Auditing Work with the Database in WAY4™

Contents

Chapter 1. Database Operation Audit

To conform to the requirements of the Payment Card Industry Data Security Standard (PCI DSS – see "Payment Card Industry (PCI) Data Security Standard"), the following user actions must be audited while working with Oracle:

- DBMS administrator actions: modifying the database scheme structure, editing and granting database objects access privileges
- Database user actions: selecting, updating, inserting, and deleting security-sensitive data

Oracle allows audit logs to be written to files or to system tables. For the possibility to accumulate audit records in one place (see "Servicing Audit Records"), it is recommended to set writing to tables.To store audit logs in tables, use the "audit_trail" Oracle parameter. For example, the following command may be used:

```
alter system set audit_trail=db, extended scope=spfile
```

Note that after executing the specified command, the database should be rebooted (shutdown immediate, startup).

Note that use of audit creates the following extra system requirements:

- Administrative actions concerning audit log access limitation and providing their storage must be performed according to the requirements presented in the WAY4™ Security Recommendations According to PCI DSS Administrator Manual.
- Procedures must be developed and executed to regularly archive audit logs due to their substantial size. This is not covered by the WAY4 Housekeeping technology and must also meet the requirements provided in the WAY4™ Security Recommendations According to PCI DSS Administrator Manual.

Administrative Action Audit

Actions related to database object creation or deletion or audit management can be audited using the Oracle Auditing mechanism.

To switch it on, execute the following directive during a "sys" user session:

```
audit
 alter system,
 CLUSTER,
 DATABASE LINK,
 INDEX,
 MATERIALIZED VIEW,
 NOT EXISTS,
 PROCEDURE,
 PUBLIC DATABASE LINK,
```

```
 PUBLIC SYNONYM,
 ROLE,
 SEQUENCE,
 SESSION,
 SYSTEM AUDIT,
 SYSTEM GRANT,
 TABLE,
 TABLESPACE,
 TRIGGER,
 USER, VIEW
by access
```

User Action Audit

The following may be used to audit user activity:

- WAY4 audit log.
- Oracle audit log using Fine Grained Auditing technology.

 It is mandatory to keep an audit log for a WAY4 instance to comply with PCI DSS.

 An Oracle audit log using Fine Grained Auditing technology is an additional means of auditing user actions.

WAY4 Audit Log

The WAY4 audit log is kept in the SY_AUDIT_LOG table. Logging to the audit log is enabled by default. The menu item "Full → DB Administrator Utilities → Users & Grants → Audit Log" is used to view the audit log. For more information, see the section "Audit Logs" of the document "WAY4 PCI DSS Implementation Guide".

Fine Grained Auditing

To log user activity, the Fine Grained Auditing technology (FGA) can be used. The technology allows user identification data, queries and bind variable values to be logged.

In WAY4, the "aud" stored procedure package is used to simplify the work with FGA.

To conform to the PCI DSS requirements to event logging in order to detect any user access to payment card data, it is recommended that access to the tables containing security-sensitive data be audited. A complete list of tables and columns that may contain such information in the standard system configuration can be accessed with the script
<OWS_Home>\install\tools\showEncryptedColumns.ssp using
<OWS_Home>\db\ssp4.bat.

The commands listed in this section must be executed during an "OWNER" user session.

An example of switching on audit:

```
begin
    aud.SET_SQLBINDS('N'); -- disable SQL text and bind values recording
    aud.SET_OPTIONS('N'); -- direct audit into tables
    aud.audit_object(objectname => 'acnt_contract', columnlist => null);
    aud.audit_object(objectname => 'appl_acnt', columnlist => null);
    aud.audit_object(objectname => 'appl_batch', columnlist => null);
    aud.audit_object(objectname => 'card_info', columnlist => null);
    aud.audit_object(objectname => 'card_stop_list', columnlist => null);
    aud.audit_object(objectname => 'coms_log', columnlist => null);
    aud.audit_object(objectname => 'mailbox', columnlist => null);
    aud.audit_object(objectname => 'original_doc', columnlist => null);
    aud.audit_object(objectname => 'pm_task', columnlist => null);
    aud.audit_object(objectname => 'remote_file_req', columnlist => null);
    aud.audit_object(objectname => 'safe_doc', columnlist => null);
    aud.audit_object(objectname => 'telex_auth', columnlist => null);
    aud.audit_object(objectname => 'usage_history', columnlist => null);
    aud.audit_object(objectname => 'voice_auth', columnlist => null);
end;
```

In this example, the "objectname" parameter contains the name of the necessary table, and the "columnlist" parameter contains a list of names of table columns access to which is logged in the audit log. The names are specified in single quotes and separated by commas, for example:

```
columnlist => 'contract_number,id'
```

If the "columnlist" parameter is set to "null", access to the table as a whole is logged in the audit log.

By default, SQL request text and bind variable values are not written to the audit log. However, if required, recording can be enabled by calling:

```
aud.SET_SQLBINDS('Y');
```

instead of the example shown above:

```
aud.SET_SQLBINDS('N');
```

Note that when recording of request text and bind variable values is enabled, critical data may fall into the audit log; for example, card numbers, which presents additional security requirements for access to the logs themselves.

Switching off audit:

```
begin
  aud.noaudit_object(objectname => 'account');
end;
```

Switching off audit of all tables:

```
begin
  aud.noaudit_all;
end;
```

Servicing Audit Records

Oracle Audit can save records in sys.aud$ and sys.fga_log$ (if FGA technology is used) files or tables. By default, records are not archived and cleared and this must be configured in accordance with internal security policies and PCI-DSS. The package DBMS_AUDIT_MGMT can be used to clear archived table records.

The PCI-DSS standard requires that all audit records can be viewed in one place. If a standard WAY4 client application (WAY4 Manager, DB Manager) is used for viewing records, Oracle Audit records must be regularly copied to the general audit storage table sy_audit_log. To do so, the Housekeeping process "Process Audit Log" should be configured to run at night once every 24 hours or once a week (since Oracle audit tables do not have indexes, a query for copying always does a full scan and should not be run too frequently).

Caution! Data will be copied to sy_audit_log even if Oracle Audit writes data to files and not to tables (since in a query, Oracle can read audit data from files), but copying productivity in this case will be lower.

Data is copied by the procedure HSK_ADMIN.APPEND_AUDIT_LOGS which remembers what has already been copied. If necessary, it can be started manually. During copying, duplication is permitted of strings whose event time corresponds to the event time of the last string copied the previous time copying was run