

General Data Protection Regulation

Kontrola bezpečnostních nastavení a bezpečnostní politika
pro technologie Oracle

David Krch
Principal Consultant, Expert Services
Oracle Consulting

Září 2016



ORACLE

ORACLE[®]
CONSULTING

Kontrola bezpečnostních nastavení pro technologie Oracle

Oracle Database | Oracle WebLogic | Oracle Service Bus

- Rychlé a přehledné zhodnocení
- Identifikace **chybných bezpečnostních konfigurací** technologií Oracle
 - Technologická bezpečnost
 - Klíčová pro celkovou bezpečnost systému
 - Eliminace možných chybných konfigurací
 - CVSS scoring identifikovaných rizik
 - Doporučení
 - Lze využít jako podklad pro navazující službu **Standardizace Bezpečnosti produktů Oracle**
- Službu lze doplnit podrobným **auditem přidělených uživatelských oprávnění**
 - Identifikace účtů se silnými oprávněními, úroveň přístupu k datům
 - Přehled o **zabezpečení aplikačních dat**

Kontrola bezpečnostních nastavení pro technologie Oracle

Výstupy

- Dokument
 - identifikovaná rizika
 - jejich CVSS scoring
 - doporučení
- Prezentace
 - podrobná prezentace výsledků auditu

Audited Area	Evaluation	Score	Risk Treatment priority	Risk Treatment
Installed Components	Risk Exists	4.6	Medium	Uninstall unnecessary components
Security patches	Risk Exists	7.1	High	Apply latest security patches, establish procedures for security patches management
Authentication	OK	0.0	N/A	N/A
User password	OK	0.0	N/A	N/A
Password management	OK	0.0	N/A	Use case sensitive passwords, setup password function for XXX_TEMP profile
SYSDBA and SYSOPER roles	OK	0.0	N/A	Check if user XXX needs SYSDBA privilege
Batch task securing	Risk Exists	4.3	High	Implement secure password store
Database dictionary securing	OK	0.0	N/A	N/A
Database privileges	Risk Exists	4.0	Medium	RMAN account shouldn't have a DBA role, verify the usage of OPSSXXXX account,XXXX has excessive privileges
Public privileges	OK	0.0	N/A	N/A
Run-time facilities securing	OK	0.0	N/A	N/A
Oracle Listener securing	Risk Exists	1.7	Low	Implement admin restrictions
External Procedures securing	Risk Exists	4.6	Medium	Check Extproc usage
TNS Listener Poison Attack	Risk Exists	7.5	High	Implement Oracle recommendation for listeners
Database Auditing	Risk Exists	4.6	Medium	Enable audit: AUDIT_SYS_OPERATIONS

Bezpečnostní politika pro technologie Oracle

- Podrobný bezpečnostní standard pro technologie Oracle
 - Obecná bezpečnostní politika je obvykle málo konkrétní
- Upraven na základě požadavků a situace konkrétního zákazníka, zapracovává
 - Naše zkušenosti
 - Stávající normy a postupy zákazníka
 - Národní, Industriální a jiné požadavky – PCI-DSS, ZoKB, EU GDPR
- Implementuje víc úrovní zabezpečení (např. ZKB, non-ZKB, PCI-DSS)
- Včetně **stanovení bezpečnostních požadavků na dodavatele pro technologie Oracle**
 - Standard má **externí a interní část**
 - Externí slouží pro definici požadavků na řešení dodavatelů

