IBM Security QRadar
Version 7.2.0

Installing QRadar with a Bootable USB Flash-drive Technical Note

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page 13.

CONTENTS

1 OVERVIEW

This technical note provides information on how to create a USB flash-drive capable of completing a new installation of any QRadar product software.

Note: This document only applies to full installations; it does not apply to upgrades or patches. Information for patches is available in the release note documentation for your product.

Supported versions

The USB create key script is intended for creating QRadar 7.2 bootable USB flash-drives to install or reinstall QRadar 7.2 appliances.

You can use the following appliances or operating systems to create a bootable USB flash-drive:

- A QRadar 7.2 appliance
- A Linux system installed with RedHat 6.3
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 2008
- Microsoft Windows 2008R2

Installation overview

This overview provides a generic procedure for creating and installing IBM Security QRadar from a bootable USB flash drive.

Note: For the full installation steps, you must refer to the installation guide or release notes for your specific QRadar product.

1. Create your bootable USB flash-drive.
2. Install the software for your QRadar product.

   For the installation procedure, see the installation guide for your QRadar product.
3. Install any patches or maintenance releases.

   For the installation procedure on patches or maintenance releases, see the release note documentation for your product.

2 CREATE A BOOTABLE USB FLASH-DRIVE WITH A QRADAR APPLIANCE

You can use a QRadar 7.2 appliance to create a bootable USB flash-drive that is capable of installing QRadar software.

Before you begin

Before you can create a bootable USB flash-drive from a QRadar appliance, you must have access to the following:

- A 2 GB (or larger) USB flash-drive
- A QRadar 7.2 ISO image file
- A physical QRadar 7.2 appliance

CAUTION: *When you create a bootable USB flash-drive, the contents of the USB flash-drive are deleted.*

Creating a bootable USB flash-drive from a QRadar appliance

You can use another QRadar 7.2 appliances from your deployment to create a bootable USB flash-drive.

If you need to re-install QRadar software and your appliance does not have Internet connectivity, you can download and copy the QRadar ISO to a desktop computer or another QRadar appliance with Internet access. You can then copy the ISO file to a QRadar system in your deployment.

Procedure

To create a bootable USB flash-drive:

Step 1 Download the QRadar ISO file:

a Access the IBM support website (*http://www.ibm.com/support*).

b Locate the IBM Security QRadar 7.2 ISO file on the IBM support website.

c Copy the ISO image to a directory on your QRadar system.

For example, /tmp.

Step 2 Using SSH, log in to your QRadar system as the root user.

Username: **`root`**

Password: **`<password>`**

Step 3 Insert your USB flash-drive in the front USB port on your system.

Depending on your system, it might take up to 30 seconds to recognize a USB flash-drive.

Step 4 Type the following command to mount the ISO image:

```
mount -o loop /tmp/<name of the iso image>.iso /media/cdrom
```

Step 5 Type the following command to copy the USB creation script from the mounted ISO to the /tmp directory:

```
cp /media/cdrom/post/create-usb-key.py /tmp/
```

Step 6 Type the following command to start the USB creation script:

```
/tmp/create-usb-key.py
```

Step 7 Press Enter.

Step 8 Press **1** and type the path to the ISO file.

For example,

```
/tmp/<name of the iso image>.iso
```

Step 9 Press **2** and select the drive containing your USB flash-drive.

Step 10 Press **3** to create your USB key.

The process of writing the ISO image to your USB flash-drive takes several minutes to complete. When the ISO is loaded onto the USB flash-drive, a confirmation message is displayed.

Step 11 Press **q** to quit the USB key script.

Step 12 Remove the USB flash-drive from your QRadar system.

The USB stick is configured to install QRadar software.

What to do next

- If your connection to the appliance is a serial connection, see **Configuring a USB flash-drive for serial-only appliances**.
- If your connection to the appliance is keyboard and mouse (VGA), see **Installing QRadar with a USB flash-drive**.

