Oracle Database Security

ISACA - Denver October 2014

Ron Reidy

Introduction
Ron Reidy

- SR IT Auditor - Wells Fargo
- Oracle Database security auditor
- Threat modeling
- Web application security
- Operating system security

Began working with Oracle in 1984 (terminal version of Oracle 4)
15 years development
- Oracle forms
- Pro*C/FORTRAN/Pascal
- PL/SQL
- UNIX shell
- Perl
- Python

10 years DBA (production and development)
7+ years security and audit

Agenda

- Overview of Oracle security
- Overview of Oracle architecture
- Data flow in an Oracle database instance
- Data access model
- The Oracle data dictionary
- Account auditing
- Database defaults
- Change management
- Finding sensitive data

Overview of Oracle security

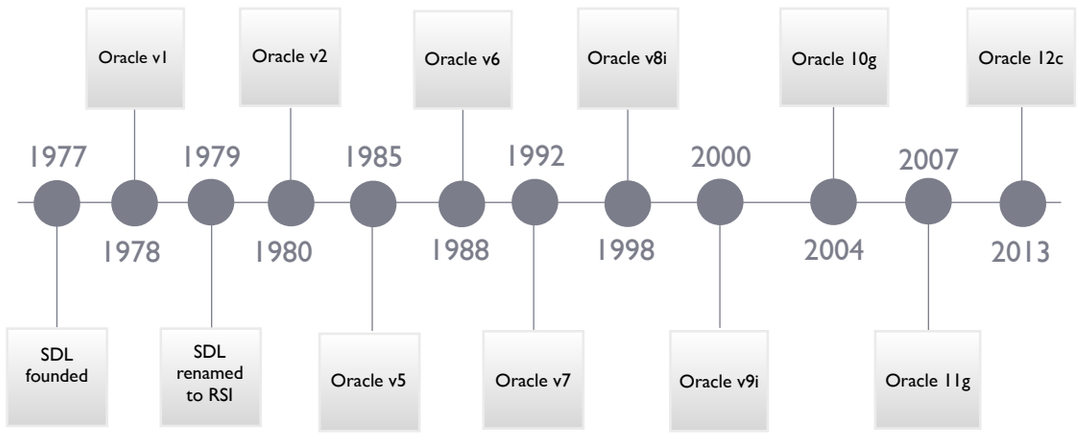
Preliminaries

- No system is 100% secure!
  - If it were100% secure, it would not stay that way
- Oracle is complex
- Oracle is an open system
- Oracle security is complex
  - The more you do it, the easier it will become
- Oracle security is about depth of access

Depth of access

- Access to system privileges or objects can be granted
  - Directly to an account
  - Indirectly through a role
  - Roles can grant access to
    - System privileges
    - Database objects
    - Other roles

Oracle Security Evolution



http://en.wikipedia.org/wiki/Oracle_Corporation#Overall_timeline

Software Development Laboratories (SDL) formed by Larry Ellison, Bob Miner, Ed Oates.

Oracle v1 never released. Oracle was a code name of a CIA project all had worked on at Ampex Corp.

Oracle v2 purchased by Wright Patterson AFB. This version had rudimentary passwords.

Oracle v5 had 3 system privileges - CONNECT, RESOURCE, DBA

Oracle v6 brought in roles. 3 roles - CONNECT, RESOURCE, DBA.

Oracle v6 through v10: 3DES hashing for passwords.

Oracle v7.3 - advanced networking

Oracle v8i - VPD (virtual private database) and FGA (fine grained audit)

Oracle v10gR2 - SHA password hashing with a salt.

Current version of Oracle provides

- Users / Schemas
- Roles

Current security features

- Users / Schemas
- Roles
- System privileges
- Object privileges (on all objects, tables, packages, views…)
- Password and resource management
- Audit features via
  - Core audit
  - Fine Grained Audit (FGA)
  - Triggers
- Identification and authentication
- Virtual Private Database (VPD)
  - Oracle Label Security (OLS)
- Built-in encryption – for database and file system (TDE)
- Network encryption solutions

What has gone wrong with database security

- Most database installations are default with little or no attempt at
  - Hardening
  - Securing
- Oracle doesn't make it easy to secure database software
  - Installation is "open" by default
    - Almost all functions and features are available to almost all users

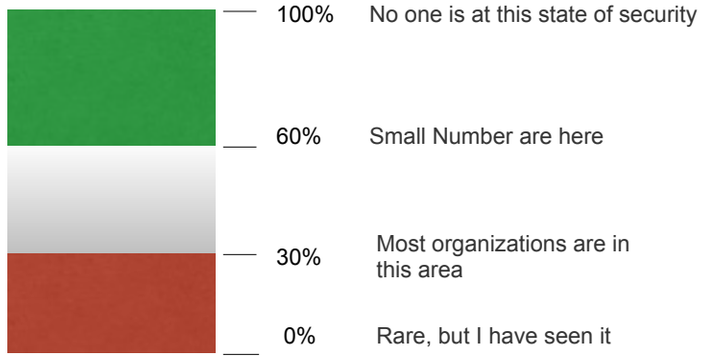
Who wants the data?

- External threat agents
  - Rival companies (espionage)
  - Hackers
  - Activists
  - Nation states
- Internal threat agents
  - Disgruntled employees
  - Hackers
  - Activists

Threat agents can be classified as follows:
- Non-Target Specific: Non-Target Specific Threat Agents are computer viruses, worms, trojans and logic bombs.
- Employees: Staff, contractors, operational/maintenance personnel, or security guards who are annoyed with the company.
- Organized Crime and Criminals: Criminals target information that is of value to them, such as bank accounts, credit cards or intellectual property that can be converted into money. Criminals will often make use of insiders to help them.
- Corporations: Corporations who are engaged in offensive information warfare or competitive intelligence. Partners and competitors come under this category.
- Human, Unintentional: Accidents, carelessness.
- Human, Intentional: Insider, outsider.
- Natural: Flood, fire, lightning, meteor, earthquakes.

Although the unknown attacker is a low probability today you still have to worry about that underpaid accountant in accounts receivables that sells financial information to competitors. Or how about that engineer who really thinks that everyone should be on a level playing field and is generously sharing product designs. Or that really upset person who didn't quit but is now in product development and selling product designs from within the company to a friend who has connections in the European technology marketplace. Not to mention those less than honorable programmers from an ally company that really are not good at doing their own work and are good at borrowing other peoples' work. Don't forget that new marketing guy came from a competitor, and is secretly still working with that competitor by selling spatial data from the demographics firm back to his old company for a handsome fee.

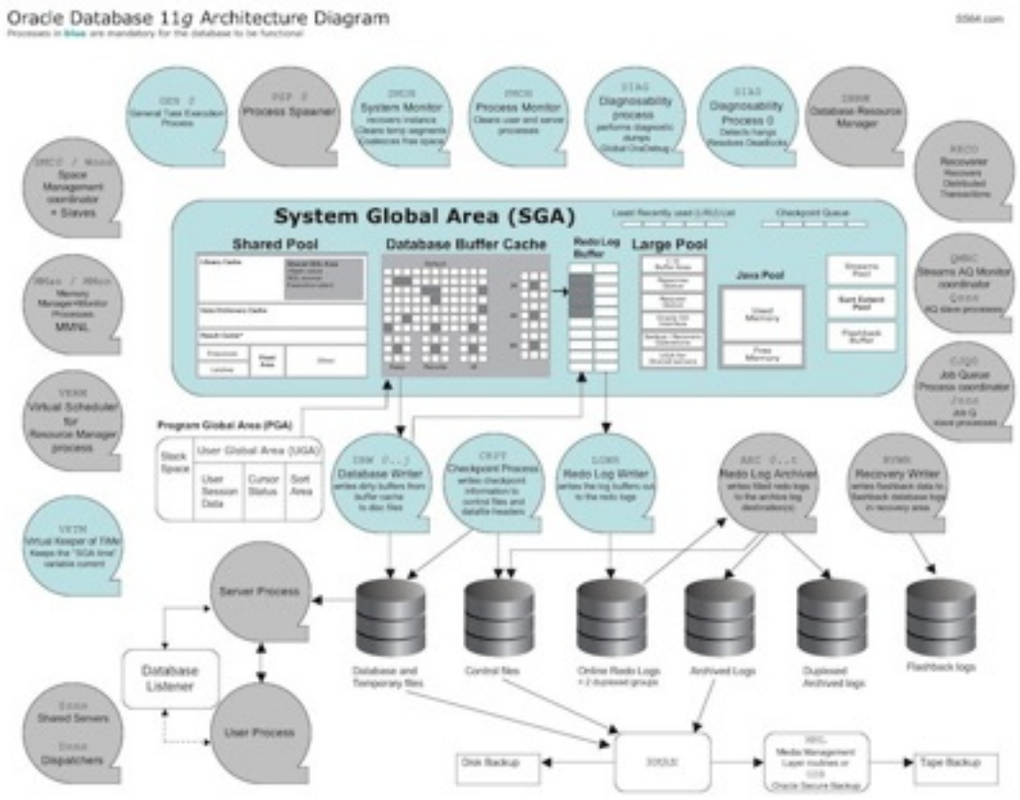
Existing state of database security



Oracle architecture

Oracle RDBMS Architecture

- Oracle database is not just a data store
- Complex system - like an operating system
- Networking services (FIFO pipes, etc.) and support for many protocols (TCP, etc.)
- File subsystem (space allocation, deletion, reuse, recovery, corruption detection, etc.)
- Job schedulers
- Kernel interrupts and instrumentation
- XML storage and processing
- Shared memory and memory pools
- Interprocess communication (IPC) and threading
- Large object storage and processing
- Encryption support at the data storage and network layers (strong algorithms, SSL support)
- Multiple authentication methods (database, Kerberos, LDAP, etc.)



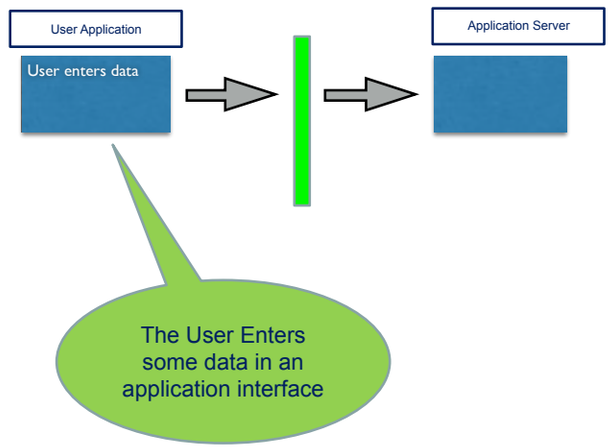
Data flow in an Oracle database instance

Data flow in an Oracle database instance

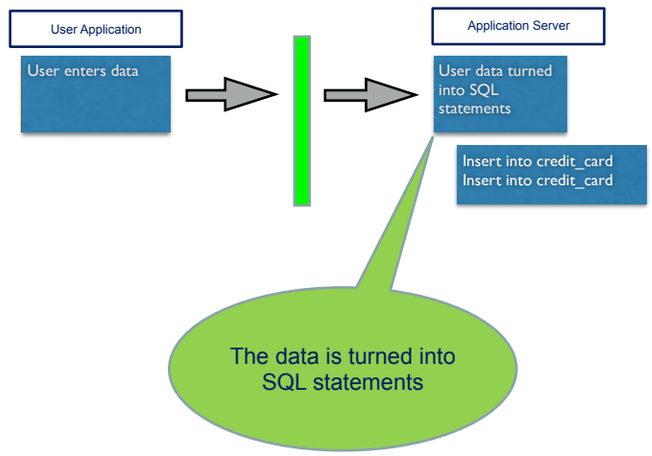
- Data is not static within an Oracle database instance
- The data dictionary is composed of
  - Fixed tables
  - Dynamic views

These structures expose data at all points throughout the system

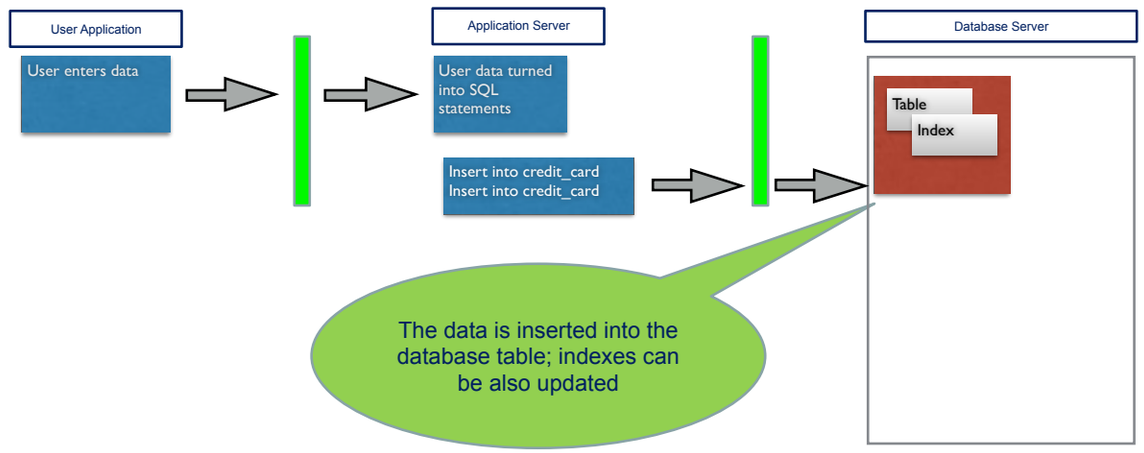
Data flow



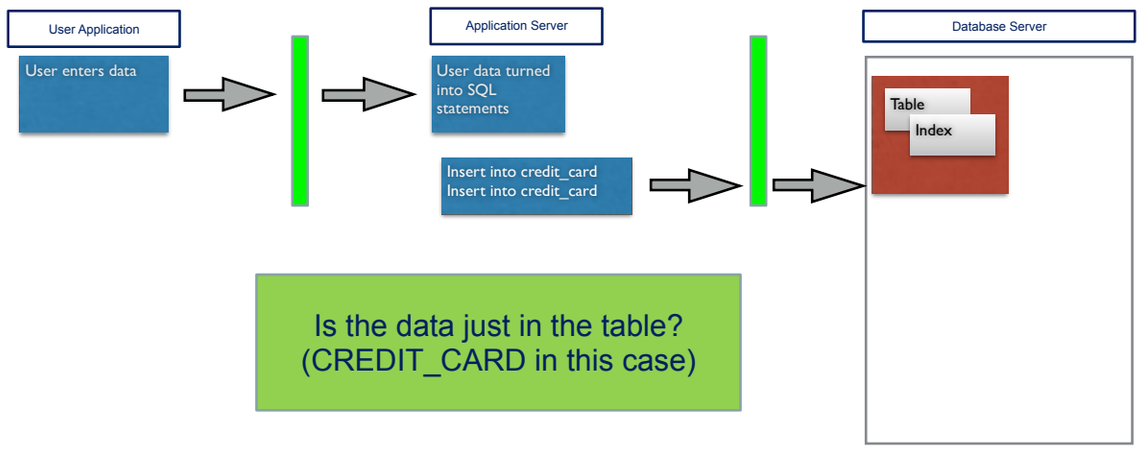
Data flow



Data flow

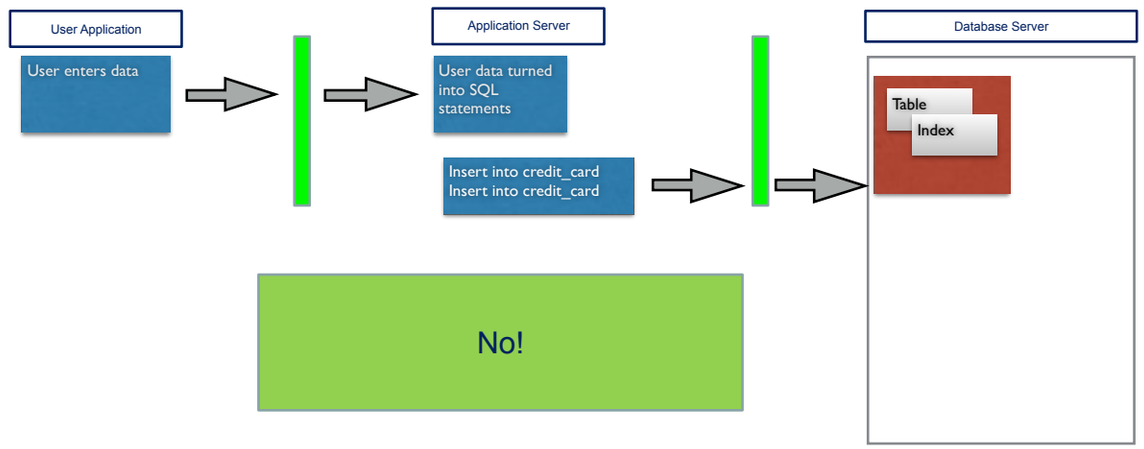


Data flow

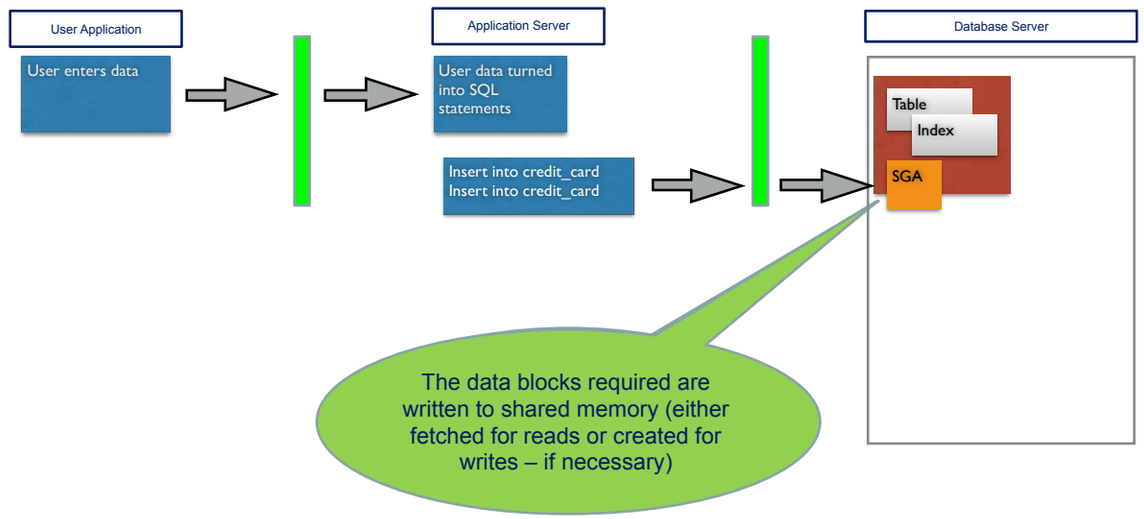


Is the data just in the table?
(CREDIT_CARD in this case)

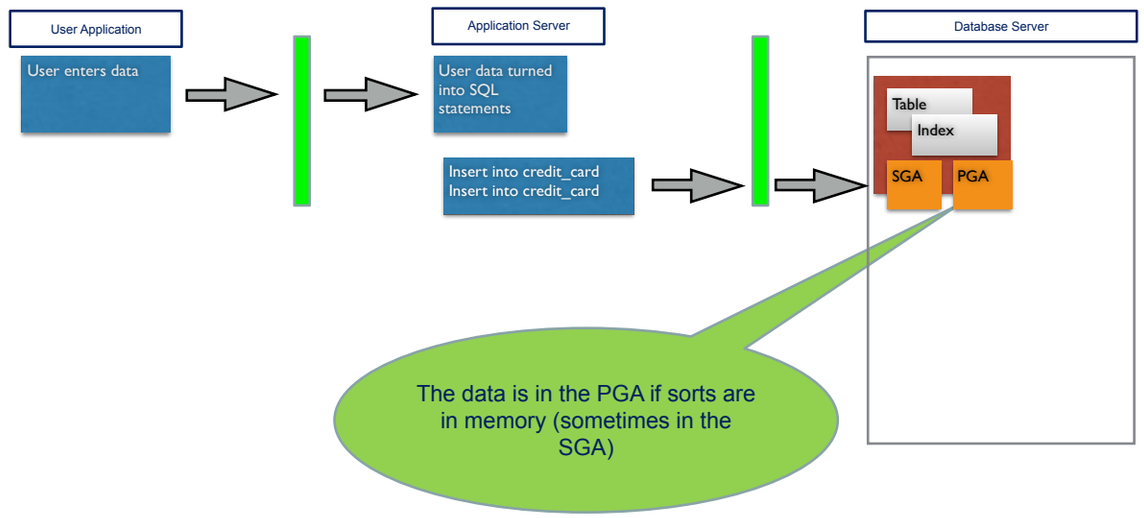
Data flow



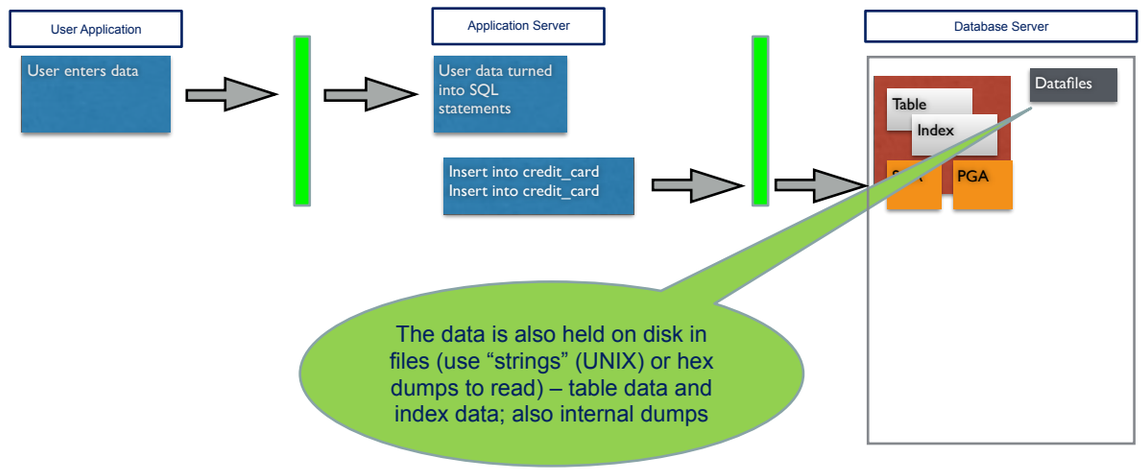
Data flow



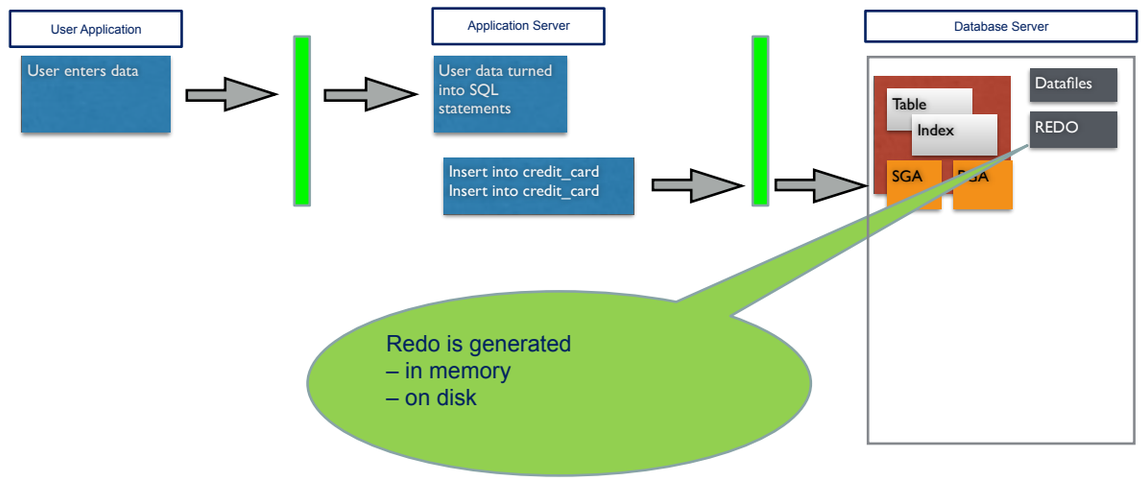
Data flow



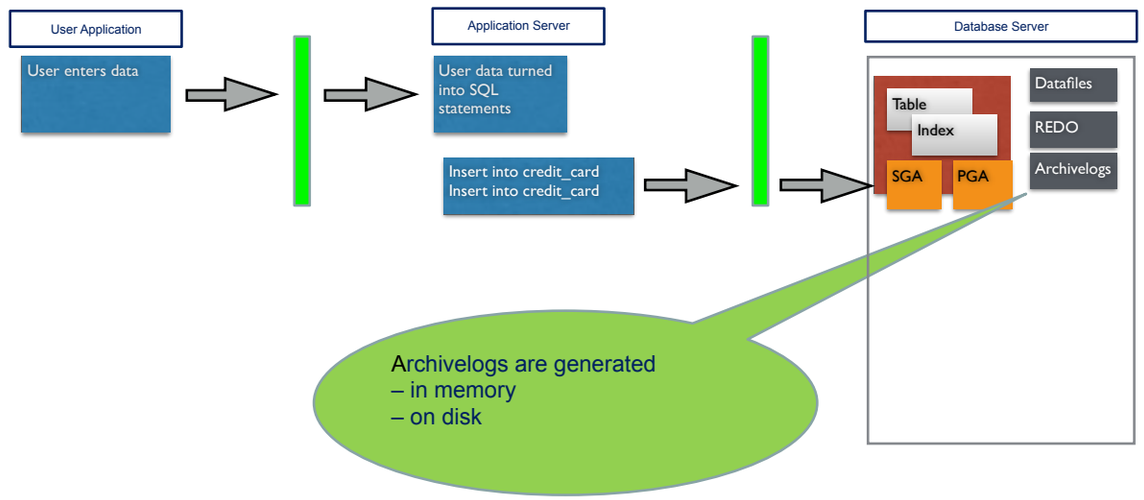
Data flow



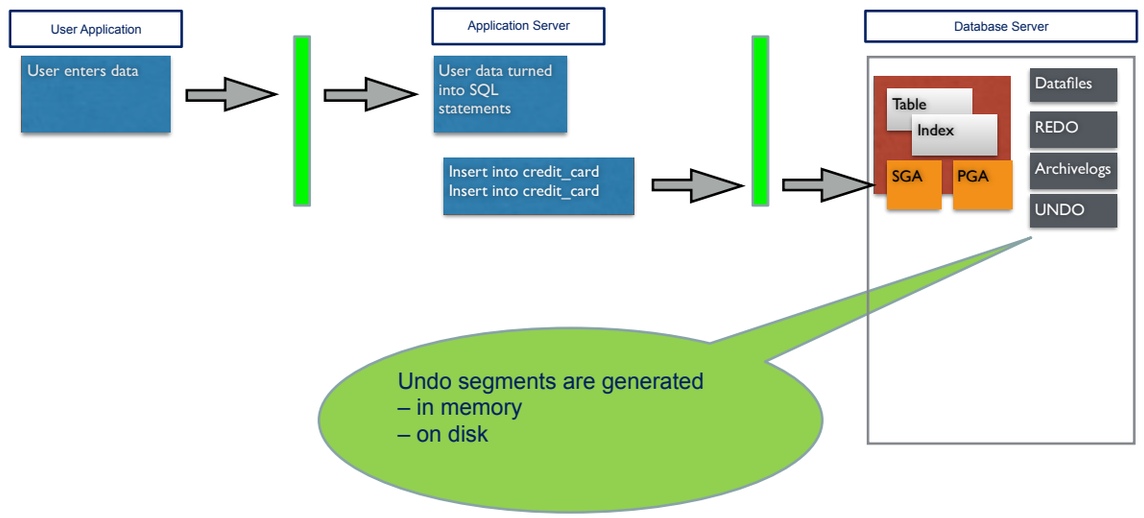
Data flow



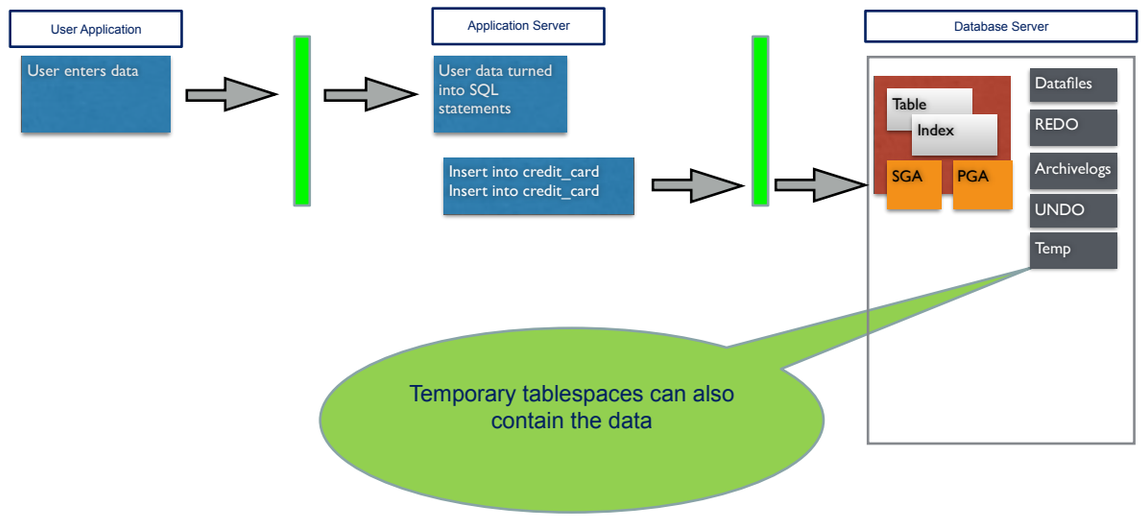
Data flow



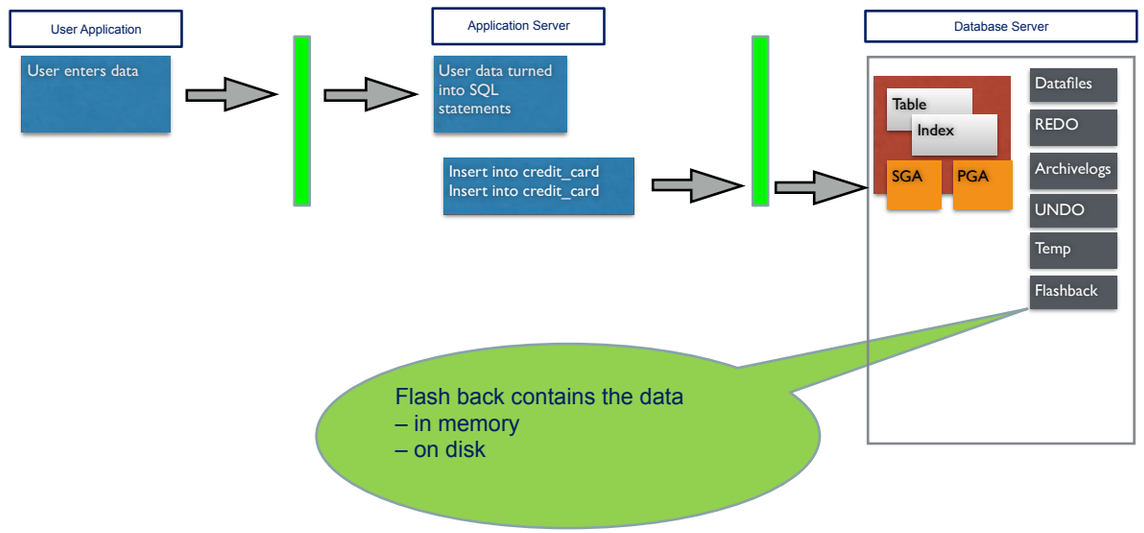
Data flow



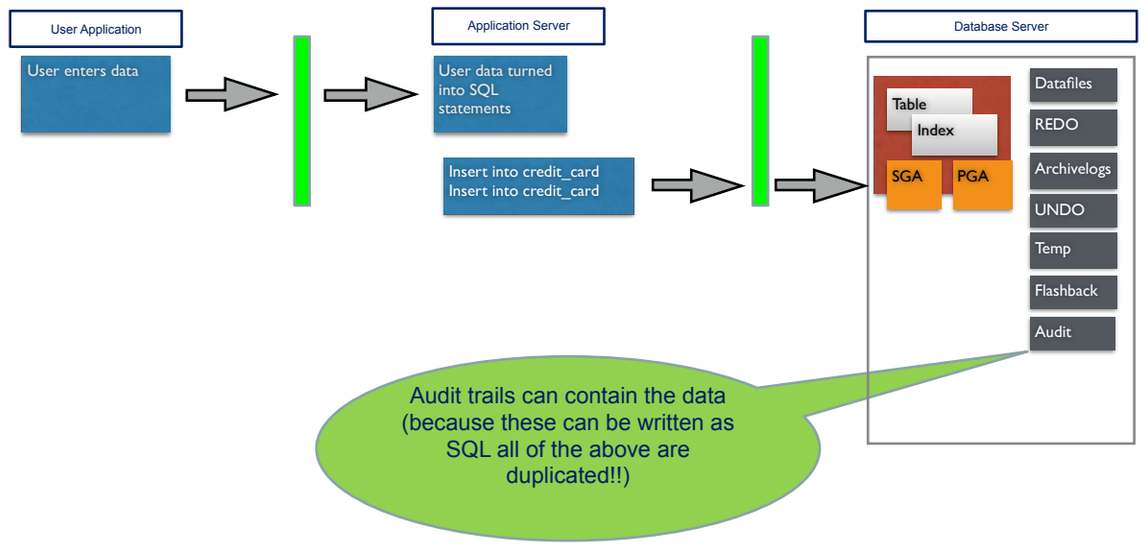
Data flow



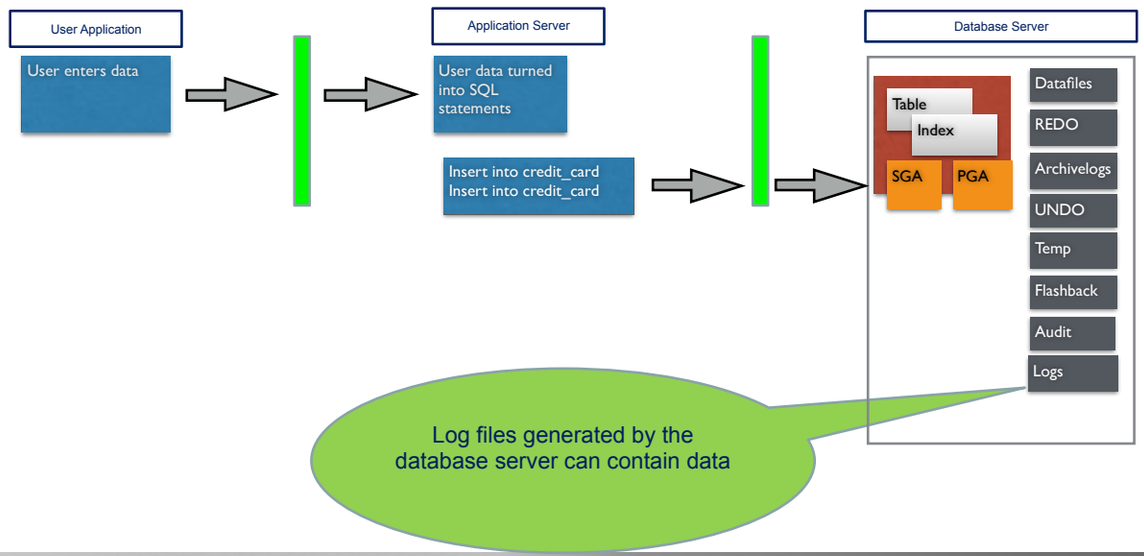
Data flow



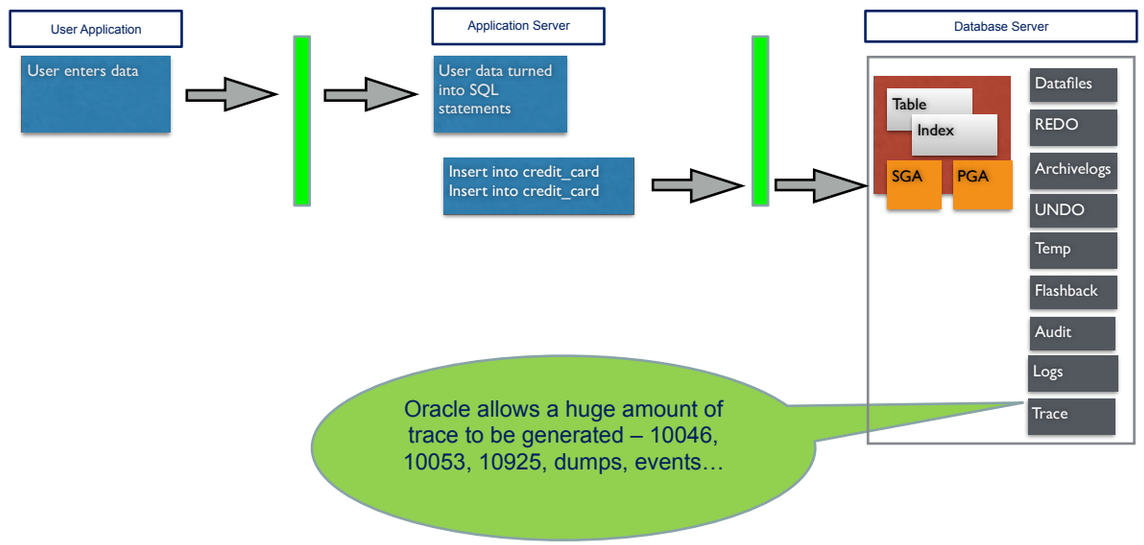
Data flow



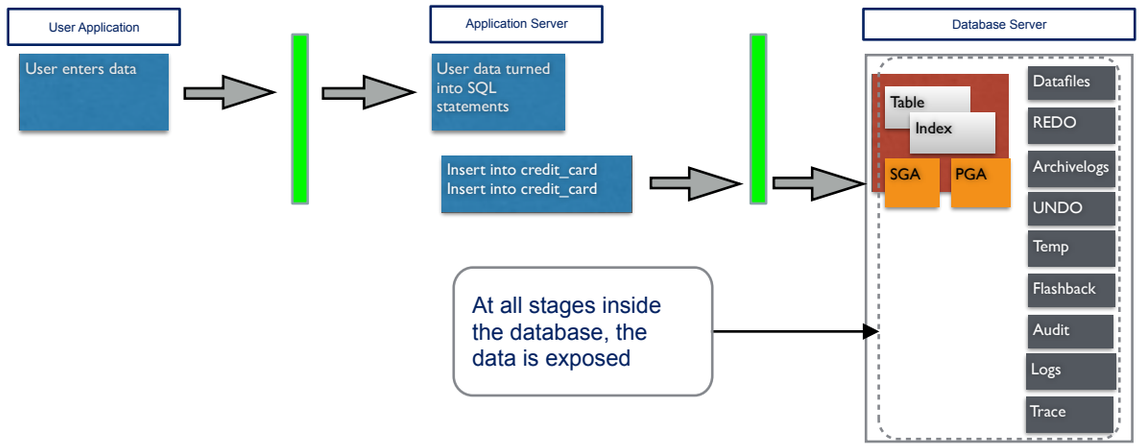
Data flow



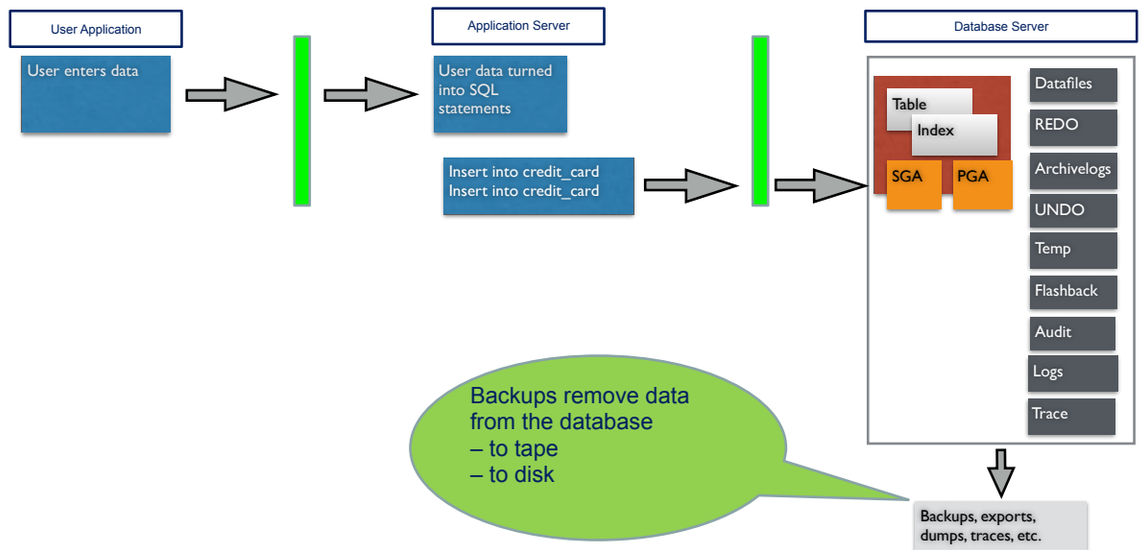
Data flow



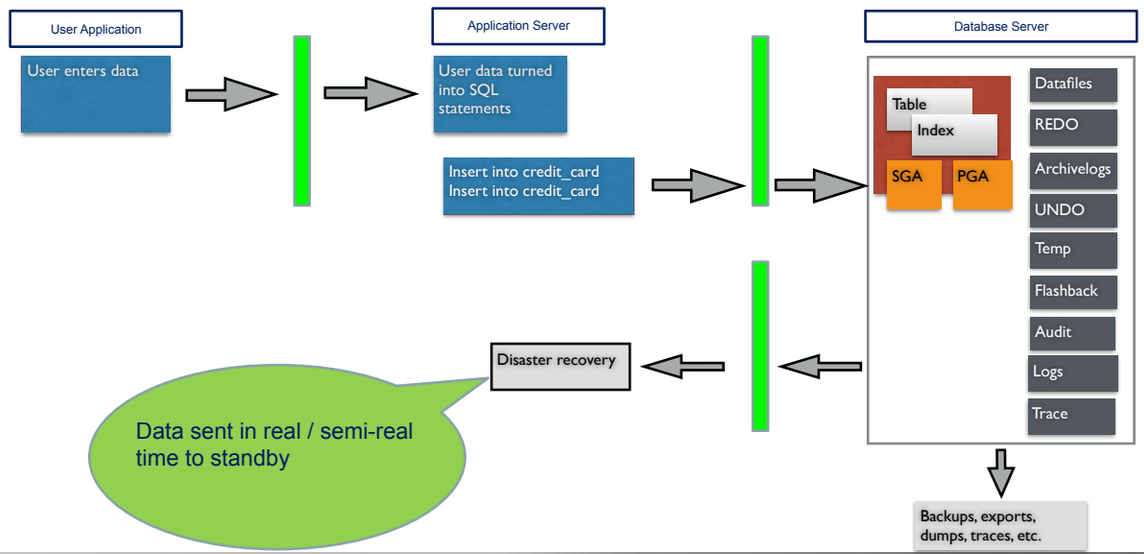
Data flow



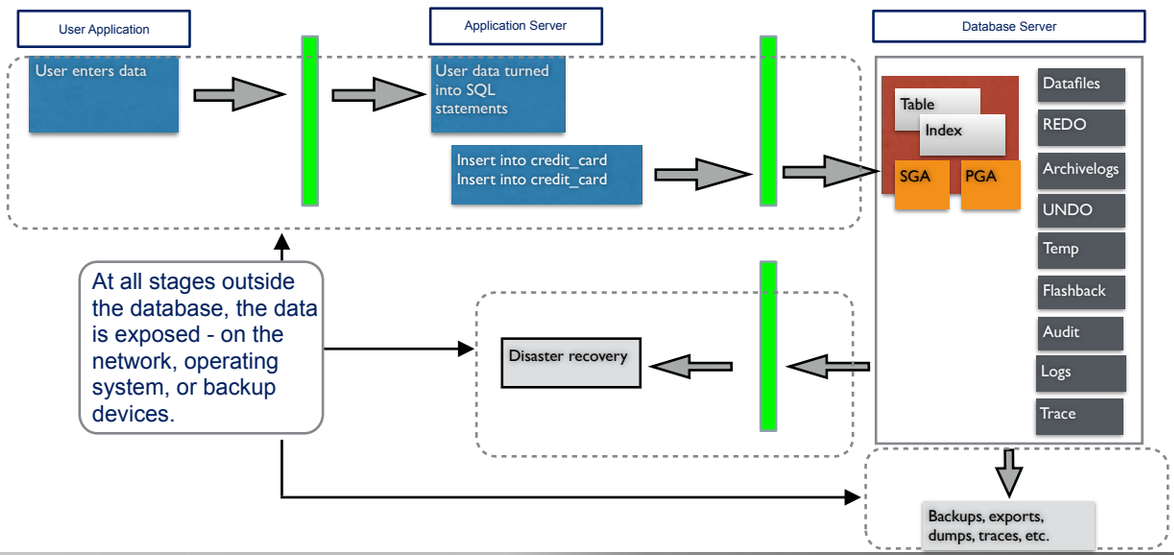
Data flow



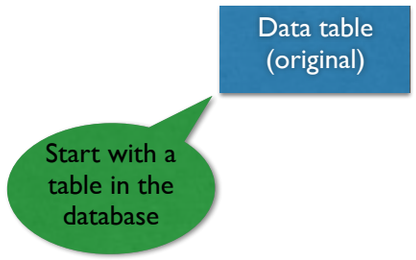
Data flow

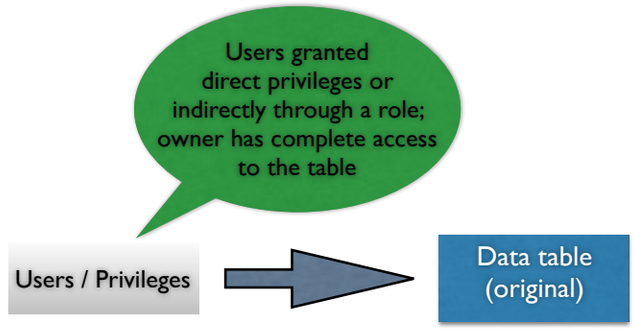


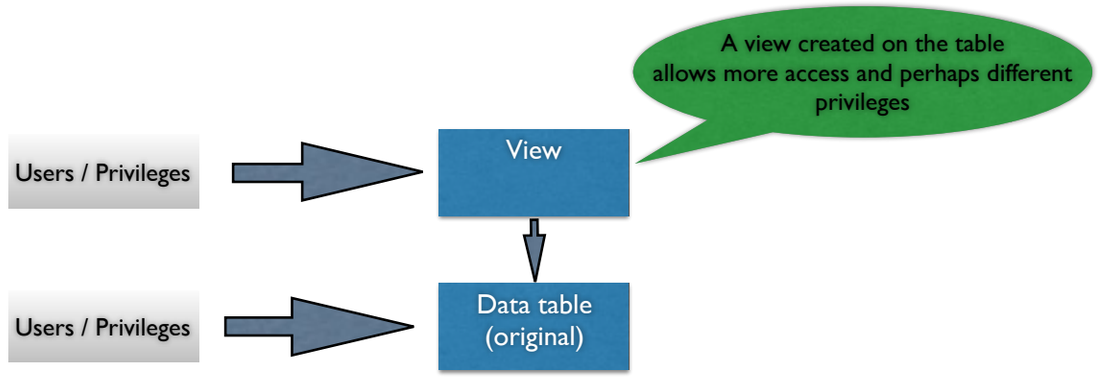
Data flow

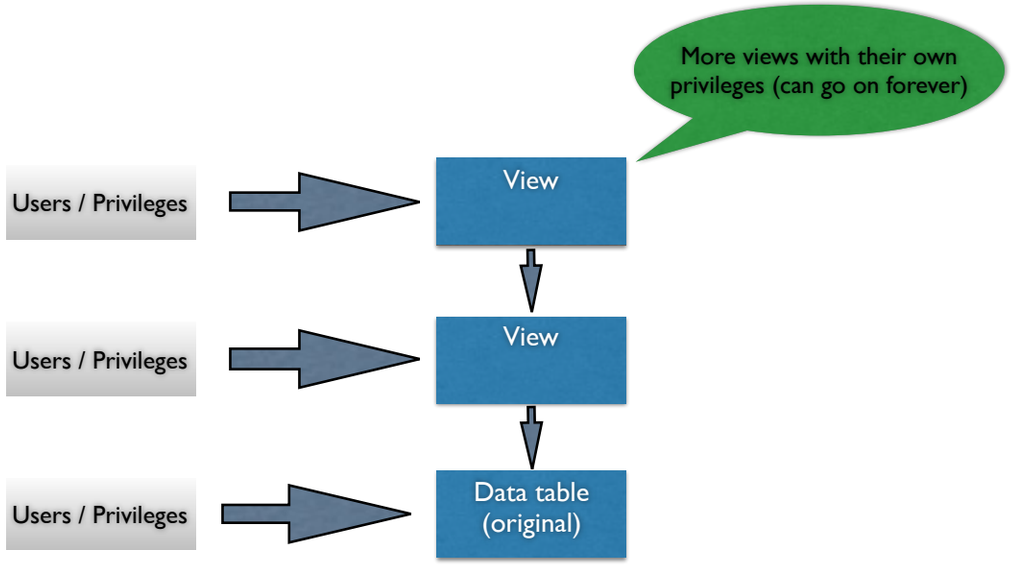


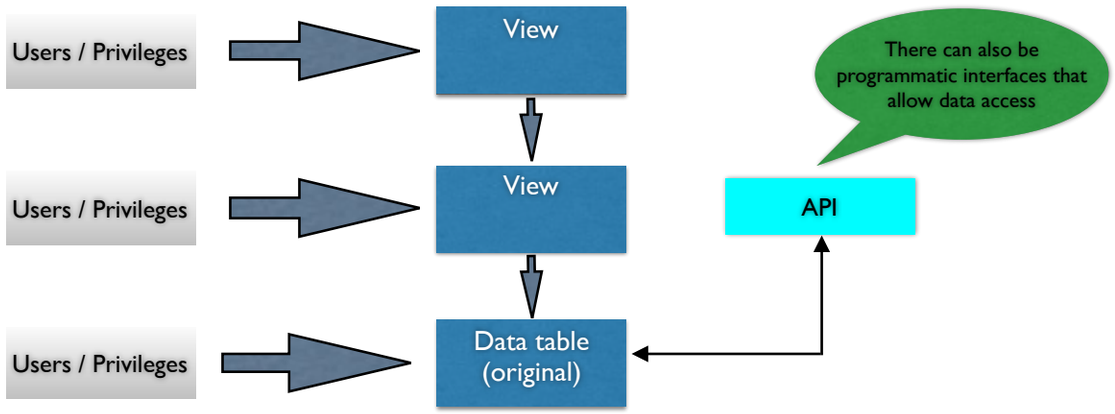
Data access model

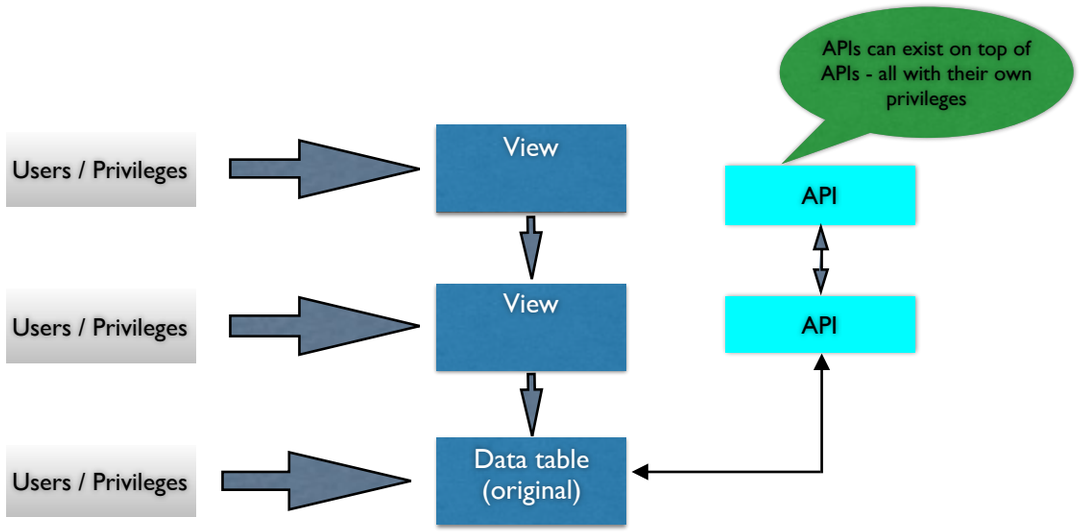


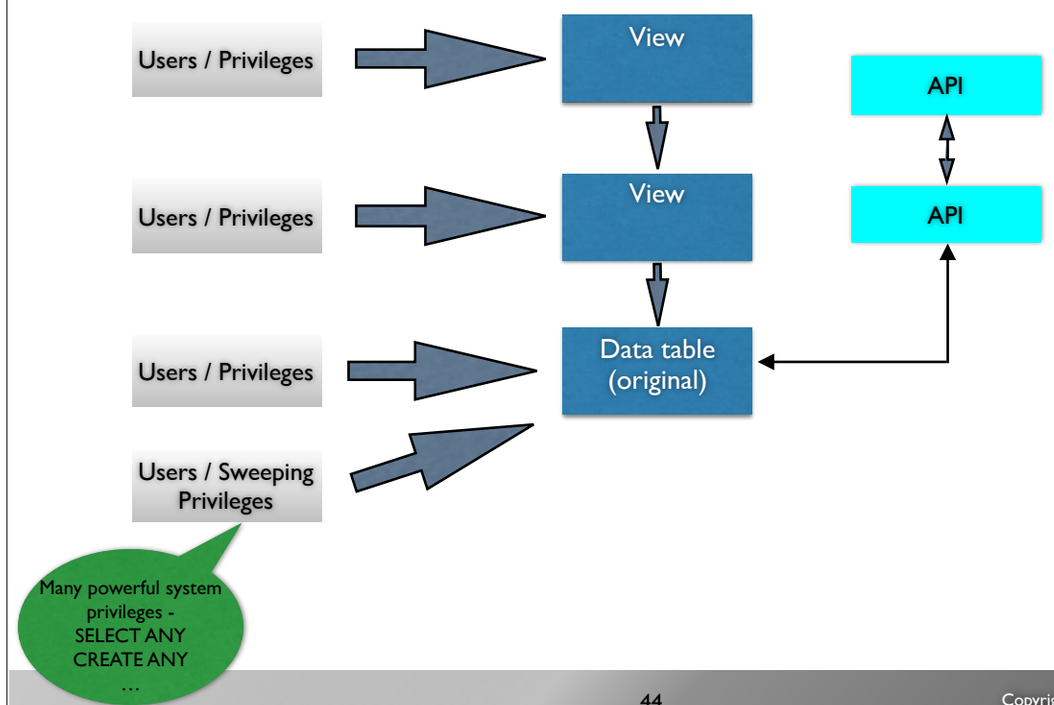


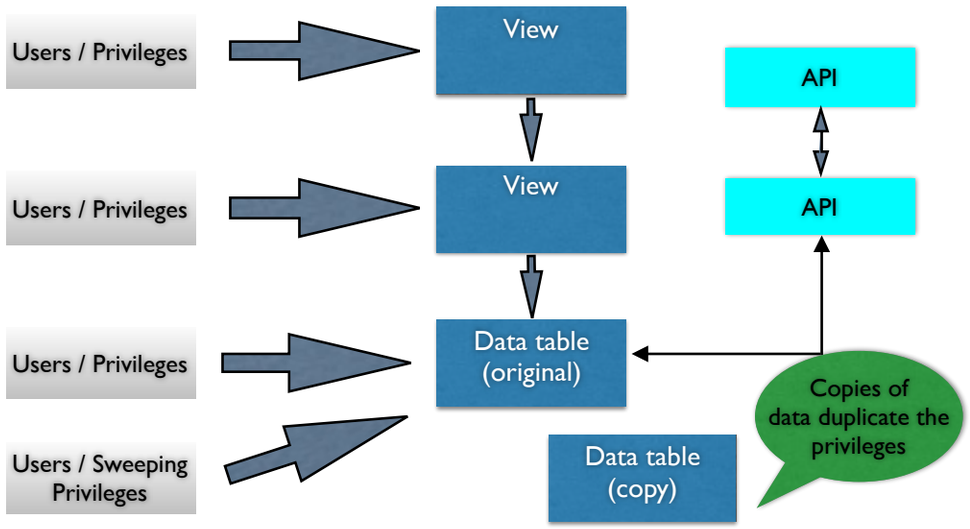


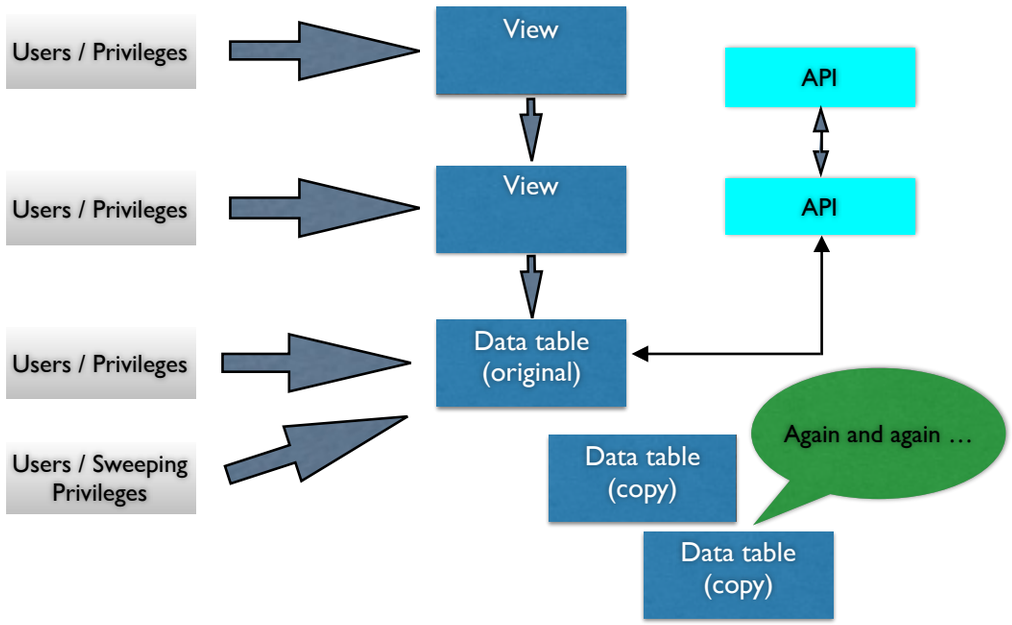


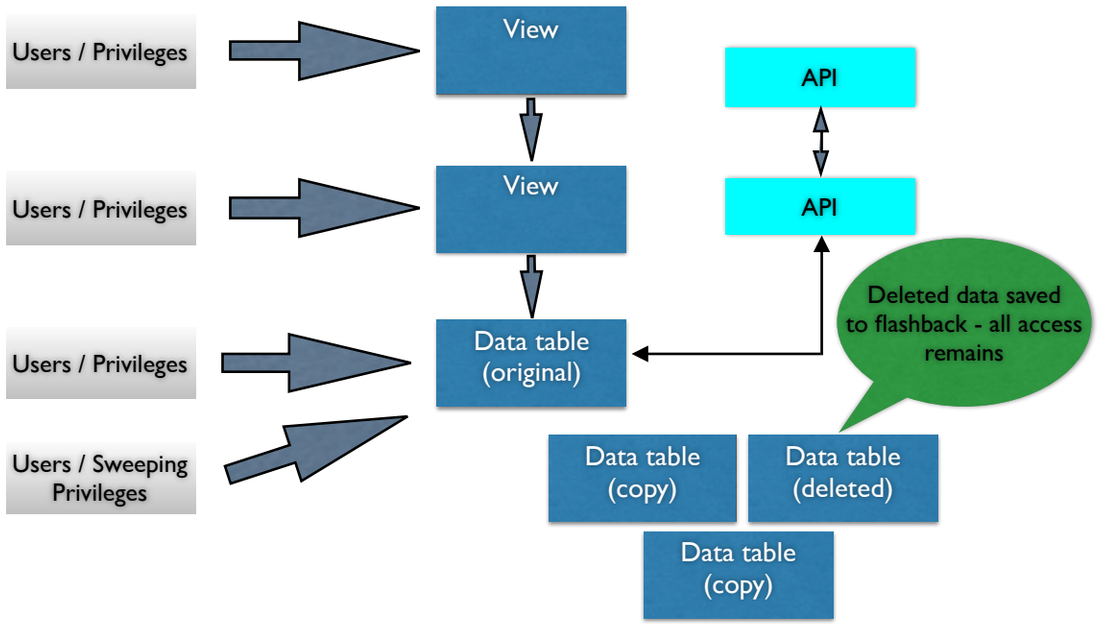












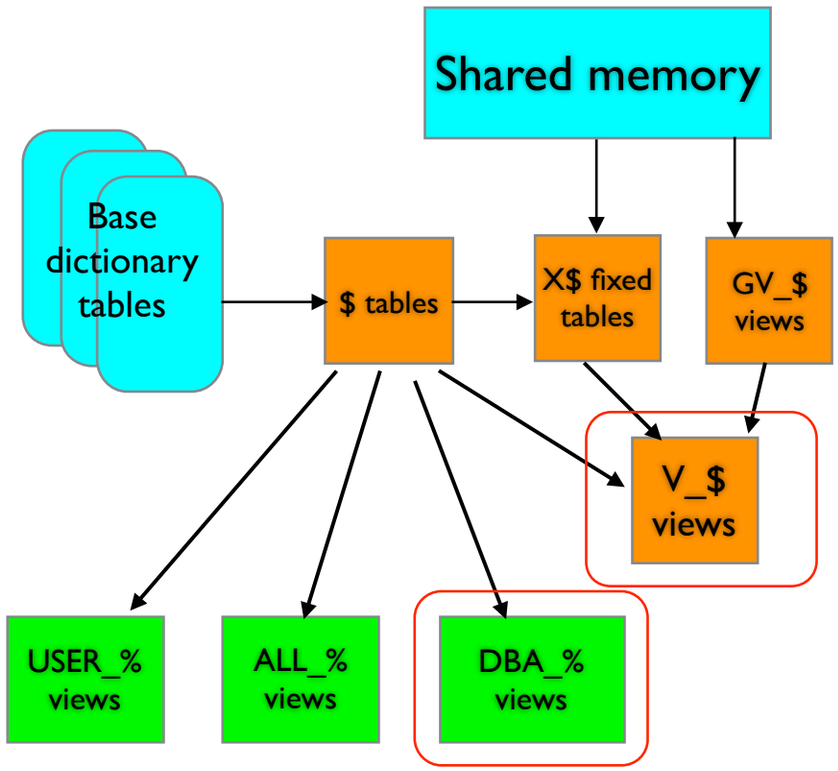
The Oracle data dictionary

Data dictionary

- Everything we need to discover is within the data dictionary
- Where is the meta data stored
- How is the meta data exposed
- The DBA_% views provide this information

Data dictionary composition

- Built in layers
- Physical data
  - Tables that expose "C" language data structures
    - X$ tables (usually)
- Views built on the physical model
  - DBA_%
  - ALL_%
  - USER_%
- Dynamic data mapping
  - V_$%
  - GV_$% (RAC)



Source code

- Code stored in the database
  - PL/SQL
  - Java (if the JVM is installed)
- Dictionary sources
  - SYS.SOURCE$, DBA_SOURCE, ALL_SOURCE, USER_SOURCE
  - SYS.VIEW$, DBA_VIEWS, ALL_VIEWS, USER_VIEWS
  - SYS.TRIGGER$, DBA_TRIGGERS, ALL_TRIGGERS, USER_TRIGGERS
  - DBA_JAVA_CLASSES, etc.

Components of an Oracle database audit

- Many points to audit
  - Operating system
  - Networking
  - Users
  - Roles
  - System privileges

PUBLIC

What is it?

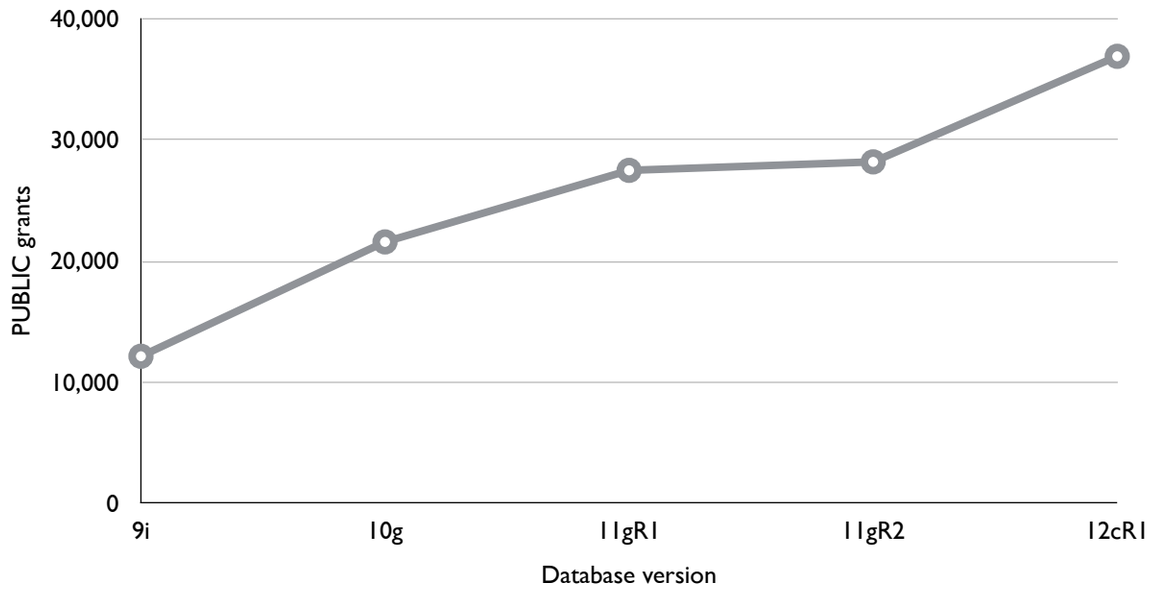
- A role that every DB user assumes
- Anything granted to PUBLIC is granted to all users

PUBLIC access growth

- Access to objects by the PUBLIC role gets bigger
- 9iR2 – 12.132
- 10gR2 – 21,530 **77.4% increase over 9iR2**
- 11gR1 – 27,461 **27.5% increase over 10gR2**
- 11gR2 – 28,160 **1% increase over 11gR1**
- 12cR1 - 36,866 **24% increase over 11gR2**

Every account in the database is a member of the PUBLIC role

PUBLIC growth



Importance

- Pay attention to anything granted to PUBLIC
  - Object access (especially application objects)
  - System privileges
  - Roles (especially application roles!)

Account auditing

Key dictionary objects

- SYS.USER$
  - Restricted access
- DBA_USERS

SYS.USER$

```
SQL> desc user$
 Name                                      Null?    Type
 ----------------------------------------- -------- ----------------------
 USER#                                     NOT NULL NUMBER
 NAME                                      NOT NULL VARCHAR2(30)
 TYPE#                                     NOT NULL NUMBER
 PASSWORD                                           VARCHAR2(30)
 DATATS#                                   NOT NULL NUMBER
 TEMPTS#                                   NOT NULL NUMBER
 CTIME                                     NOT NULL DATE
 PTIME                                              DATE
 EXPTIME                                            DATE
 LTIME                                              DATE
 RESOURCE$                                 NOT NULL NUMBER
 AUDIT$                                             VARCHAR2(38)
 DEFROLE                                   NOT NULL NUMBER
 DEFGRP#                                            NUMBER
 DEFGRP_SEQ#                                        NUMBER
 ASTATUS                                   NOT NULL NUMBER
 LCOUNT                                    NOT NULL NUMBER
 DEFSCHCLASS                                        VARCHAR2(30)
 EXT_USERNAME                                       VARCHAR2(4000)
 SPARE1                                             NUMBER
 SPARE2                                             NUMBER
 SPARE3                                             NUMBER
 SPARE4                                             VARCHAR2(1000)
 SPARE5                                             VARCHAR2(1000)
 SPARE6                                             DATE
```

Not documented by Oracle.

Base dictionary table for many dictionary views - DBA_USERS, ALL_USERS, etc. Also used by streams and log miner functionality.

Created in $ORACLE_HOME/rdbms/admin/dcore.bsq when database instance created.

```
create table user$                                          /* user table */
( user#         number not null,                   /* user identifier number */
  name          varchar2("M_IDEN") not null,                /* name of user */
               /* 0 = role, 1 = user, 2 = adjunct schema, 3 = schema synonym */
  type#         number not null,
  password      varchar2("M_IDEN"),                    /* encrypted password */
  datats#       number not null, /* default tablespace for permanent objects */
  tempts#       number not null,  /* default tablespace for temporary tables */
  ctime         date not null,                /* user account creation time */
  ptime         date,                              /* password change time */
  exptime       date,                      /* actual password expiration time */
  ltime         date,                          /* time when account is locked */
  resource$     number not null,                     /* resource profile# */
  audit$        varchar2("S_OPFL"),                  /* user audit options */
  defrole       number not null,                /* default role indicator: */
               /* 0 = no roles, 1 = all roles granted, 2 = roles in defrole$ */
  defgrp#       number,                              /* default undo group */
  defgrp_seq#   number,               /* global sequence number for  the grp *
  spare         varchar2("M_IDEN"),                  /* reserved for future */
  astatus       number default 0 not null,          /* status of the account */
                /* 0x00 =       0 = Open                                     */
                /* 0x01 =       1 = Locked                                   */
                /* 0x02 =       2 = Expired                                  */
                /* 0x03 =       3 = Locked and Expired                       */
```

DBA_USERS

```
SQL> desc dba_users
 Name                                      Null?    Type
 ----------------------------------------- -------- ----------------------------
 USERNAME                                  NOT NULL VARCHAR2(30)
 USER_ID                                   NOT NULL NUMBER
 PASSWORD                                           VARCHAR2(30)
 ACCOUNT_STATUS                            NOT NULL VARCHAR2(32)
 LOCK_DATE                                          DATE
 EXPIRY_DATE                                        DATE
 DEFAULT_TABLESPACE                        NOT NULL VARCHAR2(30)
 TEMPORARY_TABLESPACE                      NOT NULL VARCHAR2(30)
 CREATED                                   NOT NULL DATE
 PROFILE                                   NOT NULL VARCHAR2(30)
 INITIAL_RSRC_CONSUMER_GROUP                        VARCHAR2(30)
 EXTERNAL_NAME                                      VARCHAR2(4000)
 PASSWORD_VERSIONS                                  VARCHAR2(8)
 EDITIONS_ENABLED                                   VARCHAR2(1)
 AUTHENTICATION_TYPE                                VARCHAR2(8)
```

No longer displayed

Describes all users in the database

Built from SYS.USER$ and other base dictionary tables.

Created from $ORACLE_HOME/rdbms/admin/cdenv.sql when database instance is created.

http://docs.oracle.com/cd/E11882_01/server.112/e40402/statviews_5081.htm#REFRN23302

```
create or replace view DBA_USERS
    (USERNAME, USER_ID, PASSWORD, ACCOUNT_STATUS, LOCK_DATE, EXPIRY_DATE,
        DEFAULT_TABLESPACE, TEMPORARY_TABLESPACE, CREATED, PROFILE,
        INITIAL_RSRC_CONSUMER_GROUP,EXTERNAL_NAME,PASSWORD_VERSIONS,
        EDITIONS_ENABLED, AUTHENTICATION_TYPE)
as
select u.name, u.user#,
       decode(u.password, 'GLOBAL', u.password,
                          'EXTERNAL', u.password,
                          NULL),
       m.status,
       decode(u.astatus, 4, u.ltime,
                         5, u.ltime,
                         6, u.ltime,
                         8, u.ltime,
                         9, u.ltime,
                         10, u.ltime, to_date(NULL)),
       decode(u.astatus,
              1, u.exptime,
              2, u.exptime,
              5, u.exptime,
```

Putting it together

DATABASE_NAME	DATABASE_CREATED	DATABASE_AGE	ACCOUNT_NAME	ACCOUNT_TYPE	STATUS	ACCOUNT_AGE
ORCL	30-OCT-09	1727	SYS	USER ACCOUNT	OPEN	1805
ORCL	30-OCT-09	1727	PUBLIC	ROLE	OPEN	1805
ORCL	30-OCT-09	1727	CONNECT	ROLE	OPEN	1805
ORCL	30-OCT-09	1727	RESOURCE	ROLE	OPEN	1805
ORCL	30-OCT-09	1727	DBA	ROLE	OPEN	1805
ORCL	30-OCT-09	1727	SYSTEM	USER ACCOUNT	OPEN	1805
ORCL	30-OCT-09	1727	SELECT_CATALOG_ROLE	ROLE	OPEN	1805
ORCL	30-OCT-09	1727	EXECUTE_CATALOG_ROLE	ROLE	OPEN	1805
ORCL	30-OCT-09	1727	DELETE_CATALOG_ROLE	ROLE	OPEN	1805

ACCOUNT_NAME	STATUS	ACCOUNT_AGE	EXT_USERNAME	CTIME	PTIME	PASSWORD_AGE	EXPTIME	LTIME	PASSWORD	SPARE4
SYS	OPEN	1804 (null)	13-AUG-09	18-APR-10		1556	13-AUG-09	13-AUG-09	8A8F025737A9097A	S:A6B78508F3C3B8F44528C50F4CC02509C0A16A043151ABC8C2997CA10C42
PUBLIC	OPEN	1804 (null)	13-AUG-09	(null)		-1	(null)	(null)	(null)	(null)
CONNECT	OPEN	1804 (null)	13-AUG-09	(null)		-1	(null)	(null)	(null)	(null)
RESOURCE	OPEN	1804 (null)	13-AUG-09	(null)		-1	(null)	(null)	(null)	(null)
DBA	OPEN	1804 (null)	13-AUG-09	(null)		-1	(null)	(null)	(null)	(null)
SYSTEM	OPEN	1804 (null)	13-AUG-09	18-APR-10		1556	13-AUG-09	13-AUG-09	2D594E86F93B17A1	S:1ED1C777D0475A1C3086E0B0930B88BC350A4060CA7193E546377EC50630E
SELECT_CATALOG_ROLE	OPEN	1804 (null)	13-AUG-09	(null)		-1	(null)	(null)	(null)	(null)
EXECUTE_CATALOG_ROLE	OPEN	1804 (null)	13-AUG-09	(null)		-1	(null)	(null)	(null)	(null)
DELETE_CATALOG_ROLE	OPEN	1804 (null)	13-AUG-09	(null)		-1	(null)	(null)	(null)	(null)

PASSWORD	SPARE4	PASSWORD_VERSIONS	LCOUNT
8A8F025737A9097A	S:A6B78508F3C3B8F44528C50F4CC02509C0A16A043151ABC8C2997CA10C42	10G 11G	0
2D594E86F93B17A1	S:1ED1C777D0475A1C3086E0B0930B88BC350A4060CA7193E546377EC50630E	10G 11G	7
4A3BA55E08595C81	S:21C0173B851C524225B387E140110CEDEEFB377E1623F091A374CFB6B60E	10G 11G	0
CE4A36B8E06CA59C	S:99DCA3DC2E10FED6CA144418DEADFCCF53C54CA80330E8E2310067124065	10G 11G	0
5A2E020A9157958C	S:93330350193CFCFCA3C64AFAE79744CCAF0770BB45103C094B48CBC902E8	10G 11G	0
FFF45BB200C327EC	S:4A3747B7F3ACD7C4C74E0197F47CB62F297BA07A306A040202EBCEAA5CAF	10G 11G	5
519D032B7EE7F03A	S:17FC2ABA29BEB01C855004605010BACD00B1103030F7A01B0584FF3F8F57	10G 11G	0
7C9BA362F8314299	S:26AA13E8F474C24ABFDC1CF27E13208CABDF04127054223C3B2B841620D04	10G 11G	0
33C758ABE3880EE5	S:9153F5CF82106388CF01B588A02110FDA287A714489837CB5CD93CA78388	10G 11G	0

See file account_status.sql in the scripts section.

Built in database accounts

- There are many built in accounts in Oracle
  - Administrative - 22
  - Non-administrative - 9
- Used to implement database features and options
- Very powerful (usually)
- Best practice - start with nothing installed
  - Only install options if a documented need

Predefined administrative accounts: http://docs.oracle.com/cd/E11882_01/server.112/e10575/tdpsg_user_accounts.htm#TDPSG20030

Predefined non-administrative accounts: http://docs.oracle.com/cd/E11882_01/server.112/e10575/tdpsg_user_accounts.htm#TDPSG20302

Built in accounts

ACCOUNT_NAME	ACCOUNT_TYPE	ACCOUNT_STATUS
SYS	USER_ACCOUNT	OPEN
SYSTEM	USER_ACCOUNT	OPEN
OUTLN	USER_ACCOUNT	EXPIRED & LOCKED
DIP	USER_ACCOUNT	EXPIRED & LOCKED
ORACLE_OCM	USER_ACCOUNT	EXPIRED & LOCKED
DBSNMP	USER_ACCOUNT	OPEN
APPQOSSYS	USER_ACCOUNT	EXPIRED & LOCKED
WMSYS	USER_ACCOUNT	EXPIRED & LOCKED
EXFSYS	USER_ACCOUNT	EXPIRED & LOCKED
CTXSYS	USER_ACCOUNT	EXPIRED & LOCKED
XDB	USER_ACCOUNT	LOCKED
ANONYMOUS	USER_ACCOUNT	EXPIRED
ORDSYS	USER_ACCOUNT	EXPIRED & LOCKED
ORDDATA	USER_ACCOUNT	EXPIRED & LOCKED
ORDPLUGINS	USER_ACCOUNT	EXPIRED & LOCKED
SI_INFORMTN_SCHEMA	USER_ACCOUNT	EXPIRED & LOCKED
MDSYS	USER_ACCOUNT	EXPIRED & LOCKED
OLAPSYS	USER_ACCOUNT	EXPIRED & LOCKED
MDDATA	USER_ACCOUNT	EXPIRED & LOCKED
SPATIAL_WFS_ADMIN_USR	USER_ACCOUNT	EXPIRED & LOCKED
SPATIAL_CSW_ADMIN_USR	USER_ACCOUNT	EXPIRED & LOCKED
SYSMAN	USER_ACCOUNT	OPEN
MGMT_VIEW	USER_ACCOUNT	OPEN
OWBSYS	USER_ACCOUNT	EXPIRED & LOCKED
OWBSYS_AUDIT	USER_ACCOUNT	EXPIRED & LOCKED
XFILES	USER_ACCOUNT	OPEN
XDBPM	USER_ACCOUNT	LOCKED
XDBMETADATA	USER_ACCOUNT	LOCKED

Demo accounts

- Supplied as learning tools
  - Not appropriate in production systems

ACCOUNT_NAME	ACCOUNT_TYPE	ACCOUNT_STATUS
SCOTT	USER ACCOUNT	OPEN
IX	USER ACCOUNT	EXPIRED & LOCKED
SH	USER ACCOUNT	EXPIRED & LOCKED
PM	USER ACCOUNT	EXPIRED & LOCKED
BI	USER ACCOUNT	EXPIRED & LOCKED
DEMO	USER ACCOUNT	OPEN
HR1	USER ACCOUNT	OPEN
OE1	USER ACCOUNT	OPEN
OE	USER ACCOUNT	OPEN
HR	USER ACCOUNT	OPEN

Sometimes, the name gives it away

Duplicates

Valid account in eBusiness Suite

Demo scripts fro SCOTT located in:
$ORACLE_HOME/rdbms/admin/scott.sql
$ORACLE_HOME/sqlplus/demobld.sql
$ORACLE_HOME/rdbms/admin/utlsampl.sql

Demo scripts for HR, SH, PM, BI, IX, OE (and OC) located in:
$ORACLE_HOME/demo/schema

http://docs.oracle.com/cd/E11882_01/server.112/e10831/installation.htm#COMSC00002

Note: IX was renamed from QS in Oracle 10g.

Identify application schema accounts

- Own database objects
- Not human accounts

OWNER	OBJECT_TYPE	COUNT(*)
DEMO	INDEX	8
DEMO	LOB	1
DEMO	SEQUENCE	5
DEMO	TABLE	7
DEMO	TRIGGER	7

OWNER	OBJECT_TYPE	COUNT(*)
HR	INDEX	19
HR	PROCEDURE	2
HR	SEQUENCE	3
HR	TABLE	7
HR	TRIGGER	2
HR	VIEW	1

OWNER	OBJECT_TYPE	COUNT(*)
ORABLOG	FUNCTION	10
ORABLOG	INDEX	23
ORABLOG	LOB	4
ORABLOG	PACKAGE	1
ORABLOG	PACKAGE BODY	1
ORABLOG	SEQUENCE	10
ORABLOG	TABLE	11
ORABLOG	TRIGGER	11
ORABLOG	VIEW	1

Application schema accounts

```
find_all_privs: Release 1.0.7.0.0 - Production on Thu Oct 09 04:36:46 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF USER TO CHECK                [ORCL]: orablog

User => ORABLOG has been granted the following privileges
================================================================================
        ROLE => CONNECT which contains =>
                SYS PRIV => CREATE SESSION grantable => NO
        ROLE => RESOURCE which contains =>
                SYS PRIV => CREATE CLUSTER grantable => NO
                SYS PRIV => CREATE INDEXTYPE grantable => NO
                SYS PRIV => CREATE OPERATOR grantable => NO
                SYS PRIV => CREATE PROCEDURE grantable => NO
                SYS PRIV => CREATE SEQUENCE grantable => NO
                SYS PRIV => CREATE TABLE grantable => NO
                SYS PRIV => CREATE TRIGGER grantable => NO
                SYS PRIV => CREATE TYPE grantable => NO
        SYS PRIV => CREATE PUBLIC SYNONYM grantable => NO
        SYS PRIV => UNLIMITED TABLESPACE grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_CRYPTO grantable => NO

PL/SQL procedure successfully completed.
```

Built in accounts are also schema owners

- Built in accounts provide database functionality
  - Implemented with PL/SQL and/or Java code (and other objects)

Examples of DB functionality:
Context indexing
Geospatial
XML Database

Built-in account object ownership

SYS

OWNER	OBJECT_TYPE	COUNT(*)
SYS	CLUSTER	10
SYS	CONSUMER G...	25
SYS	CONTEXT	7
SYS	DESTINATION	2
SYS	DIRECTORY	11
SYS	EDITION	2
SYS	EVALUATION...	10
SYS	FUNCTION	102
SYS	INDEX	1036

Application express

OWNER	OBJECT_TYPE	COUNT(*)
APEX_040000	FUNCTION	12
APEX_040000	INDEX	1177
APEX_040000	JOB	4
APEX_040000	LOB	185
APEX_040000	PACKAGE	234
APEX_040000	PACKAGE BODY	227
APEX_040000	PROCEDURE	19
APEX_040000	SEQUENCE	3
APEX_040000	SYNONYM	54
APEX_040000	TABLE	420
APEX_040000	TRIGGER	439
APEX_040000	TYPE	4
APEX_040000	VIEW	175

XML database

OWNER	OBJECT_TYPE	COUNT(*)
XDB	FUNCTION	7
XDB	INDEX	129
XDB	INDEXTYPE	2
XDB	LIBRARY	17
XDB	LOB	342
XDB	OPERATOR	7
XDB	PACKAGE	43
XDB	PACKAGE BODY	42
XDB	PROCEDURE	4
XDB	SEQUENCE	5
XDB	TABLE	80
XDB	TRIGGER	28
XDB	TYPE	98
XDB	TYPE BODY	5
XDB	VIEW	6
XDB	XML SCHEMA	59

```
find all privs: Release 1.0.7.0.0 - Production on Thu Oct 09 04:32:03 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF USER TO CHECK                [ORCL]: apex_040000

User -> APEX_040000 has been granted the following privileges
=============================================================
        ROLE -> CONNECT which contains ->
                SYS PRIV => CREATE SESSION grantable => NO
        ROLE -> RESOURCE which contains ->
                SYS PRIV => CREATE CLUSTER grantable => NO
                SYS PRIV => CREATE INDEXTYPE grantable => NO
                SYS PRIV => CREATE OPERATOR grantable => NO
                SYS PRIV => CREATE PROCEDURE grantable => NO
                SYS PRIV => CREATE SEQUENCE grantable => NO
                SYS PRIV => CREATE TABLE grantable => NO
                SYS PRIV => CREATE TRIGGER grantable => NO
                SYS PRIV => CREATE TYPE grantable => NO
        SYS PRIV => ALTER DATABASE grantable => NO
        SYS PRIV => ALTER SESSION grantable => NO
        SYS PRIV => ALTER USER grantable => NO
        SYS PRIV => CREATE ANY CONTEXT grantable => YES
        SYS PRIV => CREATE CLUSTER grantable => YES
        SYS PRIV => CREATE DIMENSION grantable => YES
        SYS PRIV => CREATE INDEXTYPE grantable => YES
        SYS PRIV => CREATE JOB grantable => YES
        SYS PRIV => CREATE MATERIALIZED VIEW grantable => YES
        SYS PRIV => CREATE OPERATOR grantable => YES
        SYS PRIV => CREATE PROCEDURE grantable => YES
        SYS PRIV => CREATE PUBLIC SYNONYM grantable => NO
        SYS PRIV => CREATE ROLE grantable => NO
        SYS PRIV => CREATE SEQUENCE grantable => YES
        SYS PRIV => CREATE SESSION grantable => YES
        SYS PRIV => CREATE SYNONYM grantable => YES
        SYS PRIV => CREATE TABLE grantable => YES
        SYS PRIV => CREATE TABLESPACE grantable => NO
        SYS PRIV => CREATE TRIGGER grantable => YES
        SYS PRIV => CREATE TYPE grantable => YES
        SYS PRIV => CREATE USER grantable => NO
        SYS PRIV => CREATE VIEW grantable => YES
        SYS PRIV => DROP PUBLIC SYNONYM grantable => NO
        SYS PRIV => DROP TABLESPACE grantable => NO
        SYS PRIV => DROP USER grantable => NO
        SYS PRIV => UNLIMITED TABLESPACE grantable => YES
        TABLE PRIV => ALTER object => FLOWS_FILES.WWV_FLOW_FILE_OBJECTS$ grantable => YES
        TABLE PRIV => DELETE object => FLOWS_FILES.WWV_FLOW_FILE_OBJECTS$ grantable => YES
        TABLE PRIV => EXECUTE object => SYS.DBMS_CRYPTO grantable => NO
```

Use the script find_all_privs.sql

Identify DBAs

- Built in accounts are DBA accounts
  - SYS, SYSTEM
- Who are the other DBAs?

SYS and SYSTEM

- Internal administrative accounts
- Created when the database is created
- Not for casual use

These accounts are “owned” by Oracle Corp. Use should be restricted and documented.

Created in $ORACLE_HOME/rdbms/admin/dsec.bsq

https://asktom.oracle.com/pls/asktom/f?p=100:11:0%3a%3a%3a%3aP11_QUESTION_ID:2659418700346202574

SYS

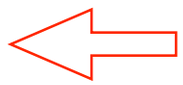
- Administrative account
- Owns the internal data dictionary
  - Analogous to the root account on UNIX
- Can bypass all controls; modify audit trail, etc.

SYSTEM

- Can perform all administrative functions **EXCEPT**
  - Backup and recovery
  - Database upgrade

Finding accounts with the DBA role

```
SQL> @who_has_role.sql



who_has_priv: Release 1.0.3.0.0 - Production on Fri Sep 26 06:00:13 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

ROLE TO CHECK                          [DBA]: dba

Investigating Role => DBA (PWD = NO) which is granted to =>
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
        User => SYS (ADM = YES)
        User => PHPDEMO (ADM = NO)
        User => SYSTEM (ADM = YES)

PL/SQL procedure successfully completed.

For updates please visit http://www.petefinnigan.com/tools.htm
```



Identify the need for any account to have the DBA role!

Power users

- Application and system support (sometimes developers)
- Usually have sweeping system and object privileges, and powerful built-in roles and application roles
  - '%ANY%'
  - SELECT ANY TABLE
  - SELECT_CATALOG_ROLE
  - Library privileges
  - Internet package access
  - etc.
- Operating system access
  - OS group access
- Need system documentation
  - System security plan
  - System and data classification

Identify power users

ACCOUNT_NAME	ACCOUNT_TYPE	ACCOUNT_STATUS	EXT_USERNAME	ACCOUNT_AGE	CTIME	PASSWORD_AGE	PTIME	EXPTIME	LTIME
JOHN_DEV	USER ACCOUNT	OPEN	(null)	1095	09-OCT-11	1095	09-OCT-11	(null)	(null)
JACK_DEV	USER ACCOUNT	OPEN	(null)	1095	09-OCT-11	1095	09-OCT-11	(null)	(null)
AUDITOR	USER ACCOUNT	OPEN	(null)	1092	12-OCT-11	155	07-MAY-14	(null)	(null)

- Identify all access for these accounts

```
find_all_privs: Release 1.0.7.0.0 - Production on Thu Oct 09 04:38:51 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF USER TO CHECK                 [ORCL]: jack_dev

User => JACK_DEV has been granted the following privileges
================================================================================
        ROLE => CONNECT which contains =>
                SYS PRIV => CREATE SESSION grantable => NO
        ROLE => RESOURCE which contains =>
                SYS PRIV => CREATE CLUSTER grantable => NO
                SYS PRIV => CREATE INDEXTYPE grantable => NO
                SYS PRIV => CREATE OPERATOR grantable => NO
                SYS PRIV => CREATE PROCEDURE grantable => NO
                SYS PRIV => CREATE SEQUENCE grantable => NO
                SYS PRIV => CREATE TABLE grantable => NO
                SYS PRIV => CREATE TRIGGER grantable => NO
                SYS PRIV => CREATE TYPE grantable => NO
        ROLE => SELECT_CATALOG_ROLE which contains =>
                ROLE => HS_ADMIN_SELECT_ROLE which contains =>
                        TABLE PRIV => SELECT object => SYS.HS_ALL_CAPS grantable => NO
                        TABLE PRIV => SELECT object => SYS.HS_ALL_DD grantable => NO
                        TABLE PRIV => SELECT object => SYS.HS_ALL_INITS grantable => NO
                        TABLE PRIV => SELECT object => SYS.HS_BASE_CAPS grantable => NO
                        TABLE PRIV => SELECT object => SYS.HS_BASE_DD grantable => NO
                        TABLE PRIV => SELECT object => SYS.HS_CLASS_CAPS grantable => NO
                        TABLE PRIV => SELECT object => SYS.HS_CLASS_DD grantable => NO
                        TABLE PRIV => SELECT object => SYS.HS_CLASS_INIT grantable => NO
                        TABLE PRIV => SELECT object => SYS.HS_FDS_CLASS grantable => NO
                        TABLE PRIV => SELECT object => SYS.HS_FDS_CLASS_DATE grantable => NO
                        TABLE PRIV => SELECT object => SYS.HS_FDS_INST grantable => NO
                        TABLE PRIV => SELECT object => SYS.HS_INST_CAPS grantable => NO
                        TABLE PRIV => SELECT object => SYS.HS_INST_DD grantable => NO
                        TABLE PRIV => SELECT object => SYS.HS_INST_INIT grantable => NO
                TABLE PRIV => EXECUTE object => SYS.DBMS_RCVMAN grantable => NO
                TABLE PRIV => EXECUTE object => SYS.KU$_MONITOR_T grantable => NO
                TABLE PRIV => EXECUTE object => SYS.LOGSTDBY$TABF grantable => NO
```

```
TABLE PRIV => SELECT object => SYS._DBA_APPLY_OBJECT_CONSTRAINTS grantable => NO
TABLE PRIV => SELECT object => SYS._DBA_STREAMS_ACTIONS grantable => NO
TABLE PRIV => SELECT object => SYS._DBA_STREAMS_COMPONENT grantable => NO
TABLE PRIV => SELECT object => SYS._DBA_STREAMS_COMPONENT_EVENT grantable => NO
TABLE PRIV => SELECT object => SYS._DBA_STREAMS_COMPONENT_LINK grantable => NO
TABLE PRIV => SELECT object => SYS._DBA_STREAMS_COMPONENT_PROP grantable => NO
TABLE PRIV => SELECT object => SYS._DBA_STREAMS_COMPONENT_STAT grantable => NO
TABLE PRIV => SELECT object => SYS._DBA_STREAMS_FINDINGS grantable => NO
TABLE PRIV => SELECT object => SYS._DBA_STREAMS_RECOMMENDATIONS grantable => NO
TABLE PRIV => SELECT object => SYS._DBA_STREAMS_TP_COMPONENT_PROP grantable => NO
SYS PRIV => CREATE ANY INDEX grantable => NO
SYS PRIV => CREATE ANY VIEW grantable => NO
SYS PRIV => DEBUG ANY PROCEDURE grantable => NO
SYS PRIV => DEBUG CONNECT SESSION grantable => NO
SYS PRIV => EXECUTE ANY PROCEDURE grantable => NO
SYS PRIV => SELECT ANY DICTIONARY grantable => NO
SYS PRIV => SELECT ANY TABLE grantable => NO
SYS PRIV => UNLIMITED TABLESPACE grantable => NO

PL/SQL procedure successfully completed.
```

Remaining accounts

- Usually end user accounts
- Check privileges and all access
- Check this access against job descriptions, management certifications, etc.

Special accounts

_NEXT_USER	ROLE	OPEN
XS$NULL	USER ACCOUNT	EXPIRED & LOCKED

Both XS$NULL and _NEXT_USER are internal accounts.

1. _NEXT_USER is used when new accounts or roles are created to increment the SYS.USER$.USER# column. This account has no privileges and no one can authenticate as __NEXT_USER, nor can authentication credentials ever be assigned to _NEXT_USER.
2. XS$NULL is an account that represents the absence of a user in a session. It is created during installation of XML DB and is used by the lightweight session infrastructure for APEX, RAS and XDB and the name of this user is hard coded in those modules. Because XS$NULL is not a user, this account can only be accessed by the Oracle Database instance. XS$NULL has no privileges and no one can authenticate as XS$NULL, nor can authentication credentials ever be assigned to XS$NULL.

Default passwords

- Many built in accounts can have default passwords
- DBA_USERS_WITH_DEFPWD
  - SYS.USER$
  - SYS.DEFAULT_PWD$ - 84 known or common password hashes

Created in $ORACLE_HOME/rdbms/admin/catdef.sql

```
CREATE OR REPLACE VIEW SYS.DBA_USERS_WITH_DEFPWD (USERNAME) AS
  SELECT DISTINCT u.name
    FROM SYS.user$ u, SYS.default_pwd$ dp
   WHERE
     (u.type#  = 1
      AND bitand(u.astatus, 16) = 16
     ) OR
     (u.type#    = 1
     AND u.password = dp.pwd_verifier
     AND u.name     = dp.user_name
     AND dp.pv_type = 0);
```

SYS.DEFAULT_PWD$ created and populated in $ORACLE_HOME/rdbms/admin/c1101000.sql

```
Rem Create SYS.DEFAULT_PWD$

BEGIN
  EXECUTE IMMEDIATE 'CREATE TABLE SYS.DEFAULT_PWD$ (user_name varchar2(128),
                    pwd_verifier varchar2(512),pv_type NUMBER default 0)';
EXCEPTION
  WHEN OTHERS THEN
  IF SQLCODE IN ( -00955) THEN NULL; --ignore when table already exists
    DBMS_OUTPUT.PUT_LINE('TABLE SYS.DEFAULT_PWD$ ALREADY EXISTS');
  ELSE RAISE;
```

Password controls

Database profiles

- List all profiles and their password settings

```
SQL> desc dba_profiles
 Name                                      Null?    Type
 ----------------------------------------- -------- ----------------------------
 PROFILE                                   NOT NULL VARCHAR2(30)
 RESOURCE_NAME                             NOT NULL VARCHAR2(32)
 RESOURCE_TYPE                                      VARCHAR2(8)
 LIMIT                                              VARCHAR2(40)
```

- We are interested in the PASSWORD settings (resource_type = 'PASSWORD')

```
select distinct resource_name from dba_profiles where resource_type = 'PASSWORD';
```

Query Result

SQL | All Rows Fetched: 7 in 0.02 seconds

	RESOURCE_NAME
1	FAILED_LOGIN_ATTEMPTS
2	PASSWORD_REUSE_TIME
3	PASSWORD_VERIFY_FUNCTION
4	PASSWORD_LOCK_TIME
5	PASSWORD_REUSE_MAX
6	PASSWORD_GRACE_TIME
7	PASSWORD_LIFE_TIME

Every account has a database profile

- All accounts have only one database profile
- If no profile is specified when account created, the DEFAULT profile is used

Parameter	Default Setting	Description
FAILED_LOGIN_ATTEMPTS	10	Sets the maximum times a user try to log in and to fail before locking the account.
PASSWORD_GRACE_TIME	7	Sets the number of days that a user has to change his or her password before it expires.
PASSWORD_LIFE_TIME	180	Sets the number of days the user can use his or her current password.
PASSWORD_LOCK_TIME	1	Sets the number of days an account will be locked after the specified number of consecutive failed login attempts. After the time passes, then the account becomes unlocked.
PASSWORD_REUSE_MAX	UNLIMITED	Sets the number of password changes required before the current password can be reused.
PASSWORD_REUSE_TIME	UNLIMITED	Sets the number of days before which a password cannot be reused.

Not secure in any way!

The DEFAULT profile is created when the database is created (denv.bsq)

Profile Parameters: http://docs.oracle.com/cd/E11882_01/server.112/e41084/statements_6010.htm

- FAILED_LOGIN_ATTEMPTS – number of consecutive failed attempts to log in to the user account before the account is locked. If you omit this clause, then the default is 10 times.

NOTE: These two parameters must be set in conjunction with each other.

- PASSWORD_REUSE_TIME – specifies the number of days before which a password cannot be reused
- PASSWORD_REUSE_MAX – specifies the number of password changes required before the current password can be reused

If you specify a value for both of these parameters, then the user cannot reuse a password until the password has been changed the number of times specified for PASSWORD_REUSE_MAX during the number of days specified for PASSWORD_REUSE_TIME.

For example, if you specify PASSWORD_REUSE_TIME to 30 and PASSWORD_REUSE_MAX to 10, then the user can reuse the password after 30 days if the password has already been changed 10 times.

1. If you specify a value for either of these parameters and specify UNLIMITED for the other, then the user can never reuse a password.
2. If you specify DEFAULT for either parameter, then Oracle Database uses the value defined in the DEFAULT profile. By default, all parameters are set to UNLIMITED in the DEFAULT profile. If you have not changed the default setting of UNLIMITED in the DEFAULT profile, then the database treats the value for that parameter as UNLIMITED.
3. If you set both of these parameters to UNLIMITED, then the database ignores both of them. This is the default if you omit both parameters.

Special profile values

- UNLIMITED
  - No value set for the parameter
- DEFAULT
  - If a *resource_name* is omitted from the profile, the value from the DEFAULT profile is used

PROFILE	RESOURCE_NAME	RESOURCE_TYPE	LIMIT
MONITORING_PROFILE	FAILED_LOGIN_ATTEMPTS	PASSWORD	UNLIMITED
MONITORING_PROFILE	PASSWORD_LIFE_TIME	PASSWORD	DEFAULT
MONITORING_PROFILE	PASSWORD_REUSE_TIME	PASSWORD	DEFAULT
MONITORING_PROFILE	PASSWORD_REUSE_MAX	PASSWORD	DEFAULT
MONITORING_PROFILE	PASSWORD_VERIFY_FUNCTION	PASSWORD	DEFAULT
MONITORING_PROFILE	PASSWORD_LOCK_TIME	PASSWORD	DEFAULT
MONITORING_PROFILE	PASSWORD_GRACE_TIME	PASSWORD	DEFAULT

List accounts and profile limits

- Dictionary views
  - DBA_USERS (refer to slide 51)
  - DBA_PROFILES

```
SQL> desc dba_profiles
 Name                                      Null?    Type
 ----------------------------------------- -------- ----------------
 PROFILE                                   NOT NULL VARCHAR2(30)
 RESOURCE_NAME                             NOT NULL VARCHAR2(32)
 RESOURCE_TYPE                                      VARCHAR2(8)
 LIMIT                                              VARCHAR2(40)
```

List all accounts and Password profile settings

USERNAME	PROFILE	RESOURCE_NAME	LIMIT
SYS	DEFAULT	PASSWORD_REUSE_TIME	100
SYS	DEFAULT	COMPOSITE_LIMIT	UNLIMITED
SYS	DEFAULT	SESSIONS_PER_USER	UNLIMITED
SYS	DEFAULT	CPU_PER_SESSION	UNLIMITED
SYS	DEFAULT	CPU_PER_CALL	UNLIMITED
SYS	DEFAULT	LOGICAL_READS_PER_SESSION	UNLIMITED
SYS	DEFAULT	LOGICAL_READS_PER_CALL	UNLIMITED
SYS	DEFAULT	IDLE_TIME	UNLIMITED
SYS	DEFAULT	CONNECT_TIME	UNLIMITED
SYS	DEFAULT	PRIVATE_SGA	UNLIMITED
SYS	DEFAULT	FAILED_LOGIN_ATTEMPTS	UNLIMITED
SYS	DEFAULT	PASSWORD_LIFE_TIME	UNLIMITED
SYS	DEFAULT	PASSWORD_REUSE_MAX	UNLIMITED
SYS	DEFAULT	PASSWORD_VERIFY_FUNCTION	NULL
SYS	DEFAULT	PASSWORD_LOCK_TIME	1
SYS	DEFAULT	PASSWORD_GRACE_TIME	7
SYSTEM	DEFAULT	PASSWORD_LOCK_TIME	1
SYSTEM	DEFAULT	PASSWORD_REUSE_TIME	100
SYSTEM	DEFAULT	COMPOSITE_LIMIT	UNLIMITED
SYSTEM	DEFAULT	SESSIONS_PER_USER	UNLIMITED
SYSTEM	DEFAULT	CPU_PER_SESSION	UNLIMITED
SYSTEM	DEFAULT	CPU_PER_CALL	UNLIMITED
SYSTEM	DEFAULT	LOGICAL_READS_PER_SESSION	UNLIMITED
SYSTEM	DEFAULT	LOGICAL_READS_PER_CALL	UNLIMITED
SYSTEM	DEFAULT	IDLE_TIME	UNLIMITED
SYSTEM	DEFAULT	CONNECT_TIME	UNLIMITED
SYSTEM	DEFAULT	PRIVATE_SGA	UNLIMITED
SYSTEM	DEFAULT	FAILED_LOGIN_ATTEMPTS	UNLIMITED
SYSTEM	DEFAULT	PASSWORD_LIFE_TIME	UNLIMITED
SYSTEM	DEFAULT	PASSWORD_REUSE_MAX	UNLIMITED
SYSTEM	DEFAULT	PASSWORD_VERIFY_FUNCTION	NULL
SYSTEM	DEFAULT	PASSWORD_GRACE_TIME	7

Use the script list_account_profile_password_settings.sql

Password complexity testing

- Oracle ships **demo** password verification code
  - $ORACLE_HOME/rdbms/admin/utlpwdmg.sql

Not suitable for production systems, ever!

- Dictionary word check is minimal and easy
- Does not check password change time for frequency of change

Role analysis

Built in roles

- 56 built in roles in Oracle 11gR2

Built in roles: http://docs.oracle.com/cd/E15586_01/network.1111/e16543/authorization.htm#i1007401

Powerful roles

- DBA (obviously)
- Demo roles
  - CONNECT
  - RESOURCE
- JAVA
- Catalog
- Export/Import
- OLAP
- Admin

Should not be used

DBA:
DBA
LBAC_DBA

JAVA roles:
JAVASYSPRIV
JAVA_ADMIN
JAVA_DEPLOY
JMXSERVER
JAVADEBUGPRIV

Catalog roles:
DELETE_CATALOG_ROLE
EXECUTE_CATALOG_ROLE

Export/Import:
IMP_FULL_DATABASE
DATAPUMP_IMP_FULL_DATABASE
EXP_FULL_DATABASE
DATAPUMP_EXP_FULL_DATABASE

OLAP roles:
OLAP_DBA

SELECT_CATALOG_ROLE

```
find_all_privs: Release 1.0.7.0.0 - Production on Thu Oct 09 04:55:33 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF USER TO CHECK                [ORCL]: select_catalog_role

User => SELECT_CATALOG_ROLE has been granted the following privileges
=====================================================================
        ROLE => HS_ADMIN_SELECT_ROLE which contains =>
                TABLE PRIV => SELECT object => SYS.HS_ALL_CAPS grantable => NO
                TABLE PRIV => SELECT object => SYS.HS_ALL_DD grantable => NO
                TABLE PRIV => SELECT object => SYS.HS_ALL_INITS grantable => NO
                TABLE PRIV => SELECT object => SYS.HS_BASE_CAPS grantable => NO
                TABLE PRIV => SELECT object => SYS.HS_BASE_DD grantable => NO
                TABLE PRIV => SELECT object => SYS.HS_CLASS_CAPS grantable => NO
                TABLE PRIV => SELECT object => SYS.HS_CLASS_DD grantable => NO
                TABLE PRIV => SELECT object => SYS.HS_CLASS_INIT grantable => NO
                TABLE PRIV => SELECT object => SYS.HS_FDS_CLASS grantable => NO
                TABLE PRIV => SELECT object => SYS.HS_FDS_CLASS_DATE grantable => NO
                TABLE PRIV => SELECT object => SYS.HS_FDS_INST grantable => NO
                TABLE PRIV => SELECT object => SYS.HS_INST_CAPS grantable => NO
                TABLE PRIV => SELECT object => SYS.HS_INST_DD grantable => NO
                TABLE PRIV => SELECT object => SYS.HS_INST_INIT grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_RCVMAN grantable => NO
        TABLE PRIV => EXECUTE object => SYS.KU$_MONITOR_T grantable => NO
        TABLE PRIV => EXECUTE object => SYS.LOGSTDBY$TABF grantable => NO
        TABLE PRIV => EXECUTE object => SYS.LOGSTDBY$UTABF grantable => NO
        TABLE PRIV => EXECUTE object => SYS.XS$CATVIEW_UTIL grantable => NO
```

EXECUTE_CATALOG_ROLE

```
find_all_privs: Release 1.0.7.0.0 - Production on Thu Oct 09 05:04:43 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF USER TO CHECK                  [ORCL]: execute_catalog_role

User => EXECUTE_CATALOG_ROLE has been granted the following privileges
================================================================
        ROLE => HS_ADMIN_EXECUTE_ROLE which contains =>
                TABLE PRIV => EXECUTE object => SYS.DBMS_HS grantable => NO
        TABLE PRIV => EXECUTE object => SYS.AS_REPLAY grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMSHSXP grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMSJEXP_SYSPKGGRNT grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_ALERT grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_APPLY_ADM grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_APPLY_POSITION grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_AQ grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_AQADM grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_AQELM grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_AQIN grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_AQJMS_INTERNAL grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_AQ_IMPORT_INTERNAL grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_AUDIT_MGMT grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_AUTO_TASK_EXPORT grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_CAPTURE_ADM grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_CAPTURE_SWITCH_ADM grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_CDC_IPUBLISH grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_CDC_PUBLISH grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_CDC_SYS_IPUBLISH grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_CDC_UTILITY grantable => NO
        TABLE PRIV => EXECUTE object => SYS.DBMS_COMPARISON grantable => NO
```

Application roles

- Find all application roles
  - Properties of the roles
    - Object access
    - System privileges
    - Other roles
  - Accounts that have these roles

Use the script list_non_default_roles.sql

Finding roles

- DBA_ROLES lists all roles

```
SQL> desc dba_roles
 Name                                      Null?    Type
 ----------------------------------------- -------- ----------------------
 ROLE                                      NOT NULL VARCHAR2(30)
 PASSWORD_REQUIRED                                  VARCHAR2(8)
 AUTHENTICATION_TYPE                                VARCHAR2(11)
```

- Cannot easily segregate built in roles from application roles

```
ROLE
------------------------------
TT_CACHE_ADMIN_ROLE

1 row selected.
```


Use list_non_default_roles.sql

Analyze all application (non built-in)__ roles

- Identify all accounts with the role

```
who_has_priv: Release 1.0.3.0.0 - Production on Fri Oct 03 03:38:46 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

ROLE TO CHECK                          [DBA]: TT_CACHE_ADMIN_ROLE

Investigating Role => TT_CACHE_ADMIN_ROLE (PWD = NO) which is granted to =>
================================================================================
        User => CACHEADM (ADM = NO)
        User => SYS (ADM = YES)

PL/SQL procedure successfully completed.
```

- Find all privileges assigned to the role

```
find_all_privs: Release 1.0.7.0.0 - Production on Fri Oct 03 03:38:59 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF USER TO CHECK                  [ORCL]: TT_CACHE_ADMIN_ROLE

User => TT_CACHE_ADMIN_ROLE has been granted the following privileges
================================================================================
        TABLE PRIV => DELETE object => TIMESTEN.TT_GRIDINFO grantable => NO
        TABLE PRIV => INSERT object => TIMESTEN.TT_GRIDINFO grantable => NO
        TABLE PRIV => SELECT object => TIMESTEN.TT_GRIDID grantable => NO
        TABLE PRIV => SELECT object => TIMESTEN.TT_GRIDINFO grantable => NO
        TABLE PRIV => UPDATE object => TIMESTEN.TT_GRIDID grantable => NO
        TABLE PRIV => UPDATE object => TIMESTEN.TT_GRIDINFO grantable => NO

PL/SQL procedure successfully completed.
```


Use the scripts who_has_role.sql and find_all_privs.sql

SYSDBA, SYSOPER, and SYSASM

- Extremely powerful database roles
- Linked into the database kernel during installation
- Allows **UNAUTHENTICATED** access to the database from the operating system layer.

Compiled into the database kernel

- Files created at installation time and used during linking to define the OS groups in the DB kernel
  - C language or assembler file, depending on your platform

```
/*  SS_DBA_GRP defines the UNIX group ID for sqldba administrative access.  */
/*  Refer to the Installation and User's Guide for further information.  */

/* IMPORTANT: this file needs to be in sync with
              rdbms/src/server/osds/config.c, specifically regarding the
              number of elements in the ss_dba_grp array.
 */

#define SS_DBA_GRP "oracle"
#define SS_OPER_GRP ""
#define SS_ASM_GRP ""

char *ss_dba_grp[] = {SS_DBA_GRP, SS_OPER_GRP, SS_ASM_GRP};
```

Uses of SYSDBA, SYSOPER, SYSASM

Privilege	Description	OS group
SYSDBA	• Perform STARTUP and SHUTDOWN operations • ALTER DATABASE: open, mount, back up, or change character set • CREATE DATABASE • DROP DATABASE • CREATE SPFILE • ALTER DATABASE ARCHIVELOG • ALTER DATABASE RECOVER • Includes the RESTRICTED SESSION privilege	dba
SYSOPER	• Perform STARTUP and SHUTDOWN operations • CREATE SPFILE • ALTER DATABASE OPEN/MOUNT/BACKUP • ALTER DATABASE ARCHIVELOG • ALTER DATABASE RECOVER (Complete recovery only. Any form of incomplete recovery, such as UNTIL TIME|CHANGE|CANCEL|CONTROLFILE requires connecting as SYSDBA.) • Includes the RESTRICTED SESSION privilege	oper
SYSASM	• Similar to SYSDBA, but restricted to ASM instance	asm

Dictionary object

```
SQL> select * from v$pwfile_users;

USERNAME                       SYSDB SYSOP SYSAS
------------------------------ ----- ----- -----
SYS                            TRUE  TRUE  FALSE
SYSTEM                         TRUE  FALSE FALSE
```


The v$pwfile_users view is a list of all users in the system who have been granted SYSDBA, SYSOPER, and/or SYSASM.

SYSTEM account: This account can perform all administrative functions except the following:
- Backup and recovery
- Database upgrade

SYS account: This account can perform all administrative functions. All base (underlying) tables and views for the database data dictionary are stored in the SYS schema. These base tables and views are critical for the operation of Oracle Database.

SYSDBA: Administrative account used to start and manage the database. Super-user account.

SYSOPER: Administrative account which can start the database. Less privileges than SYSDBA.

SYSASM: Administrative account used to manage ASM database instance. Separation of SYSDBA from disk volume management.

When a database is created, SYS is automatically a member of SYSDBA. When any user in the operating system group “dba” performs a connect “/ as sysdba”, they are the user SYS.

When an user has the operating system account “oper” performs a connect “/ as sysoper”, they are connected to the default schema, PUBLIC.

How to find ASM users in the ASM instance:
1. Run the asmcmd utility

System privileges

System privileges

- Static set of system privileges - 208 system privileges
- Built into the database when created
  - Cannot create custom system privileges

```
SQL> select count(*) from system_privilege_map;

  COUNT(*)
----------
       208
```


System privilege descriptions: http://docs.oracle.com/cd/E11882_01/server.112/e41084/statements_9013.htm#BABEFFEE

All privileges

- Identify accounts with all privileges
  - GRANT ALL PRIVILEGES
  - Given to the DBA role

```
SQL> l
  1  SELECT a.username, COUNT(b.privilege)
  2  FROM   dba_users a, dba_sys_privs b
  3  WHERE  b.grantee = a.username
  4  GROUP BY a.username
  5  HAVING COUNT(b.privilege) >= (SELECT COUNT(privilege)
  6                                FROM   dba_sys_privs
  7*                               WHERE  grantee = 'DBA')
SQL> /

no rows selected
```


Use the script all_privileges.sql

Finding system privilege assignments

- Use the script who_has_priv.sql

Use the script who_has_priv.sql

UNLIMITED TABLESPACE

- Unlimited space quota in all tablespaces (Including SYSTEM)
- Can introduce a DoS

```
SQL> @who_has_priv



who_has_priv: Release 1.0.3.0.0 - Production on Sun Sep 28 07:05:50 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

PRIVILEGE TO CHECK        [SELECT ANY TABLE]: unlimited tablespace

Privilege => UNLIMITED TABLESPACE has been granted to =>
================================================================================
        User => WMSYS (ADM = NO)
        User => XDB (ADM = NO)
        User => ORABLOG (ADM = NO)
        User => JACK_DEV (ADM = NO)
        User => MDSYS (ADM = NO)
        User => APEX_040000 (ADM = YES)
        User => DEMO (ADM = NO)
        User => PLS (ADM = NO)
        User => SYS (ADM = NO)
```


Use the script who_has_priv.sql

Dangerous system privileges

- There are many system privileges that give excessive access
  - Privileges with '%ANY%' modifier
    - Can affect any schema in the database
    - CREATE ANY TABLE
    - CREATE ANY TRIGGER

```
SQL> select count(*) from system_privilege_map where name like '%ANY%';

  COUNT(*)
----------
       132
```

ALTER SESSION/ ALTER SYSTEM

- Change session or system parameters
- Ensure these are not granted to application schemas or non-DBAs

```
SQL> @who_has_priv


who_has_priv: Release 1.0.3.0.0 - Production on Sun Sep 28 07:08:48 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

PRIVILEGE TO CHECK        [SELECT ANY TABLE]: alter session

Privilege => ALTER SESSION has been granted to =>
--------------------------------------------------------------------------------
        Role => DBA (ADM = YES) which is granted to =>
                User => SYS (ADM = YES)
                User => PHPDEMO (ADM = NO)
                User => SYSTEM (ADM = YES)
        User => SYS (ADM = NO)
        User => APEX_040000 (ADM = NO)
        User => IX (ADM = NO)
        User => SH (ADM = NO)
        User => XFILES (ADM = NO)
        User => XDBMETADATA (ADM = NO)
        Role => RECOVERY_CATALOG_OWNER (ADM = NO) which is granted to =>
                User => SYS (ADM = YES)
        User => OWBSYS (ADM = YES)
        User => OE (ADM = NO)
        User => TTNR (ADM = NO)
        User => PHPDEMO (ADM = NO)
        User => CTXSYS (ADM = NO)
        Role => OWB$CLIENT (ADM = NO) which is granted to =>
                User => SYS (ADM = YES)
                User => OWBSYS (ADM = YES)
        User => SCOTT (ADM = NO)
        User => OE1 (ADM = NO)
        User => HR1 (ADM = NO)
        User => OWBSYS_AUDIT (ADM = NO)
        User => APPQOSSYS (ADM = NO)
        User => SYSMAN (ADM = NO)
        User => HR (ADM = NO)
        User => XDB (ADM = NO)
```


ALTER SESSION: http://docs.oracle.com/cd/E11882_01/server.112/e41084/statements_2013.htm#SQLRF00901

SELECT ANY DICTIONARY

- Work around system privilege
  - Circumvents parameter o7_dictionary_accessibility

```
who_has_priv: Release 1.0.3.0.0 - Production on Sun Sep 28 07:19:36 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

PRIVILEGE TO CHECK        [SELECT ANY TABLE]: select any dictionary

Privilege => SELECT ANY DICTIONARY has been granted to =>
-------------------------------------------------------------------------
        User => OLAPSYS (ADM = NO)
        Role => DBA (ADM = YES) which is granted to =>
                User => SYS (ADM = YES)
                User => PHPDEMO (ADM = NO)
                User => SYSTEM (ADM = YES)
        User => WMSYS (ADM = YES)
        User => SYSMAN (ADM = NO)
        User => ORACLE_OCM (ADM = NO)
        Role => OEM_MONITOR (ADM = NO) which is granted to =>
                User => DBSNMP (ADM = NO)
                User => SYS (ADM = YES)
        User => DBSNMP (ADM = NO)
        User => AUDITOR (ADM = NO)
        User => EX (ADM = NO)
        User => JACK_DEV (ADM = NO)
        User => JOHN_DEV (ADM = NO)
```

Privileges “with admin” or “with grant”

- Allows holder of the privilege to give access to the privilege to others

```
 1  select count(*)
 2  from (
 3  select  'ROLE' typofgrant, grantee,        granted_role priv
 4  from    dba_role_privs
 5  where   admin_option='YES'
 6  UNION ALL
 7  select  'SYSTEM' typofgrant, grantee,      privilege priv
 8  from    dba_sys_privs
 9  where   admin_option='YES'
10* )
SQL> /

  COUNT(*)
----------
       347
```

- Beware of application accounts with these options

Use the script admin_grants.sql

Directory privileges

- Access to OS file system
- Test CREATE ANY DIRECTORY and DROP ANY DIRECTORY
  - Check the directories
  - Check all application created directories
    - File permissions
    - Sensitive data

Use the dictionary view DBA_DIRECTORIES: http://docs.oracle.com/cd/E11882_01/server.112/e40402/statviews_1078.htm#REFRN20061

ADMINISTER DATABASE TRIGGER

- System level triggers
  - Important for security

```
who_has_priv: Release 1.0.3.0.0 - Production on Mon Sep 29 03:42:32 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

PRIVILEGE TO CHECK       [SELECT ANY TABLE]: administer database trigger

Privilege => ADMINISTER DATABASE TRIGGER has been granted to =>
-------------------------------------------------------------------------
       User => WMSYS (ADM = NO)
       User => EXFSYS (ADM = NO)
       Role => DBA (ADM = YES) which is granted to =>
              User => SYS (ADM = YES)
              User => PHPDEMO (ADM = NO)
              User => SYSTEM (ADM = YES)
       User => SYS (ADM = NO)
       Role => IMP_FULL_DATABASE (ADM = NO) which is granted to =>
              User => SYS (ADM = YES)
              Role => DBA (ADM = NO) which is granted to =>
                     User => SYS (ADM = YES)
                     User => PHPDEMO (ADM = NO)
                     User => SYSTEM (ADM = YES)
              Role => DATAPUMP_IMP_FULL_DATABASE (ADM = NO) which is granted to =>
                     Role => DBA (ADM = NO) which is granted to =>
                            User => SYS (ADM = YES)
                            User => PHPDEMO (ADM = NO)
                            User => SYSTEM (ADM = YES)
                     User => SYS (ADM = YES)
```

Import/Export

- Can give access to password hashes and sensitive application data

```
who_has_priv: Release 1.0.3.0.0 - Production on Mon Sep 29 03:48:53 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

ROLE TO CHECK                          [DBA]: EXPORT FULL DATABASE

Investigating Role => EXPORT FULL DATABASE (PWD = ) which is granted to =>
======================================================================

PL/SQL procedure successfully completed.
```

Internet packages and fine grained access

- UTL_TCP, UTL_SNMP, UTL_MAIL, UTL_HTTP, UTL_INADDR
- Access to PUBLIC by default
- Test each of these for access
  - Do not use a DBA account!
- ACLs implemented from DBMS_NETWORK_ACL_ADMIN
  - Does not control package access!

Internet packages

```
SQL> @who_can_access

NAME OF OBJECT TO CHECK       [USER_OBJECTS]: utl_http
OWNER OF THE OBJECT TO CHECK          [USER]: sys

Checking object => SYS.UTL_HTTP
================================================================================


Object type is => PACKAGE (TAB)
        Privilege => EXECUTE is granted to =>
        User => APEX_040000 (ADM = NO)
        User => ORDPLUGINS (ADM = NO)
        Role => PUBLIC (ADM = NO)

PL/SQL procedure successfully completed.
```

ACLs must be enabled for non-administrative users

```
SQL> sho user
USER is "SYS"
SQL> l
  1  SELECT SUBSTR(utl_http.request('http://www.google.com'),1,80)
  2* FROM   dual
SQL> /

SUBSTR(UTL_HTTP.REQUEST('HTTP://WWW.GOOGLE.COM'),1,80)
--------------------------------------------------------------------------------
<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en"

1 row selected.

SQL> connect auditor
Enter password:
Connected.
SQL> sho user
USER is "AUDITOR"
SQL> /
SELECT SUBSTR(utl_http.request('http://www.google.com'),1,80)
              *
ERROR at line 1:
ORA-29273: HTTP request failed
ORA-06512: at "SYS.UTL_HTTP", line 1722
ORA-24247: network access denied by access control list (ACL)
ORA-06512: at line 1
```

Finding ACLs

- SYS ACL access for all database accounts

```
ACL,USERNAME,GRANTED?
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,SPATIAL_WFS_ADMIN_USR,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,DIP,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,SH,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,IX,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,MDDATA,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,ORACLE_OCM,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,SPATIAL_CSW_ADMIN_USR,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,PM,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,BI,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,XS$NULL,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,OLAPSYS,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,OWBSYS,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,ORDPLUGINS,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,OWBSYS_AUDIT,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,APPQOSSYS,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,EXFSYS,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,ORDSYS,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,SI_INFORMTN_SCHEMA,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,CTXSYS,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,ORDDATA,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,WMSYS,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,MDSYS,
/sys/acls/ANONYMOUS/ANONYMOUS711520ce1467276bc040e4adcde2121_acl.xml,OUTLN,
```


Use the script list_network_acl_privileges.sql

Change management

Object changes

- Two methods
  - Initialization parameter - ENABLE_DDL_TRACKING
  - Query the data dictionary

ENABLE_DDL_LOGGING: http://docs.oracle.com/cd/E11882_01/server.112/e40402/initparams085.htm#REFRN10302

ENABLE_DDL_LOGGING

- Writes changes to the instance alert log
- Changeable with
  - ALTER SESSION
  - ALTER SYSTEM

Logs the following changes:

ALTER/CREATE/DROP/TRUNCATE CLUSTER
ALTER/CREATE/DROP FUNCTION
ALTER/CREATE/DROP INDEX
ALTER/CREATE/DROP OUTLINE
ALTER/CREATE/DROP PACKAGE
ALTER/CREATE/DROP PACKAGE BODY
ALTER/CREATE/DROP PROCEDURE
ALTER/CREATE/DROP PROFILE
ALTER/CREATE/DROP SEQUENCE
CREATE/DROP SYNONYM
ALTER/CREATE/DROP/RENAME/TRUNCATE TABLE
ALTER/CREATE/DROP TRIGGER
ALTER/CREATE/DROP TYPE
ALTER/CREATE/DROP TYPE BODY
DROP USER
ALTER/CREATE/DROP VIEW

Query the data dictionary

- Dictionary object - DBA_OBJECTS

```
SQL> desc dba_objects
 Name                                      Null?    Type
 ----------------------------------------- -------- ----------------------------
 OWNER                                              VARCHAR2(30)
 OBJECT_NAME                                        VARCHAR2(128)
 SUBOBJECT_NAME                                     VARCHAR2(30)
 OBJECT_ID                                          NUMBER
 DATA_OBJECT_ID                                     NUMBER
 OBJECT_TYPE                                        VARCHAR2(19)
 CREATED                                            DATE
 LAST_DDL_TIME                                      DATE
 TIMESTAMP                                          VARCHAR2(19)
 STATUS                                             VARCHAR2(7)
 TEMPORARY                                          VARCHAR2(1)
 GENERATED                                          VARCHAR2(1)
 SECONDARY                                          VARCHAR2(1)
 NAMESPACE                                          NUMBER
 EDITION_NAME                                       VARCHAR2(30)
```

```
SQL> @last_changed_objs
Enter number of days back from now to test object age [30]:
OWNER,OBJECT_NAME,OBJECT_TYPE,CREATED,LAST_DDL_TIME,SYSTEM_DATE,CHANGE_DATE
SQL>
```


Object types to check:

- PROCEDURE
- TRIGGER
- OPERATOR
- VIEW
- MATERIALIZED VIEW
- SYNONYM
- All PACKAGE types (header and body)
- All JAVA types (data, resource, class, source)
- TYPE

Use the script last_changed_objs.sql

Object access

Access to objects

- Internal database objects
- File system objects

Key dictionary objects

- Identify access to dictionary objects
  - Password hashes
  - Account enumeration

Password storage

- Account passwords stored in the database
- SYS.USER$.PASSWORD **3DES hash**
- SYS.USER$.SPARE4 **SHA1 hash**
- SYS.USER_HISTORY$.PASSWORD **3DES hash**
- SYS.LINK$.PASSWORD **3DES hash**
- Many others

Access to tables with passwords

```
who_can_access: Release 1.0.3.0.0 - Production on Wed Oct 01 03:50:15 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF OBJECT TO CHECK       [USER_OBJECTS]: user$
OWNER OF THE OBJECT TO CHECK          [USER]: sys

Checking object => SYS.USER$
================================================================================


Object type is => TABLE (TAB)
       Privilege => SELECT is granted to =>
       User => APEX_040000 (ADM = NO)
       User => CTXSYS (ADM = NO)
       User => XDB (ADM = NO)

PL/SQL procedure successfully completed.
```

```
who_can_access: Release 1.0.3.0.0 - Production on Wed Oct 01 03:52:01 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF OBJECT TO CHECK       [USER_OBJECTS]: user_history$
OWNER OF THE OBJECT TO CHECK          [USER]: sys

Checking object => SYS.USER_HISTORY$
================================================================================


PL/SQL procedure successfully completed.
```

```
who_can_access: Release 1.0.3.0.0 - Production on Wed Oct 01 03:53:30 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF OBJECT TO CHECK       [USER_OBJECTS]: link$
OWNER OF THE OBJECT TO CHECK          [USER]: sys

Checking object => SYS.LINK$
================================================================================


PL/SQL procedure successfully completed.
```


Use the script who_can_access.sql

Finding sensitive data

Identify location of sensitive data

- Easiest - ask
- Look through the data dictionary

OWNER	TABLE_NAME	COLUMN_NAME	DATA_TYPE	DATA_LENGTH	DATA_PRECISION	DATA_SCALE
JACK_DEV	CCNAMES	PAN	VARCHAR2	4000	(null)	(null)
JACK_DEV	CC_TAB	PAN	RAW	100	(null)	(null)
JOHN_DEV	CC1	PAN	VARCHAR2	4000	(null)	(null)
JOHN_DEV	CREDIT_CARD	FIRST_NAME	VARCHAR2	50	(null)	(null)
JOHN_DEV	CREDIT_CARD	LAST_NAME	VARCHAR2	50	(null)	(null)
JOHN_DEV	CREDIT_CARD	NAME_ON_CARD	VARCHAR2	100	(null)	(null)
JOHN_DEV	CREDIT_CARD	PAN	RAW	100	(null)	(null)
ORABLOG	BIN$ruM7cUCCGf3gQAR/AQAMWg==$0	PAN	RAW	100	(null)	(null)
ORABLOG	CREDIT_CARD	FIRST_NAME	VARCHAR2	50	(null)	(null)
ORABLOG	CREDIT_CARD	LAST_NAME	VARCHAR2	50	(null)	(null)
ORABLOG	CREDIT_CARD	NAME_ON_CARD	VARCHAR2	100	(null)	(null)
ORABLOG	CREDIT_CARD	PAN	RAW	100	(null)	(null)
ORABLOG	PROD_CC	PAN	VARCHAR2	4000	(null)	(null)
SYSTEM	CREDIT_CARD	FIRST_NAME	VARCHAR2	50	(null)	(null)
SYSTEM	CREDIT_CARD	LAST_NAME	VARCHAR2	50	(null)	(null)
SYSTEM	CREDIT_CARD	NAME_ON_CARD	VARCHAR2	100	(null)	(null)
SYSTEM	CREDIT_CARD	PAN	RAW	100	(null)	(null)

Use the script find_data_by_table_column.sql

Find dependencies

- Identified in the data dictionary
  - Tables: views, stored code, etc.

OWNER	NAME	TYPE	REFERENCED_OWNER	REFERENCED_NAME	REFERENCED_TYPE	REFERENCED_LINK_NAME	DEPENDENCY_TYPE
ORABLOG	BI_CC	TRIGGER	ORABLOG	CREDIT_CARD	TABLE	(null)	HARD
JOHN_DEV	CC1	VIEW	ORABLOG	CREDIT_CARD	TABLE	(null)	HARD
JACK_DEV	CCNAMES	VIEW	ORABLOG	CREDIT_CARD	TABLE	(null)	HARD
ORABLOG	PROD_CC	VIEW	ORABLOG	CREDIT_CARD	TABLE	(null)	HARD

- Look at access to all the identified objects

Use the script list_dependencies.sql

```
who_can_access: Release 1.0.3.0.0 - Production on Wed Oct 01 04:57:51 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF OBJECT TO CHECK       [USER_OBJECTS]: credit_card
OWNER OF THE OBJECT TO CHECK          [USER]: orablog

Checking object => ORABLOG.CREDIT_CARD
================================================================================


Object type is => TABLE (TAB)
        Privilege => SELECT is granted to =>
        Role => PUBLIC (ADM = NO)

PL/SQL procedure successfully completed.
```

```
who_can_access: Release 1.0.3.0.0 - Production on Wed Oct 01 05:05:38 2014
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF OBJECT TO CHECK       [USER_OBJECTS]: prod_cc
OWNER OF THE OBJECT TO CHECK          [USER]: orablog

Checking object => ORABLOG.PROD_CC
================================================================================


PL/SQL procedure successfully completed.
```


Use the script who_can_access.sql

Resources

- Oracle SQL Language Reference
- Oracle database security guide
- Pete Finnigan's web site
- Paul Wright's web site
- Oracle 2 Day DBA
- Oracle 2 Day + Security Guide
- VirtualBox & pre-built VM

Oracle SQL Language Reference: http://docs.oracle.com/cd/E11882_01/server.112/e41084/toc.htm

Oracle database security guide: http://docs.oracle.com/cd/E11882_01/network.112/e16543/toc.htm

Pete Finnigan: http://petefinnigan.com

Paul Wright: http://oracleforensics.com/

Oracle 2 Day DBA: http://docs.oracle.com/cd/E11882_01/server.112/e10897/toc.htm

Oracle 2 Day + Security Guide: http://docs.oracle.com/cd/E11882_01/server.112/e10575/toc.htm

VirtualBox download: https://www.virtualbox.org/wiki/Downloads

Pre-built VM: http://www.oracle.com/technetwork/community/developer-vm/index.html#dbapp

Q & A

Thank you

ron.reidy@gmail.com