IBM Security QRadar Network Anomaly Detection
Version 7.1.0 (MR2)

Upgrade Guide

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page 15.

CONTENTS

ABOUT THIS GUIDE

This guide provides information on how to upgrade your IBM Security QRadar Network Anomaly Detection systems to QRadar Network Anomaly Detection 7.1.0 (MR2).

Intended audience

The *IBM Security QRadar Network Anomaly Detection Upgrade Guide* is intended for system administrators responsible for upgrading QRadar Network Anomaly Detection systems.

Documentation conventions

The following conventions are used throughout this guide:

Note: Indicates that the information provided is supplemental to the associated feature or instruction.

CAUTION: *Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.*

WARNING: *Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.*

Technical documentation

For information on how to access more technical documentation, technical notes, and release notes, see the ***Accessing IBM Security QRadar Network Anomaly Detection Documentation Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)

Contacting customer support

For information on contacting customer support, see the ***Support and Download Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

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 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.

1 PREPARING FOR YOUR UPGRADE

Before you upgrade, we recommend that you review the information in this section and pretest your system. Preparing for your upgrade should prevent issues from occurring during the upgrade.

Upgrade considerations

Read these upgrade considerations and prepare for your upgrade to ensure that your upgrade succeeds.

QRadar Network Anomaly Detection software version requirements

To upgrade to QRadar Network Anomaly Detection 7.1.0 (MR2), ensure the following requirements are met:

- You must be using at least QRadar Network Anomaly Detection 7.0 MR5. If you are not using at least QRadar Network Anomaly Detection 7.0 MR5, download and install QRadar Network Anomaly Detection 7.0 MR5 or higher from the Qmmunity website or *http://www.ibm.com/support*. In the QRadar Network Anomaly Detection user interface, click **Help > About** to view your QRadar Network Anomaly Detection version information.
- We require that you upgrade all of the systems in your deployment to QRadar Network Anomaly Detection 7.1.0 (MR2).

Memory and disk space requirements

Before you upgrade, you must verify your deployment meets the following requirements:

- Your appliance must have a minimum of 8 GB of memory.
- If you plan to enable payload indexing, we strongly recommend that your system include a minimum of 24 GB of memory.
- The QRadar Network Anomaly Detection 7.1.0 (MR2) upgrade requires the following minimum free disk space:

Table 1-1 Free space requirements

Partition	Free space requirement
/	3 GB
/store	4 GB
/var/log	500 MB
/store/tmp	800 MB

Additional software requirements

Before you install QRadar Network Anomaly Detection, make sure you have the following applications installed on any desktop system that you use to access the QRadar Network Anomaly Detection user interface:

- Java™ Runtime Environment (JRE)
- Adobe Flash 10.x

You can download Java 1.6.0_u24 at the following website: *http://java.com/*. Make sure that you install JRE on your desktop system, not on the QRadar Network Anomaly Detection system.

Upgrade priority order in distributed deployment

You must complete the upgrade process on your QRadar Network Anomaly Detection Console first and you must be able to access the QRadar Network Anomaly Detection user interface on your desktop system before upgrading your secondary Console and other systems in your deployment.

Pretesting your system

Before you upgrade to QRadar Network Anomaly Detection 7.1.0 (MR2), perform a pretest on all the systems in your deployment to ensure that your deployment meets the requirements for the upgrade. We recommend that you schedule the pretest during non-peak hours.

Before you begin

Ensure that there are no CDs in the disk drive before you pretest your system.

About this task

The output of the pretest determines if your system meets the upgrade system requirements, such as:

- Memory requirements
- Partitioning
- Supported and required RPMs
- Log source limits
- Licensing
- Out of memory notifications
- Disk sentry notifications
- Invalid passwords
- Failed logins
- PostgreSQL issues
- Table constraint/key issues

When pretesting your system, you are prompted to run PRETESTDOWN scripts after the initial PRETEST is complete. The PRETESTDOWN scripts require all

services to be stopped to test the integrity of the database, resulting in a data outage.

Procedure

Step 1 Using SSH, log in to QRadar Network Anomaly Detection as the root user.

Username: **root**

Password: **<password>**

Step 2 Choose one of the following:

- If you are upgrading a Console, go to **Step 3**.
- If you are upgrading a managed host, go to **Step 4**.

