WHITE PAPER

UC4.Oracle Database Security Recommendations

For more information about
UC4 products please visit
www.uc4.com.

Introduction

Database security is playing an ever increasing role in preventing the misuse of data on the one hand, and eliminating human error (updating the wrong database) on the other.

This technical white paper shows you how to increase the security of a UC4 installation (UC4 V8.0) and reduce the probability of human error at the same time.

Overview

In the standard installation of UC4, the database objects are created in the UC4 schema and all service processes and users work directly with this user (schema). As a result, the schema objects could potentially be destroyed by human error.

The security recommendation stipulates that there should be a strict separation of the UC4 schema from one or more additional user schemas that have relatively restricted authorizations. This should prevent the schema objects from being modified by accident, thereby improving database security.

SCHEMA NAME (EXAMPLE)	PURPOSE	BRIEF DESCRIPTION
UC4	Application owner	Owner of tables – only used for UC4 software upgrades and patches.
UC4worker	User for worker processes	User with limited rights; may only archive and edit data in the tables of the UC4 schema.
UC4ILM	User for ILM	Only used for ILM Partition Management – otherwise not used.
UC4reader	Interface user	Grant external applications read-only access to UC4.

Synonyms are created to guarantee transparent access to schema objects.

There are two types of synonyms:

PUBLIC SYNONYM ... visible/useable for all database users

Public synonyms are useful if only one application is running on the database.

PRIVATE SYNONYM … only valid for the database user that creates this synonym

This should be used if several applications are running on the database (e.g., UC4 Production and UC4 Development in various schemas)

Enabling the UC4 Security Schema

In the UC4 .ini files, the sixth flag (retrieving field names via owner) in the connect string for the database must be set to “N”. “O” means that only the UC4 application owner schema is working.

Avoiding Name Conflicts

To avoid problems with object or synonym names, you may not grant the UC4 users any additional access rights (this would also run counter to the idea of database security). We recommend using private synonyms in case you are using more than one application schema in the database (regardless of whether it is UC4 or another application).

UC4 Schema

The UC4 schema (user name can be freely selected) is often created with DBA permissions, even though significantly fewer rights would suffice.

The UC4 schema requires the following permissions:

System privileges:

CREATE TABLE
CREATE SEQUENCE
CREATE SESSION
CREATE PROCEDURE
CREATE VIEW
CREATE PUBLIC SYNONYM *
DROP PUBLIC SYNONYM*
ALTER SESSION

* CREATE PUBLIC SYNONYM and DROP PUBLIC SYNONYM are only required if you want to use PUBLIC SYNONYMS – see below.

Furthermore, tablespace quotas are required for all tablespaces that UC4 is supposed to use. Alternatively, you can also allocate the UNLIMITED TABLESPACE system privilege instead of the quotas.

Example of correct authorization for a UC4 schema with Oracle:

```
create user UC4 identified by <PASSWORT>;
alter user UC4 default tablespace <TBSP_NAME>;
alter user UC4 temporary tablespace <TEMPTBS>;
grant create table, create sequence, create session, create procedure, create
public synonym,
      drop public synonym, create view, alter session  to uc4;

alter user UC4 quota unlimited on <TBSP_NAME>; ### for all UC4 tablespaces
```

or alternatively:

```
grant unlimited tablespace to UC4;
```

UC4 Server Database User and UC4USER Role

A separate user is created for the UC4 Server processes, as well as for user access using SQL (several users can also be created). This user is granted all object privileges necessary to work with UC4 via a UC4USER role.

This role also enables the object privileges to be dynamically expanded if new UC4 schema objects are created, without the need for the processes/users to register again.

UC4USER role:

```
connect / as sysdba;
create role UC4user;
```

UC4READONLY role:

```
connect / as sysdba;
create role UC4readonly;
```

UC4 user account (account name can be freely selected):

```
connect / as sysdba;
create user UC4worker identified by <PASSWORT>;
alter user UC4worker temporary tablespace <TEMPTBSP>;
grant create session, alter session to UC4worker;
grant create synonym to UC4worker; ### nur wenn mit PRIVATE Synonyme gearbeitet
wird
grant UC4user to UC4worker
```

UC4 reader account (account name can be freely selected):

```
connect / as sysdba;
create user UC4reader identified by <PASSWORT>;
alter user UC4reader temporary tablespace <TEMPTBSP>;
grant create session, alter session to UC4reader;
grant create synonym to UC4reader; ### nur wenn mit PRIVATE Synonyme gearbeitet
wird
grant UC4readonly to UC4reader;
```

Allocating Object Rights to the UC4USER Role

Object rights are allocated to the UC4USER role by logging into the database as database user UC4 via SQLPLUS. The following commands (script) ensure that the role is supplied with the necessary object rights. This script can be called up again at any time to allocate new UC4 schema objects to the role.

Script UC4USER.sql

```
set head off feed off lines 132 pages 0
spool doUC4USERwork.sql

select 'grant select, update, insert, delete on ' || user || '.' || object_name
||
       ' to  uc4user;'
  from user_objects where object_type like 'TABLE';

select 'grant select on ' || user || '.' || object_name || ' to uc4user;'
  from user_objects where object_type in ('SEQUENCE','VIEW');

select 'grant execute on ' || user || '.' || object_name || ' to uc4user;'
  from user_objects where object_type in ('PACKAGE','FUNCTION','PROCEDURE');

spool off
@doUC4USERwork.sql
```

Execute script UC4USER.sql

```
sqlplus uc4/<pwd>
SQL> @UC4USER.sql
```

Script UC4READONLY.sql

```
set head off feed off lines 132 pages 0
spool doUC4READONLYwork.sql

select 'grant select on ' || user || '.' || object_name ||
       ' to  uc4readonly;'
  from user_objects where object_type like 'TABLE';

select 'grant select on ' || user || '.' || object_name || ' to uc4readonly;'
  from user_objects where object_type in ('VIEW');

spool off
@doUC4READONLYwork.sql
```

