Ethernet over USB, a user can initiate a session to the server over the management network. This means the default port for RDP, 3389 must be open.
3900	Integrated Management Module remote presence port	TCP/UDP		Use this port to interact with the QRadar console through the Integrated Management Module.

Table 23. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
4333	Redirect port	TCP		This port is assigned as a redirect port for Address Resolution Protocol (ARP) requests in QRadar offense resolution.
5000	Used to allow communication to the docker si-registry running on the Console. This allows all managed hosts to pull images from the Console that will be used to create local containers.	TCP	Unidirectional from the QRadar managed host to the QRadar Console. The port is only opened on the Console. Managed hosts must pull from the Console.	Required for apps running on an App Host.
5432	Postgres	TCP	Communication for the managed host that is used to access the local database instance.	Required for provisioning managed hosts from the **Admin** tab.
6514	Syslog	TCP	External network appliances that provide encrypted TCP syslog events use bidirectional traffic.	External log sources to send encrypted event data to QRadar components.
7676, 7677, and four randomly bound ports above 32000.	Messaging connections (IMQ)	TCP	Message queue communications between components on a managed host.	Message queue broker for communications between components on a managed host. **Note:** You must permit access to these ports from the QRadar console to unencrypted hosts. Ports 7676 and 7677 are static TCP ports, and four extra connections are created on random ports. For more information about finding randomly bound ports, see "Viewing IMQ port associations" on page 130.
5791, 7700, 7777, 7778, 7779, 7780, 7781, 7782, 7783, 7787, 7788, 7790, 7791, 7792, 7793, 7794, 7795, 7799, 8989, and 8990.	JMX server ports	TCP	Internal communications. These ports are not available externally.	JMX server (Java™ Management Beans) monitoring for all internal QRadar processes to expose supportability metrics. These ports are used by QRadar support.
7789	HA Distributed Replicated Block Device	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster.	Distributed Replicated Block Device is used to keep drives synchronized between the primary and secondary hosts in HA configurations.
7800	Apache Tomcat	TCP	From the Event Processor to the QRadar Console.	Real-time (streaming) for events.
7801	Apache Tomcat	TCP	From the Event Processor to the QRadar Console.	Real-time (streaming) for flows.
7803	Anomaly Detection Engine	TCP	From the Event Processor to the QRadar Console.	Anomaly detection engine port.
7804	QRM Arc builder	TCP	Internal control communications between QRadar processes and ARC builder.	This port is used for QRadar Risk Manager only. It is not available externally.

Table 23. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
7805	Syslog tunnel communication	TCP	Bidirectional between the QRadar Console and managed hosts	Used for encrypted communication between the console and managed hosts.
8000	Event Collection service (ECS)	TCP	From the Event Collector to the QRadar Console.	Listening port for specific Event Collection Service (ECS).
8001	SNMP daemon port	TCP	External SNMP systems that request SNMP trap information from the QRadar Console.	Listening port for external SNMP data requests.
8005	Apache Tomcat	TCP	Internal communications. Not available externally.	Open to control tomcat. This port is bound and only accepts connections from the local host.
8009	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat.	Tomcat connector, where the request is used and proxied for the web service.
8080	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat.	Tomcat connector, where the request is used and proxied for the web service.
8082	Secure tunnel for QRadar Risk Manager	TCP	Bidirectional traffic between the QRadar Console and QRadar Risk Manager	Required when encryption is used between QRadar Risk Manager and the QRadar Console.
8413	WinCollect agents	TCP	Bidirectional traffic between WinCollect agent and QRadar Console.	This traffic is generated by the WinCollect agent and communication is encrypted. It is required to provide configuration updates to the WinCollect agent and to use WinCollect in connected mode.
8844	Apache Tomcat	TCP	Unidirectional from the QRadar Console to the appliance that is running the QRadar Vulnerability Manager processor.	Used by Apache Tomcat to read information from the host that is running the QRadar Vulnerability Manager processor.
9000	Conman	TCP	Unidirectional from the QRadar Console to a QRadar App Host.	Used with an App Host. It allows the Console to deploy apps to an App Host and to manage those apps.
9090	XForce IP Reputation database and server	TCP	Internal communications. Not available externally.	Communications between QRadar processes and the XForce Reputation IP database.
9381	Certificate files download	TCP	Unidirectional from QRadar managed host or external network to QRadar Console	Downloading QRadar CA certificate and CRL files, which can be used to validate QRadar generated certificates.
9381	localca-server	TCP	Bidirectional between QRadar components.	Used to hold QRadar local root and intermediate certificates, as well as associated CRLs.
9393, 9394	vault-qrd	TCP	Internal communications. Not available externally.	Used to hold secrets and allow secure access to them to services.

