Log File Management Tool Deployment and User's Guide

LFMT Audit Information

5/5/2025

Contents

LFMT Audit Information

LFMT Audit Capability

LFMT supports an audit capability, that will write auditing details (LOGIN, LOGOUT, ADD, DELETE, CHANGE) to log files. This information will be made available in the GAX application logs where the LFMT Plug-in is installed.

The LFMT Audit logging can be turned on by setting a new key-value-pair in the "log" options section for the GAX application:

Key Name: **auditing** ; Value = **true**

The above setting will cause new auditing entries to be written to the GAX logs. These new entries will be written during the add, change or delete operation on the tables of the database used by LFMT. When needed, extract these lines from the GAX log(s) that have **LFMT_Audit**, **Log in user** or **logged out** in it.

Important

- Please note that the records for addition, deletion and change are JSON records and can be processed using any standard JSON parser.

- Each of these JSON records also contains the key **complete_record** that represents the record from the Database.

Example

Utilizing the **grep** command (on *nix or UnxUtils on Windows) to extract those entries from the log file *gax20180914_153236_788.log* into an output text file *lfmt_audit_log.txt*.

```
egrep "LFMT_Audit|Log in user|logged out" gax20180914_153236_788.log > lfmt_audit_log.txt
```

This file may contain five different types of audit logs as follows:

Type - 1

Log in: This line is written to the logs when a user logs in.

```
2018-09-14 15:32:46,710 DEBUG: com.genesyslab.gax.core.user.LoginServiceImpl
[qtp142257191-14] - [48] Log in user default
```

This line shows that the user **default** logged in at 2018-09-14 15:32:46,710.

```
2018-09-14 15:47:03,524 DEBUG: com.genesyslab.gax.core.user.LoginServiceImpl
[qtp142257191-12] - [48] Log in user ndatar
```

This line shows that the user **ndatar** logged in at 2018-09-14 15:32:46,710.

Type - 2:

Log out: This line is written to the logs when a user logs out.

```
2018-09-14 15:40:48,617 INFO : com.genesyslab.gax.webservice.UserController [qtp142257191-74]
- [273] User default logged out
```

This line shows that the user **default** logged out at 2018-09-14 15:40:48,617.

```
2018-09-14 15:48:07,165 INFO : com.genesyslab.gax.webservice.UserController
[qtp142257191-128] - [273] User ndatar logged out
```

This line shows that the user **ndatar** logged out at 2018-09-14 15:48:07,165.

Type - 3:

Added Record: This line is written to the logs when a new record is added.

```
2018-09-14 15:33:28,538 INFO : com.genesyslab.gax.lfmt.audit_log_util.AuditLogUtil
[qtp142257191-73] - [34] {"type":"LFMT_Audit_Log","complete_record":"IndexToRegex {[id:1066,
index:null, indexName:test, indexType:index, regularExpression:dds-asdas,
applicationTypes:,258,147,567,994,259,956,989,1004,1003,403,351,997,]}","timestamp":"Fri Sep
14 15:33:28 ADT 2018","mode":"Added","username":"default"}
```

This line shows that a new record was added (**mode : Added**) to the table IndexToRegex at **Fri Sep 14 15:33:28 ADT 2018** by the user **default**.

```
2018-09-14 15:47:39,071 INFO : com.genesyslab.gax.lfmt.audit_log_util.AuditLogUtil
[qtp142257191-128] - [34] {"type":"LFMT_Audit_Log","complete_record":"IndexToRegex {[id:1068,
index:null, indexName:for_testing, indexType:scrub, regularExpression:a=kjkj,
applicationTypes:,1013,916,]}","timestamp":"Fri Sep 14 15:47:39 ADT
2018","mode":"Added","username":"ndatar"}
```

This line shows that a new record was added (**mode : Added**) to the table IndexToRegex at **Fri Sep 14 15:47:39 ADT 2018** by the user **ndatar**.