Execute script UC4READONLY.sql

```
sqlplus uc4/<pwd>
SQL> @UC4READONLY.sql
```

SYNONYMS for the UC4 Schema Objects

Synonyms are required to enable UC4 Server users direct access to the UC4 schema objects (without SCHEMA.OBJECT syntax).
One advantage of PUBLIC SYNONYMS is that they only have to be defined once and as soon as you allocate the UC4USER role to another Oracle user, this user can then work with UC4.
PRIVATE SYNONYMS are created by UC4 Server users and are valid only for specific users. As a result, there can be no conflicts with other applications in the same Oracle database if UC4 was set up together with other applications in the same database.

Private synonyms are more secure, as other users in the database are not notified about the existence of the UC4 schema objects.

Execute script UC4PUBLICSYN.sql to generate the public synonyms as UC4 user (can be called up as often as desired).

```
set head off feed off lines 132 pages 0
spool doUC4PUBLICSYN.sql

select 'create public synonym ' || object_name || ' for ' || user ||
       '.' || object_name || ';'
  from user_objects
 where object_name in (select object_name from user_objects
                        where object_type in

('TABLE','VIEW','SEQUENCE','PACKAGE','FUNCTION','PROCEDURE')
                       minus
                       select synonym_name from all_synonyms
                        where table_owner=user);
spool off

@doUC4PUBLICSYN.sql
```

Execute script UC4PUBLICSYN.sql

```
      sqlplus uc4/pwd
      SQL> @UC4PUBLICSYN.sql
```

Alternatively, you can also create private synonyms for all UC4 users:

Execute script UC4PRIVATSYN.sql to generate the private synonyms as UC4worker user (can be called up as often as desired).

```
set head off feed off lines 132 pages 0
spool doUC4PRIVATSYN.sql

select 'create synonym ' || ao.object_name || ' for ' || ao.owner ||
       '.' || ao.object_name || ';'
  from all_objects ao
 where ao.object_name in (select object_name from all_objects
                           where object_type in

('TABLE','VIEW','SEQUENCE','PACKAGE','FUNCTION','PROCEDURE')
                             and owner=ao.owner
                       minus
                       select synonym_name from user_synonyms
                        where table_owner=ao.owner)
   and ao.owner in (select distinct owner from all_objects
                     where object_type='TABLE'
                       and object_name in ('OH','AH','UC_TABLE'));
spool off
@doUC4PRIVATSYN.sql
```

Execute script UC4PRIVATSYN.sql as UC4worker, UC4reader, or UC4ILM user

```
sqlplus uc4worker/<pwd>
SQL> @UC4PRIVATSYN.sql
sqlplus uc4reader/<pwd>
SQL> @UC4PRIVATSYN.sql
```

UC4ILM Schema

```
Connect / as sysdba;
create user UC4ILM identified by <PASSWORT>;
alter user UC4ILM default tablespace <TBSP_NAME>;
alter user UC4ILM temporary tablespace <TEMPTBS>;
grant create session, alter session, create synonym  to uc4ILM;
grant uc4user to uc4ILM;
```

Script UC4ILM.sql

```
set head off feed off lines 132 pages 0
spool doUC4ILM.sql

select 'grant alter  on ' || user || '.' || table_name || ' to uc4ILM;'
  from uc_table where table_ilmflag in ('S','R','M') or table_name like 'MQ%';

spool off
@doUC4ILM.sql
```

Execute script UC4ILM.sql

```
sqlplus uc4/<pwd>
SQL> @UC4ILM.sql
```

Execute the script for the PRIVATE synonyms, as long as no public synonyms exist.

```
sqlplus uc4ilm/<pwd>
SQL> @UC4PRIVATSYN.sql
```

Checking for Potential Problems with Objects from Other Application Schemas

The following SQL statement must not generate output, because otherwise other application schema objects with the same name will be displayed for UC4. The access rights to these objects must be revoked from the UC4 user.

```
sqlplus uc4/<pwd>
select owner, table_name, column_name
  from all_tab_columns
 where table_name in (select table_name from user_tab_columns) and owner <>
user;
```

Lock UC4 Schema

As soon as the users, authorizations, and synonyms have been set up, the UC4 schema user account should be locked. This will only be required again for UC4 software upgrades.

Locking the UC4 user account

alter user UC4 account lock;

Unlocking the UC4 user account

alter user UC4 account unlock;

UC4 Software Upgrades

Any UC4 software upgrades that have to be implemented must be carried out by the UC4 user. After the upgrade, the UC4USER role must be assigned the new object privileges and the synonyms must be updated. The result is the following procedure for implementing a UC4 software upgrade:

1) Back up the UC4 database

2) Unlock UC4 user account:

```
alter user UC4 account unlock;
```

3) Install and test software upgrade as UC4 user

4) Restore the authorizations as UC4 user:

```
sqlplus UC4/pwd   @UC4USER.sql
sqlplus UC4/pwd   @UC4READER.sql
sqlplus UC4/pwd   @UC4ILM.sql
```

5) Update synonyms, either
PUBLIC SYNONYMS:

```
sqlplus UC4/pwd  @UC4PUBLICSYN.sql
```

or

PRIVATE SYNONYMS:

```
sqlplus UC4ILM/pwd      @UC4PRIVATSYN.SQL
sqlplus UC4worker/pwd   @UC4PRIVATSYN.sql
sqlplus UC4reader/pwd   @UC4PRIVATSYN.sql
```

6) Lock UC4 user account:

```
alter user UC4 account lock;
```