QUOI RÉVISER POUR LE SOE 3ORC3 ?

CK 01 - Oracle Database Administration

Oracle =

Created in 1977 by Larry Ellison, with his co-founders : Bob Miner & Ed Oates.

3rd biggest company of the World after Microsoft & IBM.

Starts with databases, Exclusive mix of SQL and of relational database.

84,233 employees (09/14/08).

Corporate Headquarters in Redwood Shores, in California.

Represented in 145 countries.

Revenue : $22.43B Billion USD (05/2008).

Certifications : SQL Certified Expert / OCA / OCP / OCM

CK 02 - Basic Oracle Concepts

Relational Database Systems

SQL = System Query Language.

Tasks of an Oracle Database Admin : Install Oracle software, Create DB, Backup, Recover from failure, Monitor, etc.

Oracle Storage architecture :

Control Files

Data Files | Online Redo Log Files

Parameter File | Password File | Archie Log Files

Control Files : Contain physical database structure information

Redo Log Files : Record changes to the database

Tablespaces : Consist of one or more datafiles

Data Files : Belong to only one tablespace

Segments, Extents, and Blocks :

Segments exist within a tablespace

Segments are made of a collection of extents.

Extents are a collection of data blocks.

Data blocks are mapped to OS blocks.

An Oracle Database server consists of an Oracle database and an Oracle instance.

An Oracle instance is made up of memory buffers know as the System Global Area (SGA) and background processes that handle much of the behind-the-scenes work involved in running an instance. The instance is idle (nonexistent) until it is started. When the instance is started, an initialization parameter file is read and the instance is configured according to instructions contained within the parameter file.

After the instance is started and the database is opened, users can access the database.

CK 03 - Managing the Database

Starting and stopping iSQL\*Plus : isqlplusctl start (/stop)

Starting and stopping the listener : lsnrctl start (/stop)

Starting and stopping Enterprise Manager : emctl start (/stop) dbconsole

Startup Stages :

SHUTDOWN

NOMOUNT = Instance started

MOUNT = Control file opened for this instance

OPEN = All files opened as described by the control file for this instance

Shutdown Mode :

ABORT

IMMEDIATE = Force a checkpoint and close files

TRANSACTIONAL = + Wait until current transactions end

NORMAL = + wait until current transactions end

To start an instance, Oracle must read either an initialization parameter file or a server parameter file (SPFILE).

Connecting to Enterprise Manager :

sys/oracle as SUSDBA

SYSTEM/oracle as NORMAL

CK 04 - Administrating Users and Managing Schema Objects

Each database user account has a :

Unique username

Authentication method

Default tablespace

Temporary tablespace

User profile

Three type of authentication :

Password

External

Global

Two types of user privileges :

System= Perform particular actions in the DB. Exemple: CREATE TABLE, SELECT ANY TABLE, etc.

Object= Access and manipulate a specific object. Example: SELECT, INSERT, UPDATE, DELETE, etc.

Roles are named groups of related privileges that are granted to users or to other roles. Designed to ease the admin of privileges in the DB, and improve security.

Predefined Roles :

CONNECT (CREATE SESSION, CREATE TABLE, etc.)

RESOURCE (CREATE TABLE, CREATE INDEX, etc.)

DBA (Most system privileges, several other roles. Do not grant to nonadminstrators.)

A schema is a collection of database objects owned by a particular user. It has the same name as the user that owns it.

Schema Objects : Tables, triggers, indexes, iews, sequences, stored program units, synonyms, user-defined data types, database links.

Common data types : CHAR, VARCHAR2, DATE, NUMBER.

Other : FLOAT, INTEGER, NCHAR, NVARCHAR2, LONG, LONG RAW, RAW, ROWID, UROWID, BLOB, CLOB, NCLOB, BFILE, TIMESTAMP

Indexes : optional structures associated with tables.

Views : Customized representations of data in one ore more table or other views.

Sequence : a database object from which multiple users can generate unique integers. Generally use to generate primary keys values.

CK 05 - Manipulatin Database Data

Oracle's Data Pump utility enables high-speed transfer of data from one database to another.

Use Data Pump Import to load data extracted by Data Pump Export.

SQL\*Loader loads data from external files into tables of an Oracle database.

SQL\*Loader reads data from one or more files specified in the control file.

When SQL\*Loader begins execution, it created a log file.

The Bad Files contains records that were rejected.

Discard File is created only when it is needed and only if you have specified that a discard file should be enabled. It contains records that were filtered out of the load because they didn't match any record-selection criteria specified in the control file.

Loading Methods :

Conventional Path : builds an array of rows to be inserted and uses the SQL INSERT statement to load the data.

Direct Path : builds blocks of data in memory and saves these blocks directly into the extents allocated for the table being loaded.

CK 06 - Securing the Oracle Database

All the users created by DBCA have their accounts marked as EXPIRED & LOCKED

EXPIRED refers to the password

LOCKED means that it is impossible to connect with that account anyway

The passwords for the usable default accounts (SYS, SYSTEM, DBSNMP, and SYSMAN) are set at database creation time.

The other accounts have well-known passwords : they are the same as username.

When you unlock these accounts , you also have to change the password.

For example the SYS and SYSTEM passwords may be on the very well-known defaults of CHANGE\_ON\_INSTALL and MANAGER respectively.

APPLY THE PRINCIPLE OF LEAST PRIVILEGE :

Protect the data dictionnary

(O7\_DICTIONNARY\_ACCESSIBILITY = FALSE)

Revoke unnecessary privileges from PUBLIC

Restrict the directories accessible by users

(UTL\_FILE\_DIR config parameter)

Limit users with administrative privileges

Restrict remote database authentication (REMOTE\_OS\_AUTHENT = FALSE)

PASSWORD PROFILES PARAMETER :

FAILED\_LOGIN\_ATTEMPTS  
 PASSWORD\_LOCK\_TIME

PASSWORD\_LIFE\_TIME

PASSWORD\_GRACE\_TIME

PASSWORD\_REUSE\_TIME

PASSWORD\_REUSE\_MAX

PASSWORD\_VERIFY\_FUNCTION

DBCA expires and locks all accounts, except : SYS, SYSTEM, SYSMAN, DBSNMP.

Oracle Corporation issues regular security updates, usually in the form of patches that you must apply to your Oracle software.

CK 07 - Auditing the Oracle Database.

Monitoring for Suspicious Activity, but it increases the amount of work that the DB must do. In order to limit this workload, you should focus your auditing closely and not track events of minimal significance.

Types of Audit :

Standard database auditing : Privileges used including objects access

Value-base auditing : Data changed by DML statements

Fine-Grained-Auditing (FGA) : SQL statements(insert, update, delete, and select) based on content.

The AUDIT\_SYS\_OPERATIONS instance parameter must be set to TRUE (default is FALSE).

Standard Database Auditing : Audit\_Trail parameter (None/DB/OS).

Can audit : login events, exercise of system/objects privileges, use of SQL statements.

Data dictionnary view : ALL\_DEF\_AUDIT\_OPTS / DBA\_STMT(PRIV/OBJ)\_AUDIT\_OPTS

Audit Trail view DBA\_AUDIT\_TRAIL(EXISTS/OBJECT/STATEMENT)

Value-Based Auditing : Auditing through triggers is a much slower process than database auditing, but it does give you more information.

FGA : Audits SELECT, or INSERT, UPDATE, DELETE. Monitors data access based on content. Can be linked to a table or view. May fire a procedure. Is administered with the DBMS\_FGA package.

FGA Policy : Defines Audit criteria and Audit action. Is created with DBMS\_FGA.ADD\_POLICY

DBMS\_FGA PACKAGE Subprograms : ADD(DROP/ENABLE/DISABLE)\_POLICY

Data dictionnary view: DBA\_FGA\_AUDIT\_TRAIL, ALL(DBA/USER)\_AUDIT\_POLICIES

FGA Guidelines :

To audit all statements, use a null condition

If you try to add a policy that already exists, error ORA- 28101 is raised.

The audited table or view must already exist when you create the policy.

If the audit condition syntax is invalid, an ORA-28112 is raised when the audited object is accessed.

If the audit column does not exist in the table, no rows are audited

If the event handler does not exist, no error is returned and the audit record is still created.