Operation Manual

Выгрузка аудитного журнала системы WAY4

03.51.30

28.01.2021

СОДЕРЖАНИЕ

В документации могут использоваться следующие обозначения:

- названия полей экранных форм выделяются *курсивом*;
- комбинации клавиш приводятся в угловых скобках, например, <Ctrl>+<F3>;
- названия кнопок экранных форм и вкладок приводятся в квадратных скобках, например, [Approve];
- последовательность выбора пункта в меню пользователя или контекстном меню отображается с помощью стрелок следующим образом: "Issuing → Contracts Input & Update";
- последовательность выбора пункта в системном меню отображается с помощью стрелок следующим образом: Database => Change password;
- различные переменные значения, например, имена каталогов и файлов, а также пути к файлам, варьируемые для каждой локальной машины, приводятся в угловых скобках, например, <OWS_HOME>.

Предостережения и информационные сообщения размечаются следующим образом:

Предостережения в связи с возможностью совершения неправильных действий.

Сообщения, содержащие информацию о важных особенностях, дополнительных возможностях или оптимальном использовании некоторых функций системы.

1 Выгрузка аудитного журнала

В соответствии с требованиями стандарта PA DSS в системе WAY4 автоматически формируется аудитный журнал. Журнал ведется в таблице SY_AUDIT_LOG. Ведение аудитного журнала является обязательным условием соответствия установленного экземпляра системы WAY4 стандарту PCI DSS. Подробнее см. раздел "Ведение аудитного журнала" в документе "Руководство по обеспечению безопасности в системе WAY4™ согласно стандарту PA-DSS".

1.1 Выгрузка данных

Выгрузка данных аудитного журнала обеспечивается пайпом "com.openwaygroup.pipe.write_audit_log_file.jar". Пайп запускается с помощью пункта меню "Full → DB Administrator Utilities → Users & Grants → Dump Log".

По умолчанию данные из таблицы SY_AUDIT_LOG выгружаются в файл, размещаемый в рабочем каталоге "WORK_DIR\Data\Audit_Log" (см. параметр пайпа OUTPUT_DIRECTORY).

Следует помнить, что при первом запуске пайпа выгружаются все записи таблицы SY_AUDIT_LOG; размер формируемого файла может быть достаточно большим.

При каждом последующем запуске пайпа, на жесткий диск переносятся только новые записи, не выгружавшиеся ранее. Предварительно выполняется проверка, создавались ли файлы в текущую дату выгрузки. Если файлы создавались, проверяется размер последнего созданного файла. Если его размер не превышает заданной величины (см. параметр пайпа LENGTH_LIMIT), новые записи из таблицы SY_AUDIT_LOG выгружаются в данный файл. В противном случае формируется новый файл.

1.2 Принцип работы пайпа

Информация о выгруженных файлах регистрируется в таблицах базы данных (БД) FILE_INFO и FILE_RECORD. В таблицу FILE_INFO помещается информация о файле (дата создания, имя файла, тип файла и т. д.). В таблице FILE_RECORD размещается информация о выгружаемых данных.

Информация о процессе, в результате которого формируется файл, помещается в таблицу PROCESS_LOG. Поле STARTED таблицы PROCESS_LOG содержит временную метку начала работы процесса выгрузки данных.

В момент начала работы пайпа в таблице FILE_INFO ищется запись о последнем выгруженном файле (FILE_INFO.FILE_TYPE = 'LOG'). Для найденного файла определяется временная метка старта процесса, создавшего файл. Для выгрузки из таблицы SY_AUDIT_LOG отбираются записи, созданные после этой временной метки, для которых значение поля EVENT_DATE таблицы SY_AUDIT_LOG больше, чем значение поля STARTED таблицы PROCESS_LOG для предыдущего выгруженного файла.

2 Параметры пайпа "Write Audit Log File"

Параметр	Значения по умолчанию	Описание параметра
OUTPUT_DIRECTORY	@WORK_DIR@\Data\Audit_Log	Каталог для размещения выгруженных файлов. Не рекомендуется изменять значение по умолчанию.
LENGTH_LIMIT	20000	Максимальный размер одного выгружаемого файла в строках.
FILTER	Не задан	Параметр задает дополнительное условие для ограничения выгрузки данных из таблицы SY_AUDIT_LOG. Пример значения: `EVENT_DATE>to_date('01.01.2020','DD.MM.YYYY')`

3 Формат и данные выгружаемого файла

Формат файла соответствует RFC 5424 "The Syslog Protocol".

Файл формируется в формате TSV (tab separated values): поля в строке разделены символом табуляции, строки разделены символом перевода строки (CRLF). В Табл. 1 представлен формат имени файла.

