

TECHNICAL NOTE

CHECKING THE INTEGRITY OF EVENT AND FLOW LOGS

OCTOBER 2009

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



Note: This procedure assumes that log hashing is enabled for your STRM system. See the *STRM 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 Log in to STRM as root.

Step 2 Enter the following command:

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

[Table 1](#) lists and describes the command's parameters.

Table 1 List of Parameters

Parameter	Description
<duration>	Specify the length of time (in minutes), preceding the end time, to scan the logs. For example, if <code>-d 5</code> is entered, all logs five minutes preceding the end time are scanned.
<database name>	Specify the type of log to be scanned. Valid logs types are events and flows .
<endtime>	Specify the desired end time for the scan in the following format including the quotation marks: <code>"yyyy/mm/dd hh:mm"</code> Where hh is specified in 24-hour format. If no end time is entered, the current time is used.
<hash algorithm>	Specify 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.

Table 1 List of Parameters (continued)

Parameter	Description
<hash root directory>	Specify 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.

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

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



Note: To access the help message, enter `-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.qllabs.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 is returned for a log file, 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.

Copyright Notice

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Published: 2009-10-12