Bezpečnostní standard pro Oracle Database

Co zahrnuje – 2 dokumenty, 60 stránek, 70+ kontrolovaných parametrů

Obsah.....	iii	5.2.5 Účty aplikací.....	31
Seznam Tabulek.....	v	5.2.6 Servisní účty aplikací.....	32
Seznam Obrázků.....	v	5.2.7 Správa databázových uživatelů.....	32
1. Úvod.....	6	5.2.8 Aplicační schémata.....	33
1.1 Cíle dokumentu.....	6	5.2.9 Standardní tabulky.....	33
1.2 Formátování dokumentu.....	7	5.3 Autentizace uživatelů.....	34
2. Provozované databáze.....	8	5.3.1 Pravidla pro přístupy uživatelů.....	34
2.1 Podporované verze.....	8	5.3.2 Pravidla pro nastavení hesel.....	35
2.2 Podpora Oracle.....	8	5.3.3 Verifikační funkce pro kontrolu hesel.....	36
2.2.1 Stav podpory.....	8	5.4 Autentizace efední vřetvy.....	38
2.2.2 Aktualizace.....	8	5.5 Databázová oprávnění.....	39
3. Základní kritéria zabezpečení databáze Oracle.....	9	5.5.1 Účty.....	39
4. Integrita.....	10	5.5.2 Databázové role.....	39
4.1 Certifikace.....	10	5.5.3 Objektová oprávnění.....	39
4.2 Instalace.....	10	5.5.4 Objektová oprávnění pro External Network Services – Fine-Grained Access.....	40
4.3 Vytvoření databáze.....	11	5.5.5 Systémová oprávnění a databázové role.....	42
4.4 Aplicační schémata.....	11	5.5.6 Data dictionary.....	45
4.5 Nezávěrečné databázové a aplicační vřetvy.....	11	5.5.7 Role DBA.....	45
4.6 Aplikace bezpečnostních oprav.....	11	5.6 Databázové objekty a sdílené atributy.....	46
4.6.1 Bezpečnostní balíčky SPU/PSU a Security Alerts.....	11	5.6.1 Public synonyma.....	46
4.6.2 Četnost a termíny vydávání, proces notifikace a validace procesu.....	12	5.6.2 Databázový link.....	46
4.6.3 Proces posouzení relevance SPU/PSU a Security Alerts a validace procesu.....	13	5.6.3 Vazba na operační systém.....	46
4.6.4 Plánování a nasazení SPU/PSU.....	14	5.7 Ochrana sennitvích dat.....	47
4.6.5 Plánování a nasazení Security Alert.....	15	5.8 Oprávnění k systémovým funkcím.....	48
4.6.6 Nově instalované systémy.....	16	5.9 Java security.....	48
4.8 Aplikace Release a Patch Set Management pro Oracle RDBMS.....	16	6. Nastavení databázových instancí.....	49
4.8.1 Release databáze a Patch Set.....	16	7. Oracle Network.....	50
4.8.2 Určení Termínů vydávání Release a Patch Set a ukončení support, validace politiky support.....	17	7.1 Oracle Listener.....	50
4.8.3 Nasazení Release.....	17	7.2 Jmenné služby.....	50
4.8.4 Nasazení Patch Set.....	17	7.3 Šifrování dat přenášených po síti.....	50
4.9 Integrita Oracle SW.....	19	7.4 Oracle Enterprise Manager.....	51
4.10 Bezpečnost skriptů.....	20	8. Audit.....	52
4.11 Bezpečnost práce na sdílených unixových serverech.....	20	9. Pravidla nasazování změn v databázi pro potřeby aplikací.....	53
4.12 Bezpečnost log a trace souborů.....	21	9.1 Realizace systémových změn.....	53
4.13 Zálohování Oracle SW.....	22	9.1.1 Nástroje pro nasazování systémových změn.....	53
4.14 Integrita databázových souborů Oracle.....	23	9.1.2 Pravidla pro aplicační skripty k nasazení systémových změn.....	53
4.14.1 Databázové soubory.....	23	9.2 Realizace aplicačních změn.....	54
4.14.2 Zálohování databázi Oracle.....	24	9.2.1 Pravidla pro nasazování aplicačních změn.....	54
4.14.3 Recovery procedury.....	24	9.2.2 Postup pro nasazování aplicačních změn vyžadujících systémovou změnu.....	54
4.15 Oddělení „testovacích, vývojových a produkčních prostředí“.....	25	Příloha A – formulář pro provedení aplicační změny v databázi.....	55
4.16 Klonování pro účely testů nebo vývoje.....	25		

ORACLE

ORACLE

Framework pro zabezpečení pravidelného monitoringu

- **Aplikace umožňují sledovat a evidovat soulad se standardem**

- Vazba na konkrétní pravidla standardu
- Definovaná pravidla pro Oracle DB a MW
- Porovnání s předchozím stavem
- Identifikace chyb z pohledu předepsané konfigurace i oprávnění
- Evidence nálezů, možnost jejich klasifikace

<ul style="list-style-type: none">• Oracle Database<ul style="list-style-type: none">– Exists (SQL)– Not Exists (SQL)– Profile Parameters– Oracle Net Parameters– Oracle TNS Listener Parameters– Privileges and ownership of files specified by SQL– Privileges and ownership of files– Shell command	<ul style="list-style-type: none">• Oracle WebLogic Server<ul style="list-style-type: none">– WLST Attribute Equal– WLST Attribute Not Equal– WLST Attribute in Range/not in Range– Privileges and ownership of files specified by WLST attribute– WLST Script– Privileges and ownership of files– Shell command
---	--

- **Správa nálezů a výjimek**

- Jednotlivé nálezy lze dále zpracovávat
- Díky správě výjimek již v následných auditech řešíte jen nové nálezy

