IBM Security QRadar Risk Manager
Version 7.1.0 (MR1)

Data Backup and Restore Technical Note

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page 7.

CONTENTS

1 DATA BACKUP AND RESTORE

IBM Security QRadar Risk Manager includes a command-line interface (CLI) script for backing up stored data on IBM Security QRadar SIEM managed hosts. Use the CLI script to restore IBM Security QRadar Risk Manager after a data failure or hardware failure on the appliance.

A backup script is included in QRadar Risk Manager, which can be scheduled using crontab. The script automatically creates a daily archive of QRadar Risk Manager data at 3:00 AM. By default, QRadar Risk Manager keeps the last five backups. If you have network or attached storage, you need to create a cron job to copy QRadar Risk Manager back archives to a network storage location.

The backup archive includes the following data:

- QRadar Risk Manager device configurations
- connection data
- topology data
- policy monitor questions
- QRadar Risk Manager database tables

If you are migrating from QRadar Risk Manager Maintenance Release 5 to this current release of QRadar Risk Manager, see the *IBM Security QRadar Risk Manager Migration Guide*.

Before you begin

Before you backup or restore your data, consider these factors:

- Data is backed up in the **/store/qrm_backups** local directory.
- Daily data backups are created at 3:00 AM. Only the last five backup files are stored.
- The version of the appliance that created the backup in the archive is stored. A backup can only be restored in a QRadar Risk Manager appliance if it is the same version.
- A backup archive is not created if there is not enough free space on QRadar Risk Manager.
- Your system might include a mount /store/backup from an external SAN or NAS service. This allows long term off-line retention of data. Long term storage might be required for compliancy regulations, such as Payment Card Industry (PCI) standards.
- Backup files are saved using the format,

  backup-<target date>-<timestamp>.tgz

  Where:

  <target date> is the date that the backup file was created. The format of the target date is **<day>_<month>_<year>**.

  <timestamp> is the time that the backup file was created. The format of the timestamp is **<hour>_<minute>_<second>**.

Backing up your data

Although QRadar Risk Manager is configured to automatically create a daily backup daily at 3:00 AM, you can start the backup process manually.

To manually start a QRadar Risk Manager backup:

Step 1 Using SSH, log in your QRadar SIEM Console as the root user:

Username: **root**

Password: **<password>**

Step 2 Using SSH from the QRadar SIEM Console, log in to QRadar Risk Manager:

Username: **root**

Password: **<password>**

Step 3 To start a QRadar Risk Manager backup, type the following command:

/opt/qradar/bin/dbmaint/risk_manager_backup.sh

It can take several minutes for the script to start the backup process. After the script completes, the following message is displayed:

```
Tue Sep 11 10:14:41 EDT 2012 - Risk Manager Backup complete,
wrote /store/qrm_backups/backup-2012-09-11-10-14-39.tgz
```

Restoring data

A separate script is used to restore data. This allows you to restore data from a QRadar Risk Manager backup. Use the restore script to specify the archive that you are restoring to QRadar Risk Manager. This process requires you to stop services on QRadar Risk Manager. Stopping services logs off all QRadar Risk Manager users and stops multiple processes.

NOTE

The QRadar Risk Manager appliance and the backup archive must be the same version of QRadar Risk Manager. If the script detects a version difference between the archive and the QRadar Risk Manager managed host, an error is displayed.

To restore a QRadar Risk Manager from a backup archive:

Step 1 Using SSH, log in your QRadar SIEM Console as the root user:

Username: **root**

Password: **<password>**

Step 2 Using SSH from the QRadar SIEM Console, log in to QRadar Risk Manager:

Username: **root**

Password: **<password>**

Step 3 Type the following command to stop hostcontext:

```
service hostcontext stop
```

Step 4 To restore a backup archive to QRadar Risk Manager, type:

```
/opt/qradar/bin/risk_manager_restore.sh -r
/store/qrm_backups/<backup>
```

Where **<backup>** is the QRadar Risk Manager archive you want to restore.

For example:

```
/opt/qradar/bin/risk_manager_restore.sh -r
/store/qrm_backups/backup-2012-09-11-10-14-39.tgz
```

Table 1 Optional restore parameters

Parameters	Description
-f	Overwrites any existing QRadar Risk Manager data on your system with the data in the restore file. Selecting this parameter allows the script to overwrite any existing device configurations in Configuration Source Management with the device configurations from the backup file.
-w	Do not delete directories before restoring QRadar Risk Manager data.
-h	Displays the help for the restore script.

The following message is displayed:

```
Tue Sep 11 16:47:22 EDT 2012 - Risk Manager Restore v1 - starting
risk_manager_restore.sh; ArchiveFile=/store/qrm_backups/backup-201
12-09-11-16-27-42.tgz, Force Overwrite=true
Tue Sep 11 16:47:22 EDT 2012 - Risk Manager Restore v1 - Appliance is QRM
Tue Sep 11 16:47:22 EDT 2012 - Risk Manager Restore v1 - archive is from version
'372011'
Tue Sep 11 16:47:23 EDT 2012 - Risk Manager Restore v1 - appliance version is 372011
Tue Sep 11 16:47:33 EDT 2012 - Risk Manager Restore v1 - restoring db postgres
Tue Sep 11 16:47:34 EDT 2012 - Risk Manager Restore v1 - restoring db qradar
Tue Sep 11 16:47:36 EDT 2012 - Risk Manager Restore v1 - restoring db ziptie
Tue Sep 11 16:47:36 EDT 2012 - Risk Manager Restore v1 - complete.
```

QRadar Risk Manager data is restored from the backup archive.

Step 5 Type the following command to start hostcontext:

`service hostcontext start`

After the hostcontext services are started, then the data restore from the backup archive is complete.

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*.