Step 3 Download and mount the QRadar Network Anomaly Detection 7.1.0 (MR2) software:

a Create the /store/iso folder by typing the following command:

```
mkdir /store/iso
```

b Access the QRadar Network Anomaly Detection 7.1.0 (MR2) download on one of the following locations:

- ***https://qmmunity.q1labs.com/products/***
- ***http://www.ibm.com/support***

c Copy the file to the /store/iso folder on your system.

d Mount the ISO by typing the following command:

```
mount –o loop /store/iso/<ISO file name> /media/cdrom
```

Go to **Step 5**.

Step 4 Copy the QRadar Network Anomaly Detection 7.1.0 (MR2) ISO from the Console and mount the ISO:

a Create the /store/iso folder by typing the following:

```
mkdir /store/iso
```

b Using SSH, log in to your Console as the root user:

Username: **root**

Password: **<password>**

c Copy the QRadar Network Anomaly Detection 7.1.0 (MR2) ISO to the /store/iso folder on your system:

```
scp <ISO file name> <ip_address>:/store/iso
```

Where **<ip_address>** is the IP address of the managed host.

d Using SSH, log in to your managed host as the root user:

Username: **root**

Password: **<password>**

e Mount the QRadar Network Anomaly Detection 7.1.0 (MR2) ISO by typing the following command:

```
mount -o loop /store/iso/<ISO file name> /media/cdrom
```

Go to **Step 5**.

Step 5 Perform the pretest by typing the following:

```
/media/cdrom/setup -t
```

Step 6 Type **Y** to continue the pretest.

Step 7 Type **Y** to run the PRETESTDOWN scripts.

Result

Third-party RPMs are not supported on QRadar Network Anomaly Detection systems. If the pretest discovers unsupported RPMs, you must remove the unsupported RPMs before upgrading your system. If the pretest discovers that required RPMs have been removed, you must re-install the required RPMs before continuing with your upgrade.

If the pretest indicates a problem, contact Customer Support.

2 UPGRADING QRADAR NETWORK ANOMALY DETECTION

Use these procedures to upgrade your QRadar Network Anomaly Detection appliances and QRadar Network Anomaly Detection software running on your own appliances.

Upgrading QRadar Network Anomaly Detection appliances

Use this procedure to upgrade your QRadar Network Anomaly Detection appliances.

Before you begin

Before you begin, you recommend that take the following precautions:

- Backup your data before you begin any software upgrade. For more information on backup and recovery, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.
- Close all open QRadar Network Anomaly Detection sessions to avoid access errors in your log file.
- Move any unsupported data from the root directory. During the upgrade, the following items are removed from the system:
  - Non-QRadar Network Anomaly Detection user accounts
  - Data associated with non-QRadar Network Anomaly Detection user accounts
  - Non-QRadar Network Anomaly Detection data stored in the root directory

About this task

When you upgrade your QRadar Network Anomaly Detection appliance to QRadar Network Anomaly Detection 7.1.0 (MR2), the CentOS operating system is replaced by Red Hat Enterprise Linux. The upgrade procedure may take an extended period of time to complete. You must not cancel or turn off the appliance when an upgrade is in progress.

If your deployment includes offboard storage solutions, you must remount your external storage solutions when prompted during the upgrade to QRadar Network Anomaly Detection 7.1.0 (MR2). For more information on configuring off-board storage, see the *Configuring Offboard Storage Guide*.

If your system has multiple volumes and a DRAC card, the following message is displayed during the upgrade, indicating that the upgrade process might cancel due to an unsupported configuration: `ERROR: Upgrade on systems without sda drive not supported` or `ERROR: Upgrade on PowerEdge 2950 only supported on single RAID 10 logical disk`. If this error is displayed, contact Customer Support.

The upgrade script runs a pretest to ensure your configuration meets the requirements for upgrading to QRadar Network Anomaly Detection 7.1.0 (MR2). If the pretest encounters issues, information messages are displayed that may require your input. Answer any prompts that are displayed to continue the pretest.

When the pretest is complete, the following message is displayed:

```
The upgrade process has four phases:
   1. Pretest checks (Completed)
   2. Upgrade data and configuration settings (Next)
   3. Install Red Hat Enterprise Linux 6
   4. Install new software version with upgraded data
Would you like to automatically restart your system at the end
of the phase 2? (Y/N)
```

If you type **N** to indicate that you do not want to automatically restart your system at the end of phase 2, you are required to manually restart your system when the upgrade prompts you.

Depending on your system, phase 2 can take several minutes to complete. The upgrade might prompt you to delete patch files that are no longer required by the system to save storage space. When the phase 2 upgrade is complete, your system is automatically restarted.

