Operation

Аудит работы с базой данных в системе WAY4™

03.51.30

14.07.2020

СОДЕРЖАНИЕ

В документации используются 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 Аудит работы с базой данных

Для соответствия требованиям стандарта Payment Card Industry Data Security Standard (PCI DSS – см. документ "Payment Card Industry (PCI) Data Security Standard") при работе с СУБД Oracle необходимо выполнять аудит следующих пользовательских действий:

- действия администратора СУБД – структурные изменения схемы БД, редактирование и выдача прав доступа на объекты БД;
- действия пользователя БД – просмотр, модифицирование, добавление и удаление критичных с точки зрения соблюдения безопасности данных.

Oracle позволяет записывать журналы аудита в файлы или в системные таблицы. Для того, чтобы иметь возможность аккумулирования записей аудита в одном месте (см. "Обслуживание записей аудита"), рекомендуется настраивать запись в таблицы.

Для обеспечения хранения журналов аудита в таблицах следует использовать параметр "audit_trail" СУБД Oracle. Например, может быть использована следующая команда:

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

Следует иметь в виду, что после выполнения указанной команды следует перезагрузить БД (shutdown immediate, startup).

Следует иметь в виду, что использование аудита накладывает следующие дополнительные требования на эксплуатацию системы:

- Необходимо выполнять административные действия по разграничению доступа к журналам аудита и обеспечению их хранения. Данные действия необходимо выполнять согласно требованиям, представленным в документе "Руководство по обеспечению безопасности в системе WAY4™ согласно стандарту PA-DSS".
- Необходимо разработать и выполнять процедуры регулярного переноса в архив журналов аудита с учетом значительных объемов занимаемого ими дискового пространства. Выполнение данных процедур не покрывается технологией WAY4 Housekeeping и должно также удовлетворять требованиям, представленным в документе "Руководство по обеспечению безопасности в системе WAY4™ согласно стандарту PA-DSS".

1.1 Аудит административных действий

Аудит действий, связанных с созданием или удалением объектов БД, а также управлением аудитом может быть выполнен с помощью механизма Oracle Auditing.

Для его включения необходимо в сеансе пользователя "sys" выполнить следующую директиву:

```
  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 Аудит действий пользователей

Для аудита действий пользователей могут использоваться:

- Аудитный журнал системы WAY4.
- Аудитный журнал Oracle с использованием технологии Fine Grained Auditing.

Ведение аудитного журнала WAY4 является обязательным условием соответствия установленного экземпляра системы WAY4 стандарту PCI DSS.
Ведение аудитного журнала Oracle с использованием технологии Fine Grained Auditing является дополнительным средством аудита действий пользователей.

1.2.1 Аудитный журнал системы WAY4

Аудитный журнал системы WAY4 ведется в таблице SY_AUDIT_LOG. По умолчанию запись в аудитный журнал включена. Для просмотра аудитного журнала используется пункт меню "Full → DB Administrator Utilities → Users & Grants → Audit Log". Подробнее см. раздел "Ведение аудитного журнала" в документе "Руководство по обеспечению безопасности в системе WAY4™ согласно стандарту PA-DSS".

1.2.2 Fine Grained Auditing

Для регистрации пользовательской активности можно использовать технологию Fine Grained Auditing (FGA). Данная технология позволяет регистрировать идентификационные данные пользователя, текст запроса и значение bind-переменных.

В системе WAY4 для упрощения работы с технологией FGA используется пакет хранимых процедур "aud".

Для удовлетворения требований стандарта PCI DSS о регистрации событий с целью фиксации любого пользовательского доступа к данным платежных карт рекомендуется включать аудит обращений к таблицам, содержащим критическую для безопасности информацию. Полный список таблиц и столбцов данных, которые могут содержать подобную информацию в стандартной конфигурации системы доступен с использованием скрипта <OWS_Home>\install\tools\showEncryptedColumns.ssp с помощью <OWS_Home>\db\ssp4.bat.

Перечисленные в данном разделе команды необходимо выполнять в сеансе работы пользователя "OWNER".

Пример включения аудита:

```
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;
```

В данном примере параметр objectname содержит наименование требуемой таблицы, а параметр columnlist – список наименований столбцов таблицы, доступ к которым регистрируется в журнале аудита. Данный список указывается в одинарных кавычках через запятую, например:

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

При указании параметру columnlist значения null в журнале аудита регистрируется факт доступа к таблице в целом.

По умолчанию, текст SQL-запроса и значения bind-переменных не записываются в журнал аудита. Однако, если это необходимо, запись можно включить с помощью вызова:

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

вместо приведенного в примере выше:

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

Следует иметь ввиду, что при включении записи текста запроса и значения bind-переменных, в журнал аудита могут попасть критические данные, например, номера карт, что предъявляет дополнительные требования безопасности доступа к самим журналам.

Выключение аудита:

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

Выключение аудита всех таблиц:

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

Существует возможность включать/выключать запись действий пользователей в аудитный журнал Oracle для конкретной группы пользователей с помощью тега "aud" в поле OFFICER_GROUP.ADD_INFO. По умолчанию запись действий пользователей не выполняется для технических групп пользователей, которые имеют значение "internal=y" в поле OFFICER_GROUP.ADD_INFO. Для включения записи действий пользователей для технической группы необходимо задать значение "aud=y", для выключения записи действий пользователей для любой группы задать значение "aud=n". Добавление тега выполнятся через обновление записи в таблице OFFICER_GROUP.

1.3 Обслуживание записей аудита

Oracle Audit может сохранять записи в файлах или таблицах sys.aud$ и sys.fga_log$ (если используется технология FGA). По умолчанию, архивирование и очистка записей не производится и их нужно настраивать в соответствии с внутренней политикой безопасности и PCI-DSS. Для очистки заархивированных записей таблиц можно использовать пакет DBMS_AUDIT_MGMT.

Стандарт PCI-DSS требует, чтобы все записи аудита можно было просматривать в одном месте. Если для просмотра записей используется стандартное клиентское приложение системы WAY4 (WAY4 Manager, DB Manager), то записи Oracle Audit должны регулярно копироваться в общую таблицу хранения аудита SY_AUDIT_LOG. Для этого следует настроить процесс Housekeeping "Process Audit Log" на запуск ночью с периодичностью раз в сутки или раз в неделю (т.к. таблицы аудита Oracle не имеют индексов, то запрос отбора данных для копирования всегда делает полное сканирование (full scan) и не следует его запускать слишком часто).

Копирование данных в SY_AUDIT_LOG будет происходить даже в случае, если Oracle Audit записывает данные не в таблицы, а в файлы (так как при запросе данных аудита Oracle умеет читать их из файлов), но производительность копирования в этом случае будет ниже.

Копирование данных осуществляется процедурой HSK_ADMIN.APPEND_AUDIT_LOGS, которая запоминает, что уже было скопировано. При необходимости, ее можно запускать вручную. При копировании допускается дублирование строк, время события которых совпадает с временем строки, скопированной последней при предыдущем запуске копирования.