IBM Security QRadar
Version 7.1.0 (MR1)

Restoring Data Technical Note

Note: Before using this information and the product that it supports, read the information in “Notices and trademarks” on page 9.

CONTENTS

1 RESTORE DATA

You can backup your configuration information and data using the IBM Security QRadar SIEM Admin tab. The data portion of the backup includes all offenses (including source and destination IP address information), asset data, event category information, vulnerability data, event data, and flow data located on your QRadar SIEM Console and managed hosts with storage.

Unless otherwise noted, all references to QRadar refer to IBM Security QRadar SIEM, IBM Security QRadar Log Manager, and IBM Security QRadar Network Anomaly Detection.

For more information about backing up your configuration and data, see the *IBM Security QRadar SIEM Administration Guide*.

If you are using QRadar 6.3 and above, you can restore your configuration information using the QRadar interface, however, you must use the procedures in this document to restore your data.

Before you begin

Each managed host in your deployment, including the QRadar SIEM Console, creates all backup files in the **`/store/backup/`** directory.

Your system might include a mount /store/backup from an external SAN or NAS service, which allows for long term off-line retention of data, as often required for compliancy regulations. For example, PCI.

Before you restore the data, consider the following prerequisites:

- If you are restoring data on a newly installed console, you must restore the configuration backup before restoring the data backup.
- Locate the managed host on which the data is backed up.
- All systems in your deployment with storage capabilities store the backups locally in the following directory: **`/store/backup`**. All backup files are saved using the following format:

  `backup.<name>.<hostname_hostID>.<target date>.<backup type>.<timestamp>.tgz`

  Where:

<name> is the name associated with the backup.

<hostname_hostID> is the name of the QRadar system hosting the backup file followed by the identifier for the QRadar system.

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

<backup type> is the type of backup. The options are **data** or **config**.

<timestamp> is the time that the backup file was created.

- Make sure your **/store** (**/store/ariel**) directory includes adequate space (if your deployment includes a separate mount point for that volume) for the data you want to recover.
- Identify the date and time for the data you want to recover.

Restoring your data

To restore your data:

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

Username: **root**

Password: **<password>**

Step 2 To change the directory, type the following command:

```
cd /store/backup
```

Step 3 To locate the data files you need to restore, type the following command:

```
ls -l
```

A list of backup files is displayed.

For example:

```
total 391528
-rw-r--r--  1 root root 16780568 Apr  2 00:00
backup.scheduled.csd9_2.01_04_2008.config.1207119651365.tgz
-rw-r--r--  1 root root 77382262 Apr  2 00:02
backup.scheduled.csd9_2.01_04_2008.data.1207119722164.tgz
-rw-r--r--  1 root root  9487517 Apr  2 00:00
backup.scheduled.csd9_2.01_04_2008.db.1207119624313.tgz
-rw-r--r--  1 root root 16724841 Mar 30 00:00
backup.scheduled.csd9_2.29_03_2008.config.1206860449624.tgz
-rw-r--r--  1 root root 69970426 Mar 30 00:01
backup.scheduled.csd9_2.29_03_2008.data.1206860499469.tgz
drwxr-xr-x  2 root root     4096 Apr  2 08:58 desc
```

NOTE If no backup files are listed, skip **Step 5**.

Step 4 To change the directory to the root directory, type the following command:

```
cd /
```

The root directory is displayed.

Step 5 To extract the files to their original directory, type the following command:

```
tar -zxpvPf
/store/backup/backup.<name>.<hostname_hostID>.<target date>
.<backup type>.<timestamp>.tgz
```

For example:

```
tar -zxpvPf /store/backup/backup.scheduled.csd9_2.31_03_2008.
data.1207033304942.tgz
```

