Operation Manual

WAY4 Audit Log Export

03.53.30

29.04.2021

Contents

The following notation can be used in the document:

- Field labels in screen forms are shown in *italics.*
- Key combinations are shown in angular brackets, for example, <Ctrl>+<F3>.
- Names of screen form buttons and tabs are shown in square brackets, for example, [Approve].
- Sequences for selecting user menu items or context menu items are shown using arrows as follows: "Issuing → Contracts Input & Update".
- Sequences for selecting system menu items are shown using arrows as follows: Database => Change password.
- Variables that differ for each local instance, such as directory and file names, as well as file paths are shown in angular brackets, as in <OWS_HOME>.

Warnings and information are marked as follows:

⚠ Warnings about potentially hazardous situations or actions.

ⓘ Messages with information about important features, additional options, or the best use of certain system functions.

1 Audit log export

To comply with PA DSS requirements, an audit log is automatically generated in WAY4. The log is kept in the SY_AUDIT_LOG table. For a WAY4 instance to be PCI DSS compliant, it is mandatory to keep an audit log for this instance. For more information, see the section "Audit Logs" of the document WAY4™ PA-DSS Implementation Guide".

1.1 Data export

Audit log data is exported by the pipe "com.openwaygroup.pipe.write_audit_log_file.jar". The pipe is run using the menu item "Full → DB Administrator Utilities → Users & Grants → Dump Log".

By default, data from the SY_AUDIT_LOG table is exported to a file in the working directory "WORK_DIR\Data\Audit_Log" (see the OUTPUT_DIRECTORY pipe parameter).

Note that the first time the pipe is run, all SY_AUDIT_LOG table records are exported and the file that is generated may be quite large.

Each subsequent time the pipe is run, only new records that were not previously exported are transferred to the hard disk. A check is made beforehand of whether files have been created for the current export date. If files were created, the size of the last file created is checked. If the file's size does not exceed a certain value (see the LENGTH_LIMIT pipe parameter), new records from the SY_AUDIT_LOG are exported to this file. Otherwise, a new file is created.

1.2 Pipe operating principle

Information about exported files is registered in the FILE_INFO and FILE_RECORD database tables. Information about a file (creation date, file name, file type, etc.) is put into the FILE_INFO table. Information about exported data is put into the FILE_RECORD table.

Information about the process that results in generation of a file is put into the PROCESS_LOG table. The STARTED field of the PROCESS_LOG table contains a timestamp for the start of the data export process.

When the pipe starts, a search in the FILE_INFO table is made for a record of the last exported file (FILE_INFO.FILE_TYPE = 'LOG'). For the file that is found, a timestamp is specified for the start of the process that created the file. For export from the SY_AUDIT_LOG table, records are selected which were created after this timestamp, and for which the value of the SY_AUDIT_LOG table's EVENT_DATE field is greater than the value of the PROCESS_LOG table's STARTED field for the file that was previously exported.

2 "Write Audit Log File" pipe parameters

Parameter	Default value	Parameter description
OUTPUT_DIRECTORY	@WORK_DIR@\Data\Audit_Log	Directory for exported files. It is not recommended to change the default value.
LENGTH_LIMIT	20000	Maximum size of a single file being exported, in lines.
FILTER	Not set	The parameter sets an additional condition for limiting export of data from the SY_AUDIT_LOG table. Sample value: `EVENT_DATE>to_date('01.01.2020','DD.MM.YYYY')`

3 Exported file format and data

File format corresponds to RFC 5424 "The Syslog Protocol".

A file is generated in TSV (Tab Separated Values) format; fields in a line are separated by tab characters and lines are separated by carriage return (CRLF) characters. Table 1 shows file name format.

Table 1. File name

#	Field	Pos	Len	Req	Format	Value
1.	File Name Prefix	1	3	M	an	"LOG".
2.	Delimiter	4	1	M	an	"_" delimiter
3.	File Create Date	5	8	M	Date	File generation date in YYYYMMDD format.
4.	Delimiter	13	1	M	an	"_" delimiter
5.	File Number	14	9	M	n	Serial number of the file for the day.

