Summary of changes to the Oracle RDBMS to meet the Security Baseline

David Litchfield
david@davidlitchfield.com
January 2017

Settings	Severity	CIS	Check ID
Set AUDIT_SYS_OPERATIONS to “true”	3	Yes	0.0
Set AUDIT_TRAIL to “DB”	2	Yes	0.1
Set BACKGROUND_CORE_DUMP to “partial”	2	No	0.4
Set SHADOW_CORE_DUMP to “none”	2	No	0.5
Set O7_DICTIONARY_ACCESSIBILITY to “false”	2	Yes	0.7
Set OS_ROLES to “false”	2	Yes	0.8
Set REMOTE_LOGIN_PASSWORDFILE to “none”	2	Yes	0.10
Set REMOTE_OS_AUTHENT to “false”	2	Yes	0.11
Set REMOTE_OS_ROLES to “false”	2	Yes	0.13
Ensure UTL_FILE_DIR is neither set to “*” nor “/”	3	Yes	0.14/0.15
Set SEC_CASE_SENSITIVE_LOGON is set to “true”	2	Yes	0.16
Set SEC_MAX_FAILED_LOGIN_ATTEMPTS to 10 or less	2	Yes	0.17
Set SEC_PROTOCOL_ERROR_FURTHER_ACTION to “delay,3” or “drop,3”	2	Yes	0.18
Set SEC_PROTOCOL_ERROR_TRACE_ACTION to “log”	2	Yes	0.19
Set SEC_RETURN_SERVER_RELEASE_BANNER to “false”	2	Yes	0.20
Set SQL92_SECURITY to “true”	2	Yes	0.21
Set RESOURCE_LIMIT to “true”	2	Yes	0.22
Set OPTIMIZER_SECURE_VIEW_MERGING to “true”	2	No	0.23
Set RECYCLEBIN to “off”	2	No	0.24
Set ENABLE_DDL_LOGGING to “true”	2	No	0.25
Drop *sample* schemas: SH, IX, HR, OE, PM, SCOTT, BI	2	Yes	1.1
Drop the SYS.USER$MIG table	2	Yes	1.27
Set an OS user for Java OS exec calls	2	No	2.2
Ensure only SYS, SYSDG, SYSBACKUP and SYSKM are password file users	4	No	2.4
Ensure no user has password set to “EXTERNAL”	2	Yes	2.5
Ensure no user is assigned to the default profile	2	Yes	2.6
Revoke EXECUTE ANY PROCEDURE from DBSNMP	2	Yes	3.4
Revoke EXECUTE ANY PROCEDURE from OUTLN	2	Yes	3.5
Revoke all system privileges from all proxy users	2	Yes	3.6
Revoke all roles except CONNECT from all proxy users	2	Yes	4.20
Revoke all object privileges from all proxy users	2	Yes	5.1
Revoke EXECUTE on DBMS_JOB from PUBLIC	2	Yes	5.13
Revoke EXECUTE on DBMS_LOB from PUBLIC	2	Yes	5.14
Revoke EXECUTE on UTL_FILE from PUBLIC	2	Yes	5.15
Revoke EXECUTE on UTL_HTTP from PUBLIC	2	Yes	5.16
Revoke EXECUTE on UTL_SMTP from PUBLIC	2	Yes	5.17
Revoke EXECUTE on UTL_TCP from PUBLIC	2	Yes	5.18
Revoke EXECUTE on UTL_INADDR from PUBLIC	2	Yes	5.19
Revoke EXECUTE on DBMS_LDAP from PUBLIC	2	Yes	5.20
Revoke EXECUTE on DBMS_JVM_EXP_PERMS from PUBLIC	5	No	5.21
Revoke INDEX privileges from PUBLIC on SYS tables	5	No	5.22
Revoke INDEX privileges from PUBLIC on SYSTEM tables	5	No	5.23
Revoke INDEX privileges from PUBLIC on user tables	4	No	5.24

