IBM QRadar
7.5.0

Upgrade Guide

Note

Before you use this information and the product that it supports, read the information in “Notices” on page 7.

Contents

Introduction to upgrading QRadar software v

Chapter 1. Preparation checklist for QRadar upgrades 1

Chapter 2. Upgrading QRadar SIEM 3

Migrating event collectors from GlusterFS to Distributed Replicated Block Device 4

Notices 7

Trademarks 8

Terms and conditions for product documentation 8

IBM Online Privacy Statement 9

General Data Protection Regulation 9

Introduction to upgrading QRadar software

Information about upgrading IBM® QRadar® applies to IBM QRadar SIEM and IBM QRadar Log Manager products.

Intended audience

System administrators who are responsible for upgrading IBM QRadar systems must be familiar with network security concepts and device configurations.

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.

Chapter 1. Preparation checklist for QRadar upgrades

To successfully upgrade an IBM QRadar system, verify your upgrade path, especially when you upgrade from older versions that require intermediate steps. You must also review the software, hardware, and high availability (HA) requirements.

ISO files are used for major operating system version upgrades and SFS files are used for any upgrades that do not include a major operating system version upgrade.

Important: You cannot upgrade directly from 7.3.2 to 7.5 Update Package 2. First upgrade from 7.3.2 to 7.5 Update Package 1 before upgrading to a later release.

Use the following checklist to make sure that you are prepared for an upgrade.

__ • Review the QRadar Release Notes® (https://www.ibm.com/docs/en/qsip/7.4?topic=overview-release-notes).

__ • Run a health check and fix any failures. See "Running health checks" in the *Troubleshooting Guide*.

__ • Notify users of scheduled maintenance.

__ • Verify that running scans and reports are complete.

__ • Request that users close all QRadar sessions and **screen** sessions.

__ • When upgrading to QRadar 7.4.2 or later, ensure that all event collectors are migrated from GlusterFS to Distributed Replicated Block Device. For more information, see “Migrating event collectors from GlusterFS to Distributed Replicated Block Device” on page 4.

__ • Review the release notes for the version you are upgrading to and download the SFS file. To access the release notes and SFS file download link, go to QRadar Software 101 (https://ibm.biz/qradarsoftware).

__ • Verify the checksum of the SFS file. For information about verifying the checksum of the SFS file, see Using a Windows Host for Checksum verification of the build (https://www.ibm.com/support/pages/radar-error-installing-radar-when-using-iso).

__ • Get a CSV file that contains a list of IP addresses for each appliance in your deployment if you don't already have this information, by typing the following command:

```
/opt/qradar/support/deployment_info.sh
```

__ • Unmount all external storage which is not /store/ariel or /store.

__ • Back up all third-party data, such as:

- scripts
- personal utilities
- important files or exports
- JAR files or interim fixes that were provided by QRadar support
- static route files for network interfaces

__ • If you have HA appliances in your deployment, verify that your primary appliances are in the Active state, and your secondary appliances are in the Standby state.

__ • Ensure that you have direct access to the command line on all appliances. If you are using IMM, iDRAC, Raritan, KVM, or other technology for command line access, ensure that they are configured and functional.

__ • Verify that the firmware is the latest version for your appliances. For more information about updating firmware, see Firmware update for QRadar (http://www.ibm.com/support/docview.wss?uid=swg27047121).

__ • You can also back up your custom content by typing the following command:

```
/opt/qradar/bin/contentManagement.pl --action export --content-type all
```

Depending on the environment size, it could take hours, days, or in some cases weeks for the export to complete in large environments. For more information, see QRadar: Best practices when using the Content Management Tool to export custom data.

__ • Confirm that all appliances in your deployment are at the same software version by typing the following commands:

```
/opt/qradar/support/all_servers.sh -C -k /opt/qradar/bin/myver >
myver_output.txt
```

```
cat myver_output.txt
```

__ • Confirm that all previous updates are unmounted by typing the following commands:

```
/opt/qradar/support/all_servers.sh -k "umount /media/cdrom"
```

```
/opt/qradar/support/all_servers.sh -k "umount /media/updates"
```

__ • If you have HA appliances in your deployment:

- Verify that the `/store` file system is mounted on the primary appliance and not mounted on the secondary appliance.
- Verify that the `/transient` file system is mounted on both the primary and secondary appliances.