File line format:

```
<PRIORITY>VERSION   EVENT_TIMESTAMP   HOST_NAME   APPL_NAME   APPL_TYPE   PROCESS_ID
MESSAGE_ID   [SDID@01 STRUCTURED_DATA]   BOM   MESSAGE_TEXT
```

Tables 2 and 5 show mapping of file fields and database table fields. The third column shows the parent table field to which a link is generated in the SY_AUDIT_LOG table field.

Table 2. Correspondence of file fields and database data

#	File field	SY_AUDIT_LOG table field	Parent table field	Field description
1.	PRIORITY			Priority. The value is calculated according to the following formula: Priority = Facility * 8 + Severity (see Table 3 and Table 4).
2.	VERSION			Version (value 1 is used).
3.	EVENT_TIMESTAMP	EVENT_DATE		Event date and time in the format 'YYYY-MM-DD"T"HH24:MI:SS.FF3"Z"'.
4.	HOST_NAME	LOGIN_HISTORY__ID	LOGIN_HISTORY.COMPUTER_NAME	Computer (host) name
5.	APPL_NAME	LOGIN_HISTORY__ID	LOGIN_HISTORY.APPL_NAME	Name of the client application that was used to perform the activity. For example, "DB Manager".
6.	APPL_TYPE	LOGIN_HISTORY__ID	LOGIN_HISTORY.APPL_TYPE	Name of the client application type. For example, "W4W".
7.	PROCESS_ID	PROCESS_LOG__ID	LOGIN_HISTORY.ID	Process identifier
8.	MESSAGE_ID	ID		Message identifier
9.	STRUCTURED_DATA			Data in "key=value" format. See Table 5
10.	BOM			Encoding

#	File field	SY_AUDIT_LOG table field	Parent table field	Field description
11.	MESSAGE_TEXT	MESSAGE_TEXT		Message text generated as a result of the activity

Table 3. Facility

Number	Facility (source)	Facility	Facility (source)
0	kernel messages	12	NTP subsystem
1	user-level messages	13	log audit
2	mail system	14	log alert
3	system daemons	15	clock daemon
4	security/authorization messages	16	local use 0 (local0)
5	messages generated internally by Syslog	17	local use 1 (local1)
6	line printer subsystem	18	local use 2 (local2)
7	network news subsystem	19	local use 2 (local3)
8	UUCP subsystem	20	local use 2 (local4)
9	clock daemon	21	local use 2 (local5)
10	security/authorization messages	22	local use 2 (local6)
11	FTP daemon	23	local use 2 (local7)

Table 4. Severity

Number	Severity
0	Emergency

Number	Severity
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug

Table 5. Possible key values in STRUCTURED_DATA

#	Key	SY_AUDIT_LOG table field	Parent table field	Field description
1.	USER	USER_CODE		Unique user ID for the connection with the Oracle DB.
2.	OFFICER	OFFICER	OFFICER.NAME	User name.
3.	IS_SUCCESS	IS_SUCCESS		Event result.
4.	SESSION_ID	SESSION_ID	LOGIN_HISTORY.ID	Session ID.
5.	EVENT_TYPE	EVENT_TYPE		Event type "M" – Message "S" – Sign On "F" – Sign off

#	Key	SY_AUDIT_LOG table field	Parent table field	Field description
6.	RESOURCE_TYPE	RESOURCE_TYPE		Type of data or system object affected: "A" – Application "F" – Form "M" – Menu
7.	RESOURCE_NAME	RESOURCE_NAME		Name of data or system object type affected. For example, "Upgrade system".
8.	DATA_OBJECT_TYPE	DATA_OBJECT_TYPE		Object type.
9.	DATA_OBJECT_NAME	DATA_OBJECT_NAME		Object name.
10.	DATA_OBJECT_ID	DATA_OBJECT_ID		Object ID.

4 Example of a record in an exported file

```
<110>1  2019-08-15T14:22:08.000Z           w4w-auto             10.101.98.122
WAY4DB    -   18569240             77557240                [SDID@01
USER="TEST_WS2_AUTH500" OFFICER="TEST_WS2_AUTH500" SESSION_ID="41"
IS_SUCCESS="Y" EVENT_TYPE="Single Sign On"
RESOURCE_TYPE="Application" RESOURCE_NAME="W4W"
DATA_OBJECT_TYPE="OFFICER" DATA_OBJECT_NAME="EPICHUGIN"]             BOM
Authentication
type: W4W_PWA
```