3 CREATE A BOOTABLE USB FLASH-DRIVE WITH MICROSOFT WINDOWS

You can use a desktop or laptop system with Microsoft Windows™ to create a bootable USB flash-drive that is capable of installing or reinstalling QRadar products.

Before you begin

Before you can create a bootable USB flash-drive with Microsoft Windows™, you must have access to the following:

- A 2 GB (or larger) USB flash-drive
- A QRadar 7.2 RedHat 64-bit ISO image file
- The Create USB Install Key (CUIK) software
- A desktop or latpop system with one the following operating systems:
  - Windows 7
  - Windows Vista
  - Windows 2008
  - Windows 2008R2
- PeaZip Portable 4.8.1
- Syslinux 4.06

CAUTION: *When you create a bootable USB flash-drive, the contents of the USB flash-drive are deleted.*

Creating a bootable USB flash-drive in Windows

The Create-USB-Install-Key (CUIK) tool is a guided command-line tool for Microsoft Windows that allows you to create a bootable USB flash-drive of QRadar software.

Procedure

Step 1 Download the QRadar ISO file:

a Access the IBM support website (*http://www.ibm.com/support*).

b Locate the IBM Security QRadar 7.2 ISO file on the IBM support website.

c Save the ISO file to your Windows system.

Step 2 Download the Create-USB-Install-Key (CUIK) tool from the IBM support website.

`cuik.<version>.zip`

Step 3 Extract the Create-USB-Install-Key (CUIK) tool to a directory.

For example, C:\cuik

Step 4 From the Internet, download the following required files to the CUIK/deps folder:

- PeaZip Portable 4.8.1

  For example, c:\cuik\deps\peazip_portable-4.8.1.WINDOWS.zip

- Syslinux 4.06

  For example, c:\cuik\deps\syslinux-4.06.zip

You are not required to extract the zip files. The files only need to be available in the cuik/deps directory.

Step 5 Insert a blank USB flash-drive into the USB port on your computer.

Step 6 Verify that the USB flash-drive is be listed by drive letter and accessible in Windows.

Step 7 Right-click cuik.exe and select **Run as administrator**.

Step 8 Press Enter to continue.

Step 9 Press **1** to select your QRadar ISO file.

Step 10 Select your ISO image and click **Open**.

Step 11 Press **2** to select your USB drive letter.

Step 12 Select the number that corresponds to your USB flash-drive letter.

Step 13 Press **3** to create your USB flash-drive.

Step 14 Press Enter to confirm you are aware that the contents of the USB flash-drive are deleted.

Step 15 Type **create** to create a bootable USB flash-drive from the ISO image.

This process takes several minutes to complete and the software tool informs you if the process was successful.

Step 16 Press Enter, then type **q** to exit the Create-USB-Install-Key tool.

Step 17 Safely eject the USB flash-drive from the your desktop system.

The USB stick is configured to install QRadar software.

What to do next

- If your connection to the appliance is a serial connection, see **Configuring a USB flash-drive for serial-only appliances**.
- If your connection to the appliance is keyboard and mouse (VGA), see **Installing QRadar with a USB flash-drive**.

4 CREATE A BOOTABLE USB FLASH-DRIVE WITH REDHAT LINUX

You can use a Linux desktop or laptop system with RedHat 6.3 to create a bootable USB flash-drive that is capable of installing QRadar software.

Before you begin

Before you can create a bootable USB flash-drive for QRadar with Linux system, you must have access to the following items:

- 2 GB (or larger) USB flash-drive
- A QRadar 7.2 ISO image file
- A Linux system that is installed with the following software:
  - RedHat 6.3
  - Python 6.2 or above

CAUTION: *When you create a bootable USB flash-drive, the contents of the USB flash-drive are deleted.*

Creating a bootable USB flash-drive from a RedHat Linux system

You can use a Linux RedHat 6.3 system to create a bootable USB flash-drive for QRadar 7.2.

Procedure

Step 1 Download the QRadar ISO file:

a Access the IBM support website (*http://www.ibm.com/support*).

b Locate the IBM Security QRadar 7.2 ISO file on the IBM support website.

c Copy the ISO image to a directory on your QRadar system.