Table 23. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
9913 plus one dynamically assigned port	Web application container	TCP	Bidirectional Java Remote Method Invocation (RMI) communication between Java Virtual Machines	When the web application is registered, one additional port is dynamically assigned.
9995	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the QRadar QFlow Collector.	NetFlow datagram from components, such as routers.
9999	IBM QRadar Vulnerability Manager processor	TCP	Unidirectional from the scanner to the appliance running the QRadar Vulnerability Manager processor	Used for QRadar Vulnerability Manager (QVM) command information. The QRadar Console connects to this port on the host that is running the QRadar Vulnerability Manager processor. This port is only used when QVM is enabled.
10000	QRadar web-based, system administration interface	TCP/UDP	User desktop systems to all QRadar hosts.	In QRadar V7.2.5 and earlier, this port is used for server changes, such as the hosts root password and firewall access. Port 10000 is disabled in V7.2.6.
10101, 10102	Heartbeat command	TCP	Bidirectional traffic between the primary and secondary HA nodes.	Required to ensure that the HA nodes are still active.
12500	Socat binary	TCP	Outbound from MH to the QRadar Console	Port used for tunneling chrony udp requests over tcp when QRadar Console or MH is encrypted
14433	traefik	TCP	Bidirectional between QRadar components.	Required for app services discovery.
15432				Required to be open for internal communication between QRM and QRadar.
15433	Postgres	TCP	Communication for the managed host that is used to access the local database instance.	Used for QRadar Vulnerability Manager (QVM) configuration and storage. This port is only used when QVM is enabled.
15434				Required to be open for internal communication between Forensics and QRadar.
20000-23000	SSH Tunnel	TCP	Bidirectional from the QRadar Console to all other encrypted managed hosts.	Local listening point for SSH tunnels used for Java Message Service (JMS) communication with encrypted managed hosts. Used to perform long-running asynchronous tasks, such as updating networking configuration via System and License Management.
23111	SOAP web server	TCP		SOAP web server port for the Event Collection Service (ECS).

Table 23. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
23333	Emulex Fibre Channel	TCP	User desktop systems that connect to QRadar appliances with a Fibre Channel card.	Emulex Fibre Channel HBAnywhere Remote Management service (elxmgmt).
26000	traefik	TCP	Bidirectional between QRadar components.	Used with an App Host that is encrypted. Required for app services discovery.
26001	Conman	TCP	Unidirectional from the QRadar Console to a QRadar App Host.	Used with an App Host that is encrypted. It allows the Console to deploy apps to an App Host and to manage those apps.
32000	Normalized flow forwarding	TCP	Bidirectional between QRadar components.	Normalized flow data that is communicated from an off-site source or between QRadar QFlow Collectors.
32004	Normalized event forwarding	TCP	Bidirectional between QRadar components.	Normalized event data that is communicated from an off-site source or between QRadar Event Collectors.
32005	Data flow	TCP	Bidirectional between QRadar components.	Data flow communication port between QRadar Event Collectors when on separate managed hosts.
32006	Ariel queries	TCP	Bidirectional between QRadar components.	Communication port between the Ariel proxy server and the Ariel query server.
32007	Offense data	TCP	Bidirectional between QRadar components.	Events and flows contributing to an offense or involved in global correlation.
32009	Identity data	TCP	Bidirectional between QRadar components.	Identity data that is communicated between the passive Vulnerability Information Service (VIS) and the Event Collection Service (ECS).
32010	Flow listening source port	TCP	Bidirectional between QRadar components.	Flow listening port to collect data from QRadar QFlow Collectors.
32011	Ariel listening port	TCP	Bidirectional between QRadar components.	Ariel listening port for database searches, progress information, and other associated commands.
32000-33999	Data flow (flows, events, flow context)	TCP	Bidirectional between QRadar components.	Data flows, such as events, flows, flow context, event search queries, and Docker proxy.