Type - 4:

Changed Record: This line is written to the logs when the contents of an existing record is changed.

```
2018-09-14 15:36:39,319 INFO : com.genesyslab.gax.lfmt.audit_log_util.AuditLogUtil
[qtp142257191-17] - [34] {"type":"LFMT_Audit_Log","complete_record":"IndexToRegex {[id:1059,
index:null, indexName:sdsd, indexType:index, regularExpression:as=df,
applicationTypes:,258,147,567,1013,916,994,259,956,989,1004,1003,403,351,997,]}","change_details":[{"old_value"
"column_name":"applicationTypes"}],"timestamp":"Fri Sep 14 15:36:39 ADT
2018","mode":"Changed","username":"default"}
```

This line shows that the entry with name **asd** was changed (**mode : Changed**) in the table IndexToRegex at **Fri Sep 14 15:36:39 ADT 2018** by the user **default**.

The changes were:

- Column **regularExpression** was changed from **asd** to **as=df**.

- Column **applicationTypes** was changed from **,258,147,567,994,259,956,989,1004,1003,403,351,997,** to **,258,147,567,1013,916,994,259,956,989,1004,1003,403,351,997,**.

```
2018-09-14 15:47:51,243 INFO : com.genesyslab.gax.lfmt.audit_log_util.AuditLogUtil
[qtp142257191-127] - [34] {"type":"LFMT_Audit_Log","complete_record":"IndexToRegex {[id:1068,
index:null, indexName:for_testing, indexType:scrub, regularExpression:a=kjkj 123,
applicationTypes:,258,147,567,994,259,956,989,1004,1003,403,351,997,]}","change_details":[{"old_value":"a=kjkj
123","column_name":"regularExpression"},{"old_value":",1013,916,","new_value":",258,147,567,994,259,956,989,100
Sep 14 15:47:51 ADT 2018","mode":"Changed","username":"ndatar"}
```

This line shows that the entry with name **asd** was changed (**mode : Changed**) in the table IndexToRegex at **Fri Sep 14 15:47:51 ADT 2018** by the user **ndatar**.

The changes were:

- Column **regularExpression** was changed from **a=kjkj** to **a=kjkj 123**.

- Column **applicationTypes** was changed from **,1013,916,** to **,258,147,567,994,259,956,989,1004,1003,403,351,997,**.

Type - 5:

Deleted Record: This line is written to the logs when an existing record content is deleted.

```
2018-09-14 15:46:30,618 INFO : com.genesyslab.gax.lfmt.audit_log_util.AuditLogUtil
[qtp142257191-117] - [34] {"type":"LFMT_Audit_Log","complete_record":"IndexToRegex {[id:1067,
index:null, indexName:ggh, indexType:index, regularExpression:ghgh-jkjk001,
applicationTypes:,258,147,567,994,259,956,989,1004,1003,403,351,997,]}","timestamp":"Fri Sep
14 15:46:30 ADT 2018","mode":"Deleted","username":"default"}
```

This line shows that the entry with name **ggh** from the table IndexToRegex was deleted (**mode : Deleted**) at **Fri Sep 14 15:46:30 ADT 2018** by the user **default**.

```
2018-09-14 15:48:01,180 INFO : com.genesyslab.gax.lfmt.audit_log_util.AuditLogUtil
[qtp142257191-117] - [34] {"type":"LFMT_Audit_Log","complete_record":"IndexToRegex {[id:1068,
index:null, indexName:for_testing, indexType:scrub, regularExpression:a=kjkj 123,
applicationTypes:,258,147,567,994,259,956,989,1004,1003,403,351,997,]}","timestamp":"Fri Sep
14 15:48:01 ADT 2018","mode":"Deleted","username":"ndatar"}
```

This line shows that the entry with name **for_testing** from the table IndexToRegex was deleted (**mode : Deleted**) at **Fri Sep 14 15:48:01 ADT 2018** by the user **ndatar**.