Табл. 1 Имя файла

№	Поле	Поз	Дл	Об	Формат	Значение
1.	File Name Prefix	1	3	M	an	"LOG".
2.	Delimiter	4	1	M	an	Символ разделителя "_".
3.	File Create Date	5	8	M	date	Дата формирования файла в формате YYYYMMDD.
4.	Delimiter	13	1	M	an	Символ разделителя "_".
5.	File Number	14	9	M	n	Порядковый номер файла за день.

Формат строки файла:

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

В таблицах Табл. 2 и Табл. 5 приведено соответствие полей файла и полей таблиц БД. В третьем столбце представлено поле родительской таблицы, на которое формируется ссылка в поле таблицы SY_AUDIT_LOG.

Табл. 2 Соответствие полей файла и данных БД

№	Поле в файле	Поле в таблице SY_AUDIT_LOG	Поле в родительской таблице	Описание поля
1.	PRIORITY			Приоритет. Значение вычисляется по следующей формуле: Priority = Facility * 8 + Severity (см. Табл. 3 и Табл. 4).
2.	VERSION			Версия (используется значение 1).
3.	EVENT_TIMESTAMP	EVENT_DATE		Дата и время события в формате 'YYYY-MM-DD"T"HH24:MI:SS.FF3"Z"'.
4.	HOST_NAME	LOGIN_HISTORY__ID	LOGIN_HISTORY.COMPUTER_NAME	Имя машины (хоста).
5.	APPL_NAME	LOGIN_HISTORY__ID	LOGIN_HISTORY.APPL_NAME	Наименование клиентского приложения, с помощью которого выполнена операция. Например, "DB Manager".
6.	APPL_TYPE	LOGIN_HISTORY__ID	LOGIN_HISTORY.DBMS_SPEC (тег APPLICATION_TYPE)	Наименование типа клиентского приложения. Например, "W4W".
7.	PROCESS_ID	PROCESS_LOG__ID	LOGIN_HISTORY.ID	Идентификатор процесса
8.	MESSAGE_ID	ID		Идентификатор сообщения

№	Поле в файле	Поле в таблице SY_AUDIT_LOG	Поле в родительской таблице	Описание поля
9.	STRUCTURED_DATA			Данные в формате "key=value". См. Табл. 5
10.	BOM			Кодировка
11.	MESSAGE_TEXT	MESSAGE_TEXT		Текст сообщения, формируемого в результате выполнения операции.

Табл. 3 Объект (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)

Табл. 4 Уровень (Severity)

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

Табл. 5 Возможные значения ключей в STRUCTURED_DATA

№	Key	Поле в таблице SY_AUDIT_LOG	Поле в родительской таблице	Описание поля
1.	USER	USER_CODE		Уникальный идентификатор пользователя, используемый для соединения с БД Oracle.
2.	OFFICER	OFFICER	OFFICER.NAME	Имя пользователя.
3.	IS_SUCCESS	IS_SUCCESS		Результат выполнения события.

№	Key	Поле в таблице SY_AUDIT_LOG	Поле в родительской таблице	Описание поля
4.	EVENT_TYPE	EVENT_TYPE		Тип события: "M" – Message; "S" – Sign On; "F" – Sign off.
5.	RESOURCE_TYPE	RESOURCE_TYPE		Тип данных или объекта системы, на которые было произведено воздействие: "A" – Application; "F" – Form; "M" – Menu.
6.	RESOURCE_NAME	RESOURCE_NAME		Имя типа данных или объекта системы, на которые было произведено воздействие. Например, "Upgrade system".
7.	DATA_OBJECT_TYPE	DATA_OBJECT_TYPE		Тип объекта.
8.	DATA_OBJECT_NAME	DATA_OBJECT_NAME		Наименование объекта.
9.	DATA_OBJECT_ID	DATA_OBJECT_ID		Идентификатор объекта.

4 Пример записи в выгружаемом файле

```
<110>1  2021-01-28T12:51:08.000Z    w4w-auto    10.101.98.122   W4WEB51 W4W 21398290
   112355230   [SDID@01 USER="USER" OFFICER="USER" IS_SUCCESS="Y"
EVENT_TYPE="Message" RESOURCE_TYPE="Application" RESOURCE_NAME="START."

DATA_OBJECT_NAME=
"context_id=1440260966;recordset_limit=999;session_idt=7E54B167F7027A34502A3EF2AE56C
959C9BDDA65B561F0A37133969EFDE8B64AD59E5188549C440551D17BEC2B16B1F32931B36E2DF7C0362
FA5D21783FF5A54;"]  BOM
```