Procedure

Step 1 Using SSH, log in to QRadar Network Anomaly Detection as the root user.

Username: **root**

Password: **<password>**

Step 2 Choose one of the following:

- If you pretested your system as recommended, the ISO is already downloaded and mounted. Go to **Step 5**.
- If you are upgrading a Console, go to **Step 3**.
- If you are upgrading a managed host, go to **Step 4**.

Step 3 Download and mount the QRadar Network Anomaly Detection 7.1.0 (MR2) installer (ISO) file:

a Create the /store/iso folder by typing the following:

```
mkdir /store/iso
```

b Obtain the QRadar Network Anomaly Detection 7.1.0 (MR2) ISO file:

- Using your web browser, download the ISO from one of the following websites:

  https://qmmunity.q1labs.com/products/

  http://www.ibm.com/support

- Copy the ISO to the /store/iso folder on your system.

c Mount the ISO by typing the following command:

```
mount -o loop /store/iso/<ISO file name> /media/cdrom
```

Go to **Step 5**.

Step 4 Copy the ISO from the Console and mount the ISO:

a Create the /store/iso folder by typing the following:

```
mkdir /store/iso
```

b Using SSH, log in to your Console as the root user:

Username: **root**

Password: **<password>**

c Copy the ISO to the /store/iso folder on your system:

```
scp <ISO file name> <ip_address>:/store/iso
```

Where **<ip_address>** is the IP address of the managed host.

d Using SSH, log in to your managed host as the root user:

Username: **root**

Password: **<password>**

e Mount the ISO by typing the following command:

```
mount -o loop /store/iso/<ISO file name> /media/cdrom
```

Go to **Step 5**.

Step 5 Type the following setup command:

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

Step 6 Read the information in the End User License Agreement (EULA) window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

Step 7 At the prompt that asks for confirmation to pretest your system, type **Y** to continue.

Step 8 At the prompt that asks for confirmation to restart your system, type **Y** to continue the upgrade.

Step 9 Using SSH, log in to QRadar Network Anomaly Detection as the root user.

Username: **root**

Password: **<password>**

Result

Your upgrade is complete when the upgrade confirmation message is displayed.

What to do next

Verify that your DSMs, scanners, protocols and Juniper NSM plug-in RPM versions are current. You may be required to re-install RPMs.

Clearing the Cache

If you have trouble accessing the QRadar Network Anomaly Detection user interface after you upgrade to QRadar Network Anomaly Detection 7.1.0 (MR2), we recommend that you clear your Java™ cache.

Before you begin

Before you clear the cache, ensure you have only one instance of your browser open. If you have multiple versions of your browser open, the cache fails to clear.

The Java™ Runtime Environment must be installed on the desktop system you use to view QRadar Network Anomaly Detection. You can download Java version 1.6.0_u24 at the following website: http://java.com/.

About this task

If you are using Microsoft® Windows 7 as your operating system, the **Java** icon is typically located under the **Programs** pane, depending on how your Control Panel is configured to display features.

If you are using the Mozilla Firefox web browser, you must clear the cache in the Microsoft Internet Explorer and Mozilla Firefox web browsers.

Procedure

Step 1 Clear your Java cache:

a On your desktop, select **Start > Control Panel**.

The Control Panel is displayed.

b Double-click the **Java** icon.

The Java Control Panel is displayed.

c In the **Temporary Internet Files** pane, click **View**.

d On the Java Cache Viewer window, select all QRadar Network Anomaly Detection Deployment Editor entries.

e Click the **Delete** icon.

f Click **Close**.

g Click **OK**.

Step 2 Open your web browser.

Step 3 Clear the cache of your web browser. Choose one of the following options:

- If you are using the Microsoft Internet Explorer 7.0 or 8.0 web browser, select **Tools > Delete Browsing History**.

- If you are using the Microsoft Internet Explorer 9.0 web browser, click the gear icon in the right corner of the browser window, select **Internet Options > General**, and then click **Delete** in the **Browsing History** pane.
- If you are using the Mozilla Firefox 3.6.x web browser and above, select **Tools > Clear Recent History > Clear Now**.

Step 4 Log in to QRadar Network Anomaly Detection:

`https://<IP Address>`

Where **`<IP Address>`** is the IP address of the QRadar Network Anomaly Detection system. The default values are:

Username: **admin**

Password: **<password>**

Where **`<password>`** is the password assigned to QRadar Network Anomaly Detection during the installation process.

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.

INDEX