- **Lokální vývoj a podpora, provozováno ve významných bankách v ČR**

Oracle Database Security Compliance Report

General Info

DBNAME	Db, Version	PSU	Oldest Audit Date	Hostname	Platform	PCI Mode	Captured Date
orcl	12.1.0.2.0	-- NONE --	27.11.2013 00:06:31	db12c.cz.oracle.com	Linux x86 64-bit	No	16.12.2014 13:07:50

Script Info

Standard Version	Config Download Date	Script Version
1.1	16.12.2014 13:06:33	1.20141216

Report Summary

Chapter Name	Cust. Compliance
3.2.1.7 Mandatory OS groups exist - dba, oinstall, oper	PASSED
3.8.1.4 Oracle Software Integrity - write permission for others not allowed	FAILED
3.8.1.5 Files in ORACLE_HOME must be owned by oracle:dba	PASSED
3.8.1.6 File permissions of the redundant files in \$ORACLE_HOME/bin/ (oracleO, tnslsnr0, ...) have to be set to 0000 when no patch rollback is necessary anymore.	FAILED
3.11.1.2 Privileges on DIAGNOSTIC_DEST/diag and its subdirectories	PASSED
3.11.1.1 Directories background_dump_dest, user_dump_dest and core_dump_dest must be owned by oracle:dba with permissions rwxr-x---	PASSED
3.11.1.3 Privileges on AUDIT_FILE_DEST files - not for Unified Auditing	PASSED
	PASSED
	FAILED
	PASSED
	PASSED
	PASSED

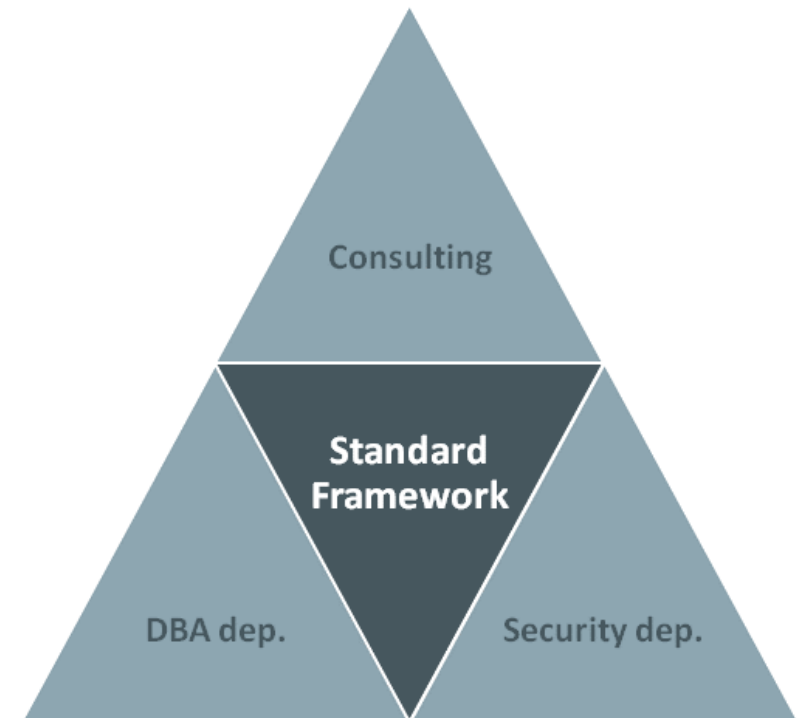
Detailed Report - Failed Items - Selected Section

3.8.1.4 - Oracle Software Integrity - write permission for others not allowed

<input type="checkbox"/>	Edit	Privileges	Owner	Group	Name	Exception, Task, Comment	Cust. Compliance
<input type="checkbox"/>		-rwxrwxrwx	oracle	oinstall	/u01/app/oracle/product/12.1.0.2/dbhome_1/javavm/doc/readme.txt	Ex: Broader privileges required by Application ABC (DKRCH/30.11.2015)	PASSED(ex)
<input type="checkbox"/>		-rwxrwxrwx	oracle	oinstall	/u01/app/oracle/product/12.1.0.2/dbhome_1/javavm/doc/javadoc.zip		FAILED
<input type="checkbox"/>		-rwxrwxrwx	oracle	oinstall	/u01/app/oracle/product/12.1.0.2/dbhome_1/rdbms/doc/README_rdbms.htm		FAILED

Dodávka

- Kontrola bezpečnostních nastavení
 - Rychlá jednorázová kontrola
 - Základní **podklad pro standardizaci**
- Bezpečnostní politika
 - Vstupem jsou **bezpečnostní směrnice** organizace
 - Standard Oracle je upraven na základě požadavků a **situace konkrétního zákazníka**
- Framework pro zabezpečení pravidelného monitoringu
 - Připraven na základě odsouhlasené Bezpečnostní politiky
 - Možná **integrace na SIEM řešení**



ORACLE®