__ • Review system notifications for errors and warnings for the following messages before you attempt to update. Resolve these error and warning system notifications before you attempt to update:

- Performance or event pipeline degradation notifications
- Memory notifications
- TX sentry messages or process stopped notifications
- HA active or HA standby failure system notifications
- Disk failure system notifications
- Disk Sentry noticed one or more storage partitions are unavailable notifications
- Time synchronization system notifications
- Unable to execute a backup request notifications
- Data replication experiencing difficulty notifications
- RAID controller misconfiguration notifications

__ • Manually deploy changes in the user interface to verify that it completes successfully.

__ • Verify that the latest configuration backup completed successfully and download the file to a safe location.

__ • Ensure that all apps on your system are updated. Out-of-date apps might not work after you upgrade QRadar.

__ • Resolve any issues with applications in an error state or not displaying properly.

__ • App Nodes are no longer supported as of V7.3.2. If you have an App Node in your deployment, follow the steps in "Migrating from an App Node" in the *IBM QRadar Administration Guide* before you start the upgrade.

Chapter 2. Upgrading QRadar SIEM

You must upgrade all of the IBM QRadar products in your deployment to the same version.

Before you begin

When you run the upgrade, any QRadar Event Collectors are detected. These event collectors must be migrated from GlusterFS to Distributed Replicated Block Device before the upgrade can continue. For more information, see "Migrating event collectors from GlusterFS to Distributed Replicated Block Device" on page 4.

Determine the minimum QRadar version that is required for the version of QRadar to which you want to update.

- Click **Help** > **About** to check your current version of QRadar.
- To determine whether you can upgrade to a version of QRadar, go to QRadar Software 101 (https://www.ibm.com/community/qradar/home/software/) and check the release notes of the version you want to upgrade to.

About this task

To ensure that IBM QRadar upgrades without errors, ensure that you use only the supported versions of QRadar software.

Important:

- Software versions for all IBM QRadar appliances in a deployment must be the same version and fix level. Deployments that use different QRadar versions of software are not supported.
- Custom DSMs are not removed during the upgrade.

Upgrade your QRadar Console first, and then upgrade each managed host. In high-availability (HA) deployments, when you upgrade the HA primary host, the HA secondary host is automatically upgraded.

The following QRadar systems can be upgraded concurrently:

- Event processors
- Event collectors
- Flow processors
- QFlow collectors
- Data nodes
- App hosts

With QRadar 7.5.0 Update Package 2 you can enable secure boot. If Secure Boot is to be enabled on the system the public key must be imported after the patch completes. For more information, see Enabling Secure Boot.

Procedure

1. Download the <*QRadar*>.sfs file from Fix Central (www.ibm.com/support/fixcentral).
2. Use SSH to log in to your system as the root user.
3. Copy the SFS file to the `/storetmp` or `/var/log` directory or to another location that has sufficient disk space.

   Important: If the SFS file is in the `/storetmp` directory and you do not upgrade, when the overnight diskmaintd.pl utility runs, the SFS file is deleted. For more information, see Daily disk maintenance (https://www.ibm.com/support/pages/qradar-732-files-storetmp-are-removed-daily-disk-maintenance).

To verify you have enough space (5 GB) in the QRadar Console, type the following command:

```
df -h /storetmp /var/log | tee diskchecks.txt
```

Important: Don't copy the file to an existing QRadar system directory such as the `/store` directory.

4. To create the `/media/updates` directory, type the following command:

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

5. Use the command **cd** to change to the directory where you copied the SFS file.
6. To mount the SFS file to the `/media/updates` directory, type the following command:

```
mount -o loop <QRadar>.sfs /media/updates
```

7. To run the installer, type the following command:

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

If you receive the following error message, you have a QRadar Incident Forensics appliance in your deployment. Download the QRadar Incident Forensics patch file from IBM Fix Central (www.ibm.com/support/fixcentral). The patch file is named similar to this one: <identifier>_Forensics_patchupdate-<build_number>.sfs. For more information about upgrading with a QRadar Incident Forensics appliance in your deployment, see Upgrading QRadar Incident Forensics.

```
Error: This patch is incompatible with Forensics deployments
[ERROR](testmode) Patch pretest 'Check for QIF appliances in deployment' failed.
(check_qif.sh)
[ERROR](testmode) Failed 1/8 pretests. Aborting the patch.
[ERROR](testmode) Failed pretests
[ERROR](testmode) Pre Patch Testing shows a configuration issue. Patching this host cannot
continue.
[INFO](testmode) Set ip-130-86 status to 'Patch Test Failed'
[ERROR](testmode) Patching can not continue
[ERROR] Failed to apply patch on localhost, not checking any managed hosts.
An error was encountered attempting to process patches.
Please contact customer support for further assistance.
```