Revoke EXECUTE on KUPP$PROC from PUBLIC	5	No	5.25
Revoke EXECUTE on INITJVMAUX from PUBLIC	5	Yes	5.26
Revoke EXECUTE on DBMS_SYS_SQL from PUBLIC	5	Yes	5.27
Revoke EXECUTE on DBMS_XMLQUERY from PUBLIC	2	Yes	5.28
Revoke EXECUTE on DBMS_JAVA from PUBLIC	2	No	5.29
Revoke EXECUTE on DBMS_JAVA_TEST from PUBLIC	2	Yes	5.30
Revoke EXECUTE on DBMS_UTILITY from PUBLIC	2	No	5.31
Revoke EXECUTE on DBMS_XMLSTORE from PUBLIC	2	No	5.32
Revoke EXECUTE on DBMS_XMLSAVE from PUBLIC	2	No	5.33
Revoke EXECUTE on DBMS_AW from PUBLIC	2	No	5.34
Revoke EXECUTE on DBMS_STATS from PUBLIC	2	No	5.35
Revoke EXECUTE on WMSYS.LT from PUBLIC	4	No	5.36
Revoke EXECUTE on DBMS_XMLGEN from PUBLIC	2	Yes	5.37
Revoke EXECUTE on DBMS_XSLPROCESSOR from PUBLIC	2	No	5.38
Revoke EXECUTE on DBMS_LDAP_API_FFI from PUBLIC	2	No	5.39
Revoke EXECUTE on HTTPURITYPE from PUBLIC	2	Yes	5.40
Revoke EXECUTE on MDSYS.SDO_NET from PUBLIC	2	No	5.41
Revoke EXECUTE on DBMS_SCHEDULER from PUBLIC	2	Yes	5.42
Revoke EXECUTE on DBMS_IJOB from PUBLIC	2	No	5.43
Revoke EXECUTE on DBMS_RLS from PUBLIC	3	No	5.44
Revoke EXECUTE on DBMS_RLS from users	3	No	5.45
Revoke EXECUTE on DBMS_FGA from PUBLIC	5	No	5.46
Revoke EXECUTE on DBMS_FGA from users	5	No	5.47
Revoke EXECUTE on DBMS_REDACT from PUBLIC	5	No	5.48
Revoke EXECUTE on DBMS_AUDIT_MGMT from PUBLIC	5	No	5.61
Revoke EXECUTE on DBMS_DBWS from PUBLIC	2	Yes	5.63
Revoke EXECUTE on DBMS_ORAMTS from PUBLIC	2	Yes	5.64
Revoke EXECUTE on DBMS_OBFUSCATION_TOOLKIT from PUBLIC	2	Yes	5.65
Revoke EXECUTE on DBMS_CRYPTO from PUBLIC	2	Yes	5.66
Revoke EXECUTE on DBMS_RANDOM from PUBLIC	2	Yes	5.67
Revoke EXECUTE on DBMS_ADVISOR from PUBLIC	2	Yes	5.68
Revoke EXECUTE on DBMS_BACKUP_RESTORE from PUBLIC	5	Yes	5.69
Revoke EXECUTE on DBMS_AQADM_SYSCALLS from PUBLIC	5	Yes	5.70
Revoke EXECUTE on DBMS_REPCAT_SQL_UTL from PUBLIC	5	Yes	5.71
Revoke EXECUTE on DBMS_STREAMS_ADM_UTL from PUBLIC	5	Yes	5.72
Revoke EXECUTE on DBMS_STREAMS_RPC from PUBLIC	5	Yes	5.73
Revoke EXECUTE on DBMS_PRVTAQIM from PUBLIC	5	Yes	5.74
Revoke EXECUTE on DBMS_FILE_TRANSFER from PUBLIC	4	Yes	5.75
Revoke EXECUTE on WWV_DBMS_SQL from PUBLIC	5	Yes	5.76
Revoke EXECUTE on WWV_EXECUTE_IMMEDIATE from PUBLIC	5	Yes	5.77
Revoke SELECT from PUBLIC on G/V_$SQL	5	No	5.78
Revoke SELECT from PUBLIC on G/V_$OPEN_CURSOR	5	No	5.79
Revoke SELECT from PUBLIC on G/V_$SQLAREA	5	No	5.80
Revoke SELECT from PUBLIC on G/V_$SQLAREA_PLAN_HASH	5	No	5.81
Revoke SELECT from PUBLIC on G/V_$SQLSTATS	5	No	5.82
Revoke SELECT from PUBLIC on G/V_$SQLSTATS_PLAN_HASH	5	No	5.83
Revoke SELECT from PUBLIC on G/V_$SQLTEXT	5	No	5.84
Revoke SELECT from PUBLIC on G/V_$SQLTEXT_WITH_NEWLINES	5	No	5.85
Revoke SELECT from PUBLIC on G/V_$SQL_MONITOR	5	No	5.86
Revoke SELECT from PUBLIC on G/V_$SQL_SHARED_MEMORY	5	No	5.87

Revoke SELECT from PUBLIC on G/V_$DB_OBJECT_CACHE	5	No	5.88
Revoke SELECT from PUBLIC on DBA_HIST_SQLTEXT	5	No	5.89
Revoke SELECT from PUBLIC on WRH$_SQLTEXT	5	No	5.90
Revoke READ access on directories from PUBLIC	3	No	5.91
Revoke WRITE access on directories from PUBLIC	3	No	5.92
Revoke UPDATE on SYS.USER$ from users	5	No	5.95
Revoke DELETE on SYS.USER$ from users	5	No	5.96
Revoke INDEX from users on other users' tables	3	No	5.102
Revoke INSERT on SYS.USER$ from users	5	No	5.103
Revoke EXECUTE on DBMS_PDB_EXEC_SQL from XBD	3	No	5.104
Revoke EXECUTE on DBMS_SYS_SQL from users	5	No	5.105
Revoke INSERT on SYS.SYSAUTH$ from users	5	No	5.106
Revoke UPDATE on SYS.SYSAUTH$ from users	5	No	5.107
Revoke DELETE on SYS.SYSAUTH$ from users	5	No	5.108
Revoke INSERT on SYS.OBJAUTH$ from users	5	No	5.109
Revoke UPDATE on SYS.OBJAUTH$ from users	5	No	5.110
Revoke DELETE on SYS.OBJAUTH$ from users	5	No	5.111
Revoke EXECUTE on LTADM from PUBLIC	3	Yes	5.112
Drop PUBLIC database links and recreate as private	2	Yes	6.0