Operation

Oracle Database Audit in Way4

03.53.30

14.07.2021

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 Database audit

To comply with the Payment Card Industry Data Security Standard (PCI DSS, see the document "Payment Card Industry (PCI) Data Security Standard"), when working with the Oracle DBMS, it is necessary to audit the following user actions:

- DBMS administrator actions: changes to the DB schema, editing and granting DB object access privileges.
- DB user actions – viewing, modifying, adding or deleting sensitive data.

Oracle allows audit logs to be written to files or to system tables. To accumulate audit records in one place (see "Managing audit records"), it is recommended to configure writing to tables.

To store audit logs in tables, use the "audit_trail" Oracle parameter. For example, the following command can be used:

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

After this command has been executed, restart the database (shutdown immediate, startup).

Note that the use of audit imposes the following additional system requirements:

- Administrative actions must be performed to restrict access to audit logs and ensure their storage. These actions must be performed pursuant to the requirements set forth in the document "Way4 PA-DSS Implementation Guide".
- It is necessary to develop and run procedures for regular archiving of audit logs, given the significant amount of disk space these logs occupy. These procedures are not covered by Way4 Housekeeping technology and also must comply with the requirements set forth in the document "Way4 PA-DSS Implementation Guide".

1.1 Auditing administrative actions

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

To enable this mechanism, execute the following directive in 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
```

1.2 Auditing user actions

The following may be used to audit user actions:

- Way4 audit log.
- Oracle audit log using Fine Grained Auditing technology.

> For PCI DSS compliance, it is mandatory to keep a Way4 audit log for a Way4 instance.
>
> An Oracle audit log using Fine Grained Auditing technology is an additional means of auditing user actions.

1.2.1 Way4 audit log

The Way4 audit log is kept in the SY_AUDIT_LOG table. Writing to the audit log is enabled by default. To view the audit log, use the menu item "Full → DB Administrator Utilities → Users & Grants → Audit Log". For more information, see the section "Audit Logs" of the document "Way4 PA-DSS Implementation Guide".

1.2.2 Fine Grained Auditing

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

In Way4, the "aud" stored procedure package is used to simplify work with FGA.

To comply with PCI DSS requirements on event logging for recording all user access to payment card data, it is recommended to enable audit of queries to tables containing sensitive data. A complete list of tables and columns that may contain sensitive data 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 in an "OWNER" user session.

Example of enabling 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 table columns to which access is logged in the audit log. 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 entire table is logged in the audit log.

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

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

instead of the example shown above:

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

Note that if logging of SQL text and bind variable values is enabled, sensitive data, for example, card numbers, might get into the audit log. This imposes additional security requirements for access to the logs themselves.

Disabling audit:

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

Disabling audit of all tables:

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

Logging of user actions to the Oracle audit log can be enabled or disabled for a specific user group. The "aud" tag in the OFFICER_GROUP.ADD_INFO field is used to do this. By default, user actions are not logged for technical user groups with "internal=y" in the OFFICER_GROUP.ADD_INFO field. To enable logging of user actions for a technical group, set "aud=y", to disable logging user actions for any group, set "aud=n". The tag is added through update of the record in the OFFICER_GROUP table.

1.3 Managing audit records

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

Pursuant to PCI-DSS, it must be possible to view all audit records in the same 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, configure the Housekeeping "Process Audit Log" process to run at night once every 24 hours or once a week (since Oracle audit tables do not have indexes, the query to select data for copying always does a full scan and should not be run too frequently).

⚠ Data will be copied to sy_audit_log even if Oracle Audit writes data to files and not to tables (since when querying audit data, Oracle can read it from files), but the copying performance in this case will be lower.