What to do next

1. Unmount `/media/updates` by typing the following command:

```
umount /media/updates
```

2. Delete the SFS file.
3. Perform an automatic update to ensure that your configuration files contain the latest network security information. For more information, see Checking for new updates.
4. Delete the patch file to free up space on the partition.
5. Clear your web browser cache. After you upgrade QRadar, the **Vulnerabilities** tab might not be displayed. To use QRadar Vulnerability Manager after you upgrade, you must upload and allocate a valid license key. For more information, see the *Administration Guide* for your product.
6. Determine whether there are changes that must be deployed. For more information, see "Deploying Changes" in *IBM Security QRadar SIEM Administration Guide*.

Related information

QRadar Software 101

Migrating event collectors from GlusterFS to Distributed Replicated Block Device

If the QRadar upgrade detects stand-alone or clustered event collectors with GlusterFS in your deployment, the upgrade fails. You must run a migration script separately on QRadar 7.3.2 Fix Pack 3

or later before you upgrade to QRadar 7.4.2 or later. If your event collectors are deployed on QRadar 7.1 or earlier and then upgraded to a later version, you must upgrade the file systems table (fstab) before you migrate GlusterFS to Distributed Replicated Block Device.

Before you begin

Ensure that terminals are closed within the `/store` partition on the event collectors before you run the script.

About this task

You can migrate the event collectors from GlusterFS to Distributed Replicated Block Device without upgrading to a new version of QRadar. However, your event collectors must be migrated to Distributed Replicated Block Device if you upgrade to QRadar 7.4.2 or later. The migration can be only started from the QRadar Console and runs sequentially on several event collectors. A backup check runs to ensure that enough space is available to back up the `/store` partition.

Important: If you have a large /store partition, for example 50 TB, creating the high-availability Distributed Replicated Block Device might take a few days to complete. You must wait until the synchronization completes before you upgrade QRadar.

Procedure

1. Download the latest version of the migration script from the Script 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).
2. Copy the migration script that you downloaded to the QRadar Console by typing the following command:

   ```
   scp <filename> <user>@<IP_address>:/opt/qradar/ha/bin/<filename>
   ```

   Important: This script must be copied to the directory `/opt/qradar/ha/bin` or it doesn't run.
3. In the directory `/opt/qradar/ha/bin/`, enter the following command to set the permissions on the script.

   ```
   chmod +x glusterfs_migration_manager-<script_version>.bin
   ```
4. To verify the script, run the following command:

   ```
   ls -ltrh glusterfs_migration_manager-<script_version>.bin
   ```

   The result might look similar to this example:

   ```
    -rwxr-xr-x 1 root root 9.8M Feb  9 12:14 glusterfs_migration_manager-<script_version>.bin
   ```
5. For all versions of QRadar, run the migration script from the QRadar Console by typing the following command:

   ```
   /opt/qradar/ha/bin/glusterfs_migration_manager-<script_version>.bin -m
   ```

   Important: If you get an error that there is not enough storage space during migration from GlusterFS to Distributed Replication Block Device, do not point to the `/store` directory. Pointing to the `/store` directory interferes with the stability of the system. For more information, see https://www.ibm.com/support/pages/node/6413281 (https://www.ibm.com/support/pages/node/6413281).

   The following table describes the migration parameters that you can use in the command.

Table 1. GlusterFS migration parameters	
Parameters	**Description**
-h	Shows the help information for GlusterFS migration.
-p	Copies this executable file and runs the precheck on all hosts that might require a migration.
-m	Starts the migration process on all applicable hosts. By default the /storetmp/backup partition is used to back up the /store partition but you can provide a different backup partition with the migrate option.
-s	Provides details about the migration status of applicable hosts in the deployment.
--debug	Runs with another option to enable debug output.

The time to complete the migration of a single HA event collector host is approximately 20 - 25 minutes. The time depends on how much data is backed up before the `/store` partition is wiped to make space for Distributed Replicated Block Device.

Results

All services are stopped on the event collectors during migration from GlusterFS to Distributed Replicated Block Device. After the event collectors are migrated, the event collector works the same way as any other host that uses Distributed Replicated Block Device.

What to do next

Chapter 2, “Upgrading QRadar SIEM,” on page 3

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.

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.

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