ČESKÁ SPRÁVA SOCIÁLNÍHO ZABEZPEČENÍ
ÚSTŘEDÍ - SEKCE INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

Křížová 25, 225 08 Praha 5

STANDARD IMPLEMENTACE DATABÁZE ORACLE

Česká Správa sociálního zabezpečení

Datové úložiště

Připraveno firmou Oracle

Autor: Petr Kysela, Vít Hlaváček

Identifikace akce:

Datum vytvoření: 14.9.2007

Datum aktualizace: 17.11.2015

Verze: 1.12

Schváleno:

Zákazník

Zástupce Oracle Services

Záznam změn

Datum	Autor	Verze	Popis změny
4.9.2007	Petr Kysela	0.1	Nový dokument
5.9.2007	Vít Hlaváček	0.5	Aktualizace
4.10.2007	Petr Kysela	0.6	Finalizace
7.11.2007	Vít Hlaváček	1.10	Zapracování připomínek ČSSZ
16.7.2015	Roman Krejčík, Oracle	1.11	Revize pro Oracle 12c Release 1
29.7.2015	Radovan Beneš	1.12	Aktualizace

Revize

Jméno	Funkce

Obsah

1. Terminologie

1.1 Terminologie

Tato kapitola podává přehled terminologie a zkratek používaných dále v tomto dokumentu.

Zkratka/Termín	Význam
Databáze	Databáze je sada souborů uložených na disku obsahující data
Instance (databázová instