INTEGRIGY

Oracle Database Security Quick Reference

Version 5.1 – April 2018

1. Standard Oracle Database Accounts

Standard Oracle Database accounts that may be present –

User Name	Default Password	Source
SYS	CHANGE_ON_INSTALL	Installation
SYSTEM	MANAGER	Installation
ANONYMOUS	ANONYMOUS	XDB
APPQOSSYS	APPQOSSYS	Service Mgmt
AUDSYS	AUDSYS	Auditing (12c)
CTXSYS	CTXSYS	Oracle Text
DBSNMP	DBSNMP	Intelligent Agent
DIP	DIP	Internet Dir
DMSYS	DMSYS	Data Mining
EXFSYS	EXFSYS	Expression Filters
LBACSYS	LBACSYS	Label Security
MDDATA	MDDATA	Spatial
MDSYS	MDSYS	Spatial
MGDSYS	MGDSYS	Identity Code (RFID)
ODM	ODM	Data Mining
ODM_MTR	MTRPW	Data Mining
OLAPDBA	OLAPDBA	OLAP
OLAPSVR	OLAPSVR	OLAP
OLAPSYS	OLAPSYS	OLAP
ORACLE_OCM	ORACLE_OCM	Config Mgr
ORDPLUGINS	ORDPLUGINS	interMedia
ORDSYS	ORDSYS	interMedia
OUTLN	OUTLN	Plans
OWBSYS	OWBSYS	Warehouse Builder
RMAN	RMAN	RMAN
SCOTT	TIGER	Sample
SI_INFORMTN_SCHEMA	SI_INFORMTN_SCHEMA	interMedia
SYSMAN	OEM_TEMP	OEM
TSMSYS	TSMSYS	Migration
WK_TEST	WK_TEST	Ultra Search
WKPROXY	CHANGE_ON_INSTALL	Ultra Search
WKSYS	CHANGE_ON_INSTALL	Ultra Search
WMSYS	WMSYS	Workspace Mgr
XDB	CHANGE_ON_INSTALL	XDB

A simplistic check for the above passwords in 11g and later –

```
SQL> select * from sys.dba_users_with_defpwd;
```

2. Password Controls and Profiles

A custom PASSWORD_VERIFY_FUNCTION must be created to enforce password length and complexity for all database accounts – see $ORACLE_HOME/rdbms/admin/utlpwdmg.sql for example. 11g initialization parameter "sec_case_sensitive_logon = true" may be used to allow case sensitive passwords.

Resource Name	Units	10g Default	11g Default
FAILED_LOGIN_ATTEMPTS [1]	Attempts	10	10
PASSWORD_GRACE_TIME	Days	unlimited	7
PASSWORD_LIFE_TIME	Days	unlimited	unlimited
PASSWORD_LOCK_TIME	Days	unlimited	1
PASSWORD_REUSE_MAX [2]	Passwords	unlimited	unlimited
PASSWORD_REUSE_TIME [2]	Days	unlimited	unlimited

[1] The SYS account is exempt from the FAILED_LOGIN_ATTEMPTS settings, therefore, cannot be locked due to excessive number of failed logins.

[2] PASSWORD_REUSE_MAX and PASSWORD_REUSE_TIME work in conjunction – setting PASSWORD_REUSE_MAX to 5 and PASSWORD_REUSE_TIME to 360 days will not allow a user to reuse the same password for at least 5 passwords and in a 360 day period. Setting either value to UNLIMITED never permits a user to reuse the same password.

To set a password profile parameter –

```
SQL> alter profile <profile name> limit \
      <resource name> <value>;
```

3. Critical Patch Updates (CPU) Baseline

Database Version	Includes the following CPU
9.2.0.8	July 2006
10.1.0.5	October 2005
10.2.0.3	October 2006
10.2.0.4	April 2008
10.2.0.5	October 2010
11.1.0.6	October 2007
11.1.0.7	January 2009
11.2.0.1	January 2010
11.2.0.2	January 2011
11.2.0.3	July 2011
11.2.0.4	October 2013
12.1.0.1	July 2013
12.1.0.2	July 2014

4. Critical Patch Update (CPU) Applied

11g `SQL> select * from sys.dba_registry_history;`

12c `SQL> select * from sys.dba_registry_sqlpatch;`

5. Security Related SYS Views and Tables

Users and Roles	
dba_users	dba_roles
dba_users_with_defpwd	user$
dba_profiles	user$history
dba_proxies	v$pwfile_users
Privileges	
dba_col_privs	dba_connect_role_grantees
dba_role_privs	system_privilege_map
dba_sys_privs	table_privilege_map
dba_tab_privs	dba_ts_quotas
Auditing	
aud$	dba_priv_audit_opts
dba_audit_exists	dba_stmt_audit_opts
dba_audit_object	stmt_audit_option_map
dba_audit_session	dba_audit_policies
dba_audit_statement	dba_audit_policy_columns
dba_audit_trail	dba_fga_audit_trail
dba_common_audit_trail	fga_log$
dba_obj_audit_opts	
Other Security	
dba_encrypted_columns	dba_policies
dba_java_policy	dba_policy_contexts
dba_network_acls	dba_policy_groups
dba_network_acl_privileges	registry$history

6. Recommended File Permissions

Path	Files	Unix Perm
$ORACLE_HOME	all	750
$ORACLE_HOME/bin	all	751
$ORACLE_HOME/dbs	init.ora	644
$ORACLE_HOME/dbs	spfile.ora	640
$ORACLE_HOME/network/admin	listener.ora sqlnet.ora	644
init.ora – audit_file_dest	all	600
init.ora – background_dump_dest	all	660
init.ora – core_dump_dest	all	660
init.ora – diagnostic_dest	all	660
init.ora – control files	control files	640
init.ora – log_archive_dest_n	all	750
init.ora – user_dump_dest	all	660
Unix/Linux umask	oracle account	022

7. Security Related Initialization Parameters

Parameter	Default	Suggest
Security Settings		
_trace_files_public	FALSE	FALSE
db_securefile (11g)	PERMITTED	ALWAYS
dispatches (XDB)	XDB setting	(null)
global_names	FALSE	TRUE
o7_dictionary_accessibility	FALSE	FALSE
remote_listener	(null)	(null)
remote_login_passwordfile	SHARED	NONE
sec_case_sensitive_logon (11g)	TRUE	TRUE
sec_max_failed_login_attempts (11g)	10	3
sec_protocol_error_further _action (11g)	CONTINUE	DELAY,2
sec_protocol_error_trace_action (11g)	TRACE	LOG
sec_return_server_release_ banner (11g)	FALSE	FALSE
sql92_security	FALSE	TRUE
utl_file_dir	(null)	(null)
OS Authentication		
os_authent_prefix	ops$	(null)
os_roles	FALSE	FALSE
remote_os_authent	FALSE	FALSE
remote_os_roles	FALSE	FALSE
Auditing		
audit_trail	NONE	not NONE
audit_sys_operations	FALSE	TRUE
audit_syslog_level (10.2+)	(null)	local1.info

8. Useful SQL Security Statements

```
alter user <username> identified by <password>;

alter user <username> account lock;
alter user <username> password expire;
alter user <username> profile <profile>;

revoke <privilege> [on <object name>]
       from <user|role>;

grant <privilege> [on <object name>]
      to <user|role>;

audit <audit> [on <object name>]
     [whenever successful|not successful]
     [by <user>] [by session] [by access];
```

9. Important System and Object Privileges

Object	Grantable System Privileges
Database	alter database, alter system, audit system
Database Links	create database link, create public database link, drop public database link
Directories	create any directory, drop any directory
Indexes	create any index, alter any index, drop any index
Procedures	create procedure, create any procedure, alter any procedure, drop any procedure, execute any procedure
Profiles	create profile, alter profile, drop profile
Roles	create role, alter any role, drop any role, grant any role
Sessions	create session, alter resource cost, alter session, restricted session
Synonyms	create synonym, create any synonym, create public synonym, drop any synonym, drop public synonym
Tables	create table, create any table, alter any table, backup any table, delete any table, drop any table, insert any table, lock any table, select any table, flashback any table, update any table
Triggers	create trigger, create any trigger, alter any trigger, drop any trigger, administer database trigger, create any trigger
Users	create user, alter user
Views	create view, create any view, drop any view, under any view, flashback any table, merge any view
Misc.	analyze any, audit any, become user, exempt access policy, grant any object privilege, grant any privilege, select any dictionary, sysdba, sysoper

Object	Grantable Object Privileges
Table	alter, delete, debug, flashback, on commit refresh, query rewrite, index, insert, references, select, update
View	debug, delete, flashback, insert, references, select, under, update
Sequence	alter, select
Proc, Func, Pack	debug, execute
Materialized View	delete, flashback, on commit refresh, query rewrite, select, insert, update
Directory	read, write, execute (11g)
Library	execute
Object Type	debug, execute, under
Indextype	execute
Operator	execute
Edition	use
Mining Model	alter, select
OLAP	insert, alter, delete, select, update
Scheduler	execute, alter

10. Auditing Configuration

AUDIT_TRAIL Settings	9.2	10.1	10.2	11.x
OS	x	x	x	x
DB	x	x	x	x
DB, EXTENDED		x	x	x
XML			x	x
XML, EXTENDED			x	x
OS -> AUDIT_SYSLOG_LEVEL			x	x

Audit Shortcut	SQL Statements Audited
database link	create database link, drop database link
directory	create directory, drop directory
grant <object>	grant <privilege> on <object>, revoke <privilege> from <object>
index	create index, alter index, analyze index, drop index
procedure	create function, create library, create package, create package body, create procedure, drop function, drop library, drop package, drop procedure
profile	create profile, alter profile, drop profile
public database link	create public database link, drop public database link
public synonym	create public synonym, drop public synonym
role	create role, alter role, drop role, set role
system audit	audit, noaudit
system grant	grant, revoke *(system privileges and roles only)*
table	create table, drop table, truncate table
user	create user, alter user, drop user
view	create view, drop view
-	alter system, not exists, session, execute procedure, select table, update table, insert table, delete table, alter table

http://www.integrigy.com

Version 5.1 – April 2018

Oracle Database versions 10.2, 11.1, 11.2, 12.1