IBM Security QRadar
Version 7.2

Reference Data Collections 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 REFERENCE DATA COLLECTIONS

A NOTICES AND TRADEMARKS

1 REFERENCE DATA COLLECTIONS

Use the ReferenceDataUtil.sh utility to make complex reference data collections, such as a Reference Map, Reference Map of Sets, and Reference Map of Maps. This technical note applies to QRadar SIEM, QRadar Network Anomaly Detection, and QRadar Log Manager.

About reference data collections

Reference data collections enable the storage, retrieval and testing of complex data structures. You can create the following reference data collection types:

- **Reference Map** - In a Reference Map, data is stored in records that map a key to a value. For example, to correlate user activity on your network, you can create a reference map that uses the Username parameter as a key and the user's global ID as a value.
- **Reference Map of Sets** - In a Reference Map of Sets, data is stored in records that map a key to multiple values. For example, to test for authorized access to a patent, you can create a Map of Sets that uses a custom event property for **Patent ID** as the key and the **Username** parameter as the value to populate a list of authorized users.
- **Reference Map of Maps** - In a Reference Map of Maps, data is stored in records that map one key to another key, which is then mapped to single value. For example, to test for network bandwidth violations, you can create a Map of Maps that uses the **Source IP** parameter as the first key, the **Application** parameter as the second key, and the **Total Bytes** parameter as the value.

Creating a reference data collection

Using the ReferenceDataUtil.sh utility, you can create a reference data collection.

Before you begin

If you plan to load an external file containing data elements, ensure that the file is in Comma Separated Value (CSV) format. Also ensure that you have copied the file to your QRadar SIEM system.

The file must follow the format in the following examples reference data collections:

Example 1

```
#
# ReferenceMap
#
key1,data
key1,value1
key2,value2
```

Example 2

```
#
# ReferenceMapOfSets
#
key1,data
key1,value1
key1,value2
```

Example 3

```
#
# ReferenceMapOfMaps
#
key1,key2,data
map1,key1,value1
map1,key2,value2
```

The # symbol in the first column indicates a comment line.The first non-comment line is the column header and identifies the column name (ie., key1, key2, data). Then each non-commented line after that is a data record that gets added to the map. Keys are alphanumeric strings.

About this task

See **Utility command reference** for a list of all commands and parameters you can use to manage your reference data collections. You can also type **`./ReferenceDataUtil.sh`** and press **Enter** to access a list these commands

Procedure

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

Username: **`root`**

Password: **`<password>`**

Step 2 Create a reference data collection:

a To change to the /opt/qradar/bin directory, type the following command:

```
cd /opt/qradar/bin
```

b To create the reference data collection, type the following command:

```
./ReferenceDataUtil.sh create <name> [MAP | MAPofSETS |
MAPofMAPS] [timeout_type] [timeToLive]
```

Step 3 To populate the map with data from an external file, type the following command:

```
./ReferenceDataUtil.sh load <name> <filename> [-encoding=...]
[-sdf=" ... "]
```

What to do next

Log in to the QRadar SIEM user interface to create rules that add data to your reference data collections or rule tests that detect activity from elements in your reference data collection. For more information on creating rules and rule tests, see the *IBM Security QRadar SIEM Users Guide*.

Utility command reference

Use the following commands to manage your reference data collections:

Table 1-1 Command reference

Command	Parameters
create	<name> is the name of the reference data collection. [timeout_type] specifies whether the timeToLive is from the time the element was inserted (0) or last seen (1). [timeToLive] specifies the amount of time reference data collection elements remain in the collection. [MAP | MAPofSETS | MAPofMAPS] specifies the type of reference data collection.
update	<name> is the name of the reference data collection. <count> is the maximum number of elements that the reference data collection can contain. [timeout_type] specifies whether the timeToLive is from the time the element was inserted (0) or last seen (1). [timeToLive] specifies the amount of time reference data collection elements remain in the collection.
add	<name> is the name of the reference data collection. <value key1 [key2]> specifies the values you want to add. Key1 is required for MAP, MAPofSETS and key2 is required for MAPofMAPS. Keys are alphanumeric strings.
delete	<name> is the name of the reference data collection <value key1 [key2]> specifies the values you want to delete. Key1 are required for MAP, MAPofSETS and key2 is required for MAPofMAPS [-sdf=" ... "] specifies the Simple Date Format string used to parse the date data.
remove	<name> is the name of the reference data collection

Table 1-1 Command reference

Command	Parameters
purge	<name> is the name of the reference data collection
list	<name> is the name of the reference data collection [loadElements] displays all elements in the specified reference data collection.
listall	[loadElements] displays all elements in all reference data collections.
load	<name> is the name of the reference data collection <filename> is a fully qualified filename to be loaded, with each line in the file representing a record to be added to the reference data collection [-encoding=...] specifies encoding to use when reading the file. [-sdf=" ... "] specifies the Simple Date Format string used to parse the date data.

A NOTICES AND TRADEMARKS

What's in this appendix:

- **Notices**
- **Trademarks**

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.