Table 23. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
40799	PCAP data	UDP	From Juniper Networks SRX Series appliances to QRadar.	Collecting incoming packet capture (PCAP) data from Juniper Networks SRX Series appliances. **Note:** The packet capture on your device can use a different port. For more information about configuring packet capture, see your Juniper Networks SRX Series appliance documentation.
ICMP	ICMP		Bidirectional traffic between the secondary host and primary host in an HA cluster.	Testing the network connection between the secondary host and primary host in an HA cluster by using Internet Control Message Protocol (ICMP).

Viewing IMQ port associations

Several ports that are used by IBM QRadar allocate extra random port numbers. For example, Message Queues (IMQ) open random ports for communication between components on a managed host. You can view the random port assignments for IMQ by using telnet to connect to the local host and doing a lookup on the port number.

Random port associations are not static port numbers. If a service is restarted, the ports that are generated for the service are reallocated and the service is provided with a new set of port numbers.

Procedure

1. Using SSH, log in to the QRadar Console as the root user.
2. To display a list of associated ports for the IMQ messaging connection, type the following command:

   `telnet localhost 7676`

   The results from the telnet command might look similar to this output:

```
[root@domain ~]# telnet localhost 7676
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
101 imqbroker 4.4 Update 1
portmapper tcp PORTMAPPER 7676
[imqvarhome=/opt/openmq/mq/var,imqhome=/opt/openmq/mq,sessionid=<session_id>]
cluster_discovery tcp CLUSTER_DISCOVERY 44913
jmxrmi rmi JMX 0 [url=service:jmx:rmi://domain.ibm.com/stub/<urlpath>]
admin tcp ADMIN 43691
jms tcp NORMAL 7677
cluster tcp CLUSTER 36615
```

   The telnet output shows 3 of the 4 random high-numbered TCP ports for IMQ. The fourth port, which is not shown, is a JMX Remote Method Invocation (RMI) port that is available over the JMX URL that is shown in the output.

   If the telnet connection is refused, it means that IMQ is not currently running. It is probable that the system is either starting up or shutting down, or that services were shut down manually.

Searching for ports in use by QRadar

Use the **netstat** command to determine which ports are in use on the IBM QRadar Console or managed host. Use the **netstat** command to view all listening and established ports on the system.

Procedure

1. Using SSH, log in to your QRadar Console, as the root user.
2. To display all active connections and the TCP and UDP ports on which the computer is listening, type the following command:

```
netstat -nap
```

3. To search for specific information from the netstat port list, type the following command:

```
netstat -nap | grep port
```

Examples:

- To display all ports that match 199, type the following command:

```
netstat -nap | grep 199
```

- To display information on all listening ports, type the following command:

```
netstat -nap | grep LISTEN
```

QRadar public servers

To provide you with the most current security information, IBM QRadar requires access to a number of public servers.

Public servers

Table 24. Public servers that QRadar must access. This table lists descriptions for the IP addresses or hostnames that QRadar accesses. https://www.ibm.com/support/pages/node/6244622

IP address or hostname	Description
194.153.113.31	IBM QRadar Vulnerability Manager DMZ scanner
194.153.113.32	QRadar Vulnerability Manager DMZ scanner
auto-update.qradar.ibmcloud.com/	QRadar auto-update servers. For more information about auto-update servers, see QRadar: Important auto update server changes for administrators (https://www.ibm.com/support/pages/node/6244622).
update.xforce-security.com	X-Force® Threat Feed update server
license.xforce-security.com	X-Force Threat Feed licensing server

Chapter 11. Receiving update notifications

Sign up to stay informed of critical QRadar software support updates.

Procedure

1. Go to Stay up to date - IBM Support (http://ibm.biz/MyNotification).
2. Click **Subscribe now!**.
3. Sign in with your IBMid.
4. Enter `QRadar` in the **Product lookup** field.
5. Click **Subscribe** to choose which product you want to receive notifications for.
6. Select the notifications that you want to receive.

© Copyright IBM Corp. 2004, 2021

Notices

This information was developed for products and services offered in the U.S.A.

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
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

© Copyright IBM Corp. 2004, 2021

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

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.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., 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 www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds 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.

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

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details/ the section entitled “Cookies, Web Beacons and Other Technologies”.

General Data Protection Regulation

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about the IBM GDPR readiness journey and our GDPR capabilities and Offerings here: https://ibm.com/gdpr