For example, /tmp.

Step 2 Log in to your Linux-based system as the root user.

Username: **`root`**

Password: **`<password>`**

Step 3 Update your Linux-based system to include the following packages:

- syslinux
- mtools
- dosfstools
- parted

For information on the specific package manager for your Linux system, see your vendor documentation.

Step 4 Insert your USB flash-drive into the USB port on your system.

Depending on your system, it might take up to 30 seconds to recognize a USB flash-drive.

Step 5 Type the following command to mount the ISO image:

```
mount -o loop /tmp/<name of the iso image>.iso /media/cdrom
```

Step 6 Type the following command to copy the create usb key script from the mounted ISO to the /tmp directory of your Linux system:

```
cp /media/cdrom/post/create-usb-key.py /tmp/
```

Step 7 Type the following command to start the USB creation script:

```
/tmp/create-usb-key.py
```

Step 8 Press Enter.

Step 9 Press **1** and type the path to the ISO file.

For example,

```
/tmp/Rhe664QRadar7_1_0_<build>.iso
```

Step 10 Press **2** and select the drive containing your USB flash-drive.

Step 11 Press **3** to create your USB key.

The process of writing the ISO image to your USB flash-drive takes several minutes to complete. When the ISO is loaded onto the USB flash-drive, a confirmation message is displayed.

Step 12 Press **q** to quit the USB key script.

Step 13 Remove the USB flash-drive from your QRadar system.

The USB stick is configured to install QRadar software.

What to do next

- If your connection to the appliance is a serial connection, see **Configuring a USB flash-drive for serial-only appliances**.
- If your connection to the appliance is keyboard and mouse (VGA), see **Installing QRadar with a USB flash-drive**.

5 QRadar Software Installation

Installation procedures vary depending the product you are attempting to install. For the full installation procedure, you must read the installation guide written for your QRadar product.

Configuring a USB flash-drive for serial-only appliances

Bootable USB flash-drives created to install QRadar software on appliances that use a serial connection must complete an additional configuration procedure before you being your installation.

If you have a keyboard and mouse connected (VGA) to your appliance, then this procedure is optional.

Procedure

Step 1 Insert the bootable USB flash-drive into the USB port of your appliance.

Step 2 On your USB flash-drive, locate the syslinux.cfg file.

Step 3 Edit the syslinux configuration file to change the default installation from **default linux** to **default serial**.

Step 4 Save the changes to the syslinux configuration file.

You are now ready to install your software.

What to do next

Installing QRadar with a USB flash-drive

Installing QRadar with a USB flash-drive

This installation procedure provides a generic outline for installing IBM Security QRadar from a bootable USB flash drive.

Procedure

Step 1 Install all necessary hardware.

Step 2 Choose one of the following options:

- Connect a laptop to the serial port on the rear of the appliance.
- Connect a keyboard and monitor to their respective ports.

Step 3 Insert the bootable USB flash-drive into the USB port of your appliance.

Step 4 Restart the appliance.

Most appliances are capable of booting from USB by default. If you are installing QRadar software on your own hardware, you may be required to set the device boot order to prioritize USB.

After the appliance boots, the USB flash-drive prepares the appliance for installation. This process can take up to an hour to complete.

Step 5 When the RedHat Enterprise Linux menu is displayed, select one of the following options:

- If you connected a keyboard and monitor, select **Install or upgrade using VGA console**.
- If you connected a laptop with a serial connection, select **Install or upgrade using Serial console**.

Step 6 Type **SETUP** to begin the installation.

Step 7 When the login prompt is displayed, log in to the system as the root user.

Username: **root**

The username is case sensitive.

Step 8 Press Enter.

Step 9 Follow the prompts to install QRadar.

The complete installation process is documented in the installation guide for your QRadar product.

A NOTICES AND TRADEMARKS

What's in this appendix:

This section describes some important notices, trademarks, and compliance information.

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 *http://www.ibm.com/legal/copytrade.shtml*.

The following terms are trademarks or registered trademarks of other companies:

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

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

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