IBM Security Intelligence on Cloud

Getting Started Guide

IBM

Note

Before using this information and the product that it supports, read the information in "Notices" on page 11.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.

Contents

Introduction to IBM Security Intelligence on Cloud Onboarding

Use IBM® Security Intelligence on Cloud to monitor your network with IBM Security QRadar® in a subscription model.

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 Security QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc_cloud/c_hosted_inst.html).

For information about how to access more technical documentation in the QRadar products library, see Accessing IBM Security QRadar documentation (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 Security 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 Security QRadar.

Chapter 1. IBM Security Intelligence on Cloud overview

IBM Security Intelligence on Cloud allows you to enjoy the benefits and customer support of IBM Security QRadar, but in a hosted deployment. In an environment where security requirements are dynamic, IBM Security Intelligence on Cloud provides both the security monitoring that you need, and the flexibility to modify your monitoring as your requirements change. With IBM Security Intelligence on Cloud, you can use the capabilities of QRadar without investing in all of the required hardware and software of an on-premises QRadar deployment.

You connect to QRadar through a gateway appliance. Other than the gateway appliance, you do not need to install any extra hardware on your premises. Download and install the enabling software on your gateway appliance to collect events from all log sources that are supported on your premises or in the cloud. The enabling software forwards the collected events to the QRadar running in the IBM cloud, through a secure VPN tunnel, where the data is stored and managed. Log on to the QRadar console from a web browser to manage all your security and threat management tasks, just as you would with QRadar deployed on your premises.

The following image shows devices on your network sending information to the Gateway appliance on your premises. The Gateway appliance then communicates with an instance of QRadar running in the IBM cloud

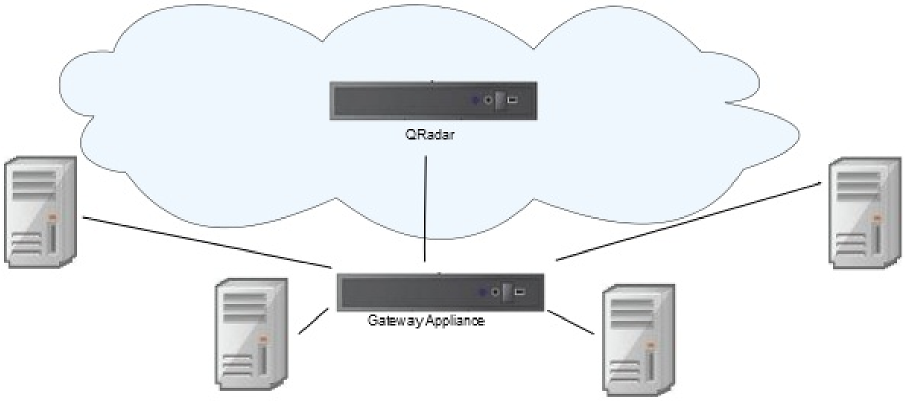

Figure 1. IBM Security Intelligence on Cloud deployment example

IBM Security Intelligence on Cloud has capabilities of IBM Security QRadar SIEM hosted in IBM SoftLayer. The base license includes 1000 events per second (EPS), and you can upgrade your license to 10, 000 EPS when you need to.

You can have a maximum of 6 IBM Security Intelligence on Cloud users. You can give any of these users the security administrator access.

The operational health and performance of the IBM cloud infrastructure is monitored 24 x 7 by the IBM service team. Your customer support is provided by the existing QRadar support team. IBM Security Intelligence on Cloud is always up-to-date with the latest QRadar features and software updates.

IBM Security Intelligence on Cloud provides both pricing and monitoring flexibility to meet your organization's changing needs.

Important: IBM Security Intelligence on Cloud does not support flow data.

Chapter 2. IBM Security Intelligence on Cloud onboarding

After you purchase IBM Security Intelligence on Cloud, IBM sends you the information required for you to use IBM Security Intelligence on Cloud.

IBM will send you an email after you have purchased IBM Security Intelligence on Cloud. This email contains a link to the Gateway Landing Page, which contains the following information:

- Your IBM Security Intelligence on Cloud token. You need a token for each Gateway appliance that you want to use to connect to IBM Security QRadar on the IBM cloud.
- A download link to the IBM Security QRadar ISO for your gateway appliance.
- A copy of Red Hat Enterprise Linux (RHEL) 6.7.
- The software installation activation key for each gateway appliance.
- The public Host Name of the console that you connect to through the gateway appliance.
- The required licenses for your 6 IBM Security Intelligence on Cloud users.

Gateway appliance prerequisites

You must meet the following prerequisites before you can use the IBM Security Intelligence on Cloud gateway appliance:

- You must have a static IP address to connect to IBM Security Intelligence on Cloud through your gateway appliance.
- You must have adequate bandwidth to send your security data to IBM Security Intelligence on Cloud.

  Example: On average, 10 MBps is required for 1000 events per second (EPS), 100 Mbps for 10,000 EPS.

  The above example is derived from using the following formula, and rounding up:

  EPS * (average event size+200) bytes * 8 = Mbps value.

  1000 * 1056 * 8 = 8.4 Mbps.
- Your gateway appliance must meet the recommended system requirements.

Gateway appliance system requirements

The gateway appliance that you install on your premises communicates with IBM Security Intelligence on Cloud must have the following specifications:

Table 1. Gateway system requirements for physical appliances

Specification	Required value
CPU	2.6 GHz, 6 Core, 15 MB Cache
RAM	16 GB, 4 x 4 GB 1600 MHz RDIMM

Table 1. Gateway system requirements for physical appliances (continued)

Specification	Required value
HDD	2 TB: 200 GB for software installation, and use the following formula to determine space for events: (Seconds in a day) x (Events per second rate) x (Average size of a log event x 1.5 QRadar normalized event overhead) **Example:** 86400 x 10,000 EPS x 600 bytes = 518400000000 bytes = 518.4 GB, + 200 GB for storage = 718.4 GB.

Table 2. Gateway system requirements for virtual appliances

Specification	Required value
CPU	4 cores for 1000 events per second (EPS) or less. 8 cores for 1000 -10,000 EPS.
RAM	16 GB, 4 x 4 GB 1600 MHz RDIMM
HDD	2 TB: 300 GB for software installation, and use the following formula to determine space for events: (Seconds in a day) x (Events per second rate) x (Average size of a log event x 1.5 QRadar normalized event overhead) **Example:** 86400 x 10,000 EPS x 600 bytes = 518400000000 bytes = 518.4 GB, + 200 GB for storage = 718.4 GB.

DSM certificates

Contact q1saas@us.ibm.com if you require certificates for any of the following DSMs, or adapters to import certain data into QRadar.

- Amazon
- Generic Firewall
- Generic Auth Server
- IBM Endpoint Manager
- IBM Fiberlink
- Juniper Steel-Belted Radius
- Juniper Binary
- Open LDAP
- PostFix
- Salesforce Security Monitoring
- Sourcefire eStreamer
- Verdasys

Chapter 3. Gateway software installation

You can install IBM Security QRadar SIEM on a virtual appliance or a physical appliance.

Restriction: Resizing logical volumes by using a logical volume manager (LVM) is not supported.

Creating your virtual machine

Create a virtual machine where you can install IBM Security QRadar if you do not want to install it on a physical appliance.

Before you begin

To install a virtual appliance, you must first use VMware vSphere Client 5.1 to create a virtual machine.

About this task

Build your virtual machine to match the recommended specifications for IBM Security Intelligence on Cloud. For more information, see Chapter 2, "IBM Security Intelligence on Cloud onboarding," on page 3.

Procedure

1. From the VMware vSphere Client, click **File** > **New** > **Virtual Machine**.
2. Use the following steps to guide you through the choices:
   a. In the **Configuration** pane of the Create New Virtual Machine window, select **Custom**.
   b. In the **Virtual Machine Version** pane, select **Virtual Machine Version: 7**.
   c. For the **Operating System (OS)**, select **Linux**, and select **Red Hat Enterprise Linux 6 (64-bit)**.
   d. On the **CPUs** page, configure the number of virtual processors that you want for the virtual machine:
      - For less than 1000 events per second (EPS), select 4 cores.
      - For 1000 EPS or more, select 8 cores.
   e. In the **Memory Size** field, type or select `16` or greater.
   f. Use the following table to configure you network connections.

Table 3. Descriptions for network configuration parameters

Parameter	Description
How many NICs do you want to connect	You must add at least one Network Interface Controller (NIC)
Adapter	`VMXNET3`

   g. In the **SCSI controller** pane, select **VMware Paravirtual**.
   h. In the **Disk** pane, select **Create a new virtual disk** and use the following table to configure the virtual disk parameters.

Table 4. Settings for the virtual disk size and provisioning policy parameters

Property	**Option**
Capacity	2 TB or higher
Disk Provisioning	Thin provision
Advanced options	Do not configure

3. On the **Ready to Complete** page, review the settings and click **Finish**.

Linux partition properties for your own gateway appliance

If you use your own gateway appliance, 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 recreate the partitioning on your Red Hat Enterprise Linux operating system.

Restriction: Resizing logical volumes by using a logical volume manager (LVM) is not supported.

Table 5. Partition guide for RHEL

Partition	**Description**	**Mount point**	**File system type**	**Size**	**Forced to be primary**	**SDA or SDB**
`/boot`	System boot files	`/boot`	EXT4	200 MB	Yes	SDA
`/`	Installation area for QRadar, the operating system, and associated files.	`/`	EXT4	20000 MB	No	SDA
`/store/tmp`	Storage area for QRadar temporary files	`/store/tmp`	EXT4	10000 MB	No	SDA
`/var/log`	Storage area for QRadar and system log files	`/var/log`	EXT4	10000 MB	No	SDA
		4094	swap			
`/store`	Storage area for QRadar data and configuration files	`/store`	XFS	The remaining space from the 2 TB allocation.	No	SDA If 2 disks, SDB

Installing RHEL on your own appliance

You can install the Red Hat Enterprise Linux operating system on your own appliance for use with IBM Security QRadar.

Procedure

1. Create a bootable Red Hat Enterprise Linux image using one of the following portable storage devices:
   - Digital Versatile Disk (DVD)
   - Bootable USB flash drive
2. Insert the portable storage device into your appliance and restart your appliance.
3. From the Boot menu, select one of the following options:

- Select the USB or DVD drive as the boot option.
- To install on a system that supports Extensible Firmware Interface (EFI), you must start the system in legacy mode.

4. Follow the instructions in the installation wizard to complete the installation:
   a. Select the **Basic Storage Devices** option.
   b. When you configure the host name, the **Hostname** property can include letters, numbers, and hyphens.
   c. When you configure the network, in the Network Connections window, select **System eth0** and then click **Edit** and select **Connect automatically**.
   d. On the **IPv4 Settings** tab, from the **Method** list, select **Manual**, and enter your IP address, net mask and gateway address.
   e. In the **DNS servers** field, type a comma-separated list.
   f. Select **Create Custom Layout** option.
   g. Configure EXT4 for the file system type for the /, /boot, /store/tmp, and /var/log partitions.
   h. Create the swap partition with a file system type of swap.
   i. Assign all remaining space to the /store partition, and select xfs as the file type.
   j. Select **Basic Server**, and make any customizations required by your deployment.
5. When the installation is complete, click **Reboot**.

What to do next

After installation, ensure that the system has network connectivity by logging into it, using SSH, from another system, and sending a ping from another system.

Installing QRadar software on a gateway appliance

Install the IBM Security QRadar software on a physical appliance, or on the virtual machine. You connect to IBM Security Intelligence on Cloud through a gateway appliance.

Before you begin

Ensure that you have the following information:

- The activation key for your gateway appliance
- The token for IBM Security Intelligence on Cloud
- The full host name of the console that you connect to through your gateway appliance.

Procedure

1. Use SSH to log in to your virtual or physical machine as the root user.
2. Create the directories for the QRadar and Red Hat Enterprise Linux ISO images on your virtual machine by using the following commands:

```
mkdir /media/cdrom

mkdir /media/redhat

mkdir /store/iso
```

3. Copy the QRadar and Red Hat Enterprise Linux version 6.7 ISOs to the /store/iso directory on the system.

4. Mount the ISOs with the following commands:

   ```
   mount -o loop <path to the QRadar ISO> /media/cdrom
   mount -o loop <path to the redhat ISO> /media/redhat
   ```

5. Start the installation by using the following command:

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

6. Accept the End User License Agreement (EULA) that is displayed.

   Tip: Press the Space bar key to advance through the document.

7. Enter the Activation Key when prompted.
8. Follow the instructions in the Installation Wizard.
9. In the Gateway Setup window of the installation wizard, select **yes Configure the connection now** and click **Yes**.
10. In the Deployment Configuration window, Enter the domain name for the console, and the token for IBM Security Intelligence on Cloud. Click **Next**.
11. In the Internet Access window, select how the gateway connects to the Internet: **direct** or **proxy**, and click **Next**.
12. If you selected **proxy** on the Internet Access window, enter the **HTTP IP address** and **HTTP proxy port**
13. Follow the instructions in the installation wizard to complete the installation.

    After you configure the installation parameters, a series of installation messages are displayed, including configuration download messages, "waiting for do deploy to complete" messages, and reboot messages. The installation process can take several minutes.

Chapter 4. End your IBM Security Intelligence on Cloud subscription

If you decide to stop using IBM Security Intelligence on Cloud, you must retrieve your data.

If you decide to stop using IBM Security Intelligence on Cloud, email q1saas@us.ibm.com with information about when you want your service to stop.

IBM will send you an email that contains the tokens that are required to stop your service, and instructions about how to retrieve your data. After you apply these tokens, you can no longer send events to IBM Security QRadar, and you have 30 days to retrieve any data that you want to keep.

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

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 states 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply 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 Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All 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 the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

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.

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

Privacy policy considerations

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” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Index