IBM Security QRadar
Version 7.1.0 (MR1)

Checking the Integrity of Event and Flow Logs 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 CHECKING THE INTEGRITY OF EVENT AND FLOW LOGS

This document provides information on how to check the integrity of event and flow logs to determine if the logs have been modified.

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

NOTE This procedure assumes that log hashing is enabled for your QRadar SIEM system. See the *IBM Security QRadar SIEM Administration Guide* for information on enabling the Flow Log Hashing or Event Log Hashing parameters.

To check the integrity of event and flow logs:

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

Username: **root**

Password: **<password>**

Step 2 Type the following command:

```
/opt/qradar/bin/check_ariel_integrity.sh -d <duration>
-n <database name> [-t <endtime>] [-a <hash algorithm>]
[-r <hash root directory>] [-k <hmac key>]
```

Where:

- **<duration>** is the length of time (in minutes), preceding the end time, to scan the logs. For example, if -d 5 is entered, all logs five minutes preceding the end time are scanned.
- **<database name>** is the type of log to be scanned. Valid logs types are events and flows.
- **<endtime>** is the desired end time for the scan in the following format including the quotation marks: “yyyy/mm/dd hh:mm” where hh is specified in 24-hour format. If no end time is entered, the current time is used.
- **<hash algorithm>** is the hashing algorithm to be used. This algorithm must be the same one that was used to create the hash keys. If no algorithm is entered, SHA-1 is used.

- **<hash root directory>** is the location of the log hashing. This argument is only required if the log hashing is not in the location specified in the configuration file, that is /opt/qradar/conf/arielConfig.xml.
- **<hmac key>** is the key used for Hash-based Message Authentication Code (HMAC) encryption. If you do not specify an HMAC key and your system is enabled for HMAC encrypted, the check_ariel_integrity.sh script defaults to the key specified in the System Settings.

For example, to validate the last ten minutes of event data, type the following command:

```
/opt/qradar/bin/check_ariel_integrity.sh -n events -d 10
```

NOTE To access the help message, type **-h** anywhere in the command line.

```
/usr/java/j2sdk/bin/java -Dapplication.baseURL=file:
/opt/qradar/conf/ -Djava.awt.headless=true -server
-Dapp_id=check_ariel_integrity
com.q1labs.ariel.io.SecureFileWriter -n events -d 10
Verifying files for data base events in
/store/ariel/events/records using hashes from
/store/ariel/events/md
Start time:2008/01/02 09:05
End time:2008/01/02 09:15
Verifying
/store/ariel/events/records/2008/1/2/9/events~14_0~1f87532bbc1e
492b~b6b950c5b22d91f6:OK
Verifying
/store/ariel/events/payloads/2008/1/2/9/payload_events~14_0~1f8
7532bbc1e492b~b6b950c5b22d91f6:OK
Verifying
/store/ariel/events/records/2008/1/2/9/events~13_0~998f550b8888
4eba~841da599f57fe9e7:OK
Verifying
/store/ariel/events/payloads/2008/1/2/9/payload_events~13_0~998
f550b88884eba~841da599f57fe9e7:OK
Verifying
/store/ariel/events/records/2008/1/2/9/events~12_0~33bd57b2286b
4418~a526804245f7a8b1:OK
Verifying
/store/ariel/events/payloads/2008/1/2/9/payload_events~12_0~33b
d57b2286b4418~a526804245f7a8b1:OK
Verifying
/store/ariel/events/records/2008/1/2/9/events~11_0~19f78d8d9f36
4d2b~bc99c943a4493fba:OK
Verifying
/store/ariel/events/payloads/2008/1/2/9/payload_events~11_0~19f
78d8d9f364d2b~bc99c943a4493fba:OK
Verifying
/store/ariel/events/records/2008/1/2/9/events~10_0~fe522c092249
459c~bff4ac8681e01849:OK
```

```
Verifying
/store/ariel/events/payloads/2008/1/2/9/payload_events~10_0~fe5
22c092249459c~bff4ac8681e01849:OK
Verifying
/store/ariel/events/records/2008/1/2/9/events~9_0~ed36bbcfb2584
ff9~b2d802280ef6dc92:OK
Verifying
/store/ariel/events/payloads/2008/1/2/9/payload_events~9_0~ed36
bbcfb2584ff9~b2d802280ef6dc92:OK
Verifying
/store/ariel/events/records/2008/1/2/9/events~8_0~672d8e2f75b94
597~bca3dabe91a03a9a:FAILED
Verifying
/store/ariel/events/payloads/2008/1/2/9/payload_events~8_0~672d
8e2f75b94597~bca3dabe91a03a9a:FAILED
```

If a FAILED or ERROR message is returned, it means that the hash key generated from the current data on the disk does not match the hash key that was created when the data was written to the disk; either the key or the data have been modified.

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.