Output may resemble the following:

```
/store/tmp/backup/database.dump

/var/log/audit/audit.log

/store/reporting/reports/logos/default.png

/store/reporting/reports/admin/reports/DAILY#^#admin#$#1e3d00ea
-69d0-4cda-859c-b7ae72bf7ffa#^#1204174811979/XLS/1e3d00ea-69d0-
4cda-859c-b7ae72bf7ffa.xls

/store/reporting/reports/admin/reports/DAILY#^#admin#$#1e3d00ea
-69d0-4cda-859c-b7ae72bf7ffa#^#1204174811979/data.xml

/store/reporting/reports/admin/reports/DAILY#^#admin#$#1e3d00ea
-69d0-4cda-859c-b7ae72bf7ffa#^#1204174811979/PDF/1e3d00ea-69d0-
4cda-859c-b7ae72bf7ffa.pdf

/store/reporting/reports/admin/reports/DAILY#^#admin#$#Daily At
A Glance Network Security Health
Summary#^#1204174825109/data.xml

/store/reporting/reports/admin/reports/DAILY#^#admin#$#Daily At
A Glance Network Security Health
Summary#^#1204174825109/PDF/Daily At A Glance Network Security
Health Summary.pdf

/store/reporting/reports/admin/reports/DAILY#^#admin#$#Daily
Attacker and Target Summary#^#1204174839555/data.xml

/store/reporting/reports/admin/reports/DAILY#^#admin#$#Daily
Attacker and Target Summary#^#1204174839555/PDF/Daily Attacker
and Target Summary.pdf

/store/reporting/reports/admin/reports/DAILY#^#admin#$#Daily
Delta Network Usage Summary#^#1204174853767/data.xml

/store/reporting/reports/admin/reports/DAILY#^#admin#$#Daily
Delta Network Usage Summary#^#1204174853767/PDF/Daily Delta
Network Usage Summary.pdf

/store/reporting/reports/admin/reports/DAILY#^#admin#$#Daily
Enterprise Network Usage Summary#^#1204174868310/data.xml

/store/reporting/reports/admin/reports/DAILY#^#admin#$#Daily
Enterprise Network Usage Summary#^#1204174868310/PDF/Daily
Enterprise Network Usage Summary.pdf
```

```
/store/reporting/reports/admin/reports/DAILY#^#admin#$#Daily
Executive Application Usage Summary#^#1204174882593/data.xml
/store/reporting/reports/admin/reports/DAILY#^#admin#$#Daily
Executive Application Usage Summary#^#1204174882593/PDF/Daily
Executive Application Usage Summary.pdf
```

Daily backup of data captures all data on each host. The above example reflects a single, all-in-one console, and includes reports, PDF files, event, and flow data. If you want to restore data on a managed host that only contains event or flow data, only that data is restored to that host.

NOTE If you want to maintain the restored data, you can increase your data retention settings to prevent the nightly disk maintenance routines from deleting your restored data. To ensure your restored data is not deleted, see **Verifying data is restored**.

Verifying data is restored

To verify that your data has been restored correctly:

Step 1 To verify the files are restored by investigating one of the restored directories, type the following command:

```
cd /store/ariel/flows/payloads/<yyyy/mm/dd>
```

For example:

```
cd /store/ariel/flows/payloads/2008/3/31
ls
0  1  10  11  12  13  14  15  16  17  18  19  2  20  21  22  23
3  4  5  6  7  8  9
```

You can view the restored directories that are created for each hour of the day. If directories are missing, this may indicate that no data was captured for that time period. For example, the list of files in one of the restored directories can include:

```
ls 0|more
payload_flows~0_0~eb8d3826c5724b01~b56774a558286d05
payload_flows~10_0~ecfb94ded5814c4d~9c5d33d0ec9ec0a6
payload_flows~1_0~94fca21391be44ea~bd32d5dbe8c6a60a
payload_flows~11_0~4d98ae53d2354d41~bde1b8f0684e3829
payload_flows~12_0~2c45af65412c41c6~af424b6b3e5c2e48
payload_flows~13_0~388fe28e9484859~8ca4462103a72bfb
payload_flows~14_0~3e2c90e566d442ca~b7bb031ae09876db
payload_flows~15_0~d382f047a5164281~b2d99a661a9a8e28
payload_flows~16_0~3e18d2a93a1746ca~914d4395a0756c4b
payload_flows~17_0~13383fec3302441f~b237970768894b79
payload_flows~18_0~dcaa5df8d3764c65~a125bd6ca4cd3b76
```

```
payload_flows~19_0~d1ea417c7faf4551~869ef92249918994
```

Step 2 Verify the restored data is now available:

a Log into the QRadar interface.

b Click the **Log Activity** or **Network Activity** tab.

c Select **Edit Search** from the **Search** list box on the toolbar.

The search window is displayed.

d In the Time Range pane, select **Specific Interval**.

e Select the time range of the data you restored in **Step 5**.

f Click **Filter**.

g View the results to verify the restored data.

NOTE

After you have verified that your data is restored to your system, you must re-apply RPMs for any DSMs, vulnerability assessment (VA) scanners, or log source protocols.

For more information on log source protocols, see the *Log Sources Users Guide*.

For more information on DSMs, see the *Configuring DSMs Guide*.

For more information on VA scanners, see the *Managing VA Guide*.

Troubleshoot data restore

If your restored data is not available in the QRadar interface, then you need to verify that:

- Data is restored in the proper location.

  For example, the restored files need to be located in the **`/store`** directory, however, if you typed **`cd`** instead of **`cd /`** in **Step 4**, the files are restored in the directory in which you typed the command (the **`/root/store`** directory). Also, if you omitted **Step 4**, the files are restored in the **`/store/backup/store`** directory.

- File permissions are correctly configured. Typically, files are restored with the original permissions. However, if the files are owned by the root user account, this can cause issues. If this is the case, adjust the files permissions using the **`chown`** and **`chmod`** commands. For assistance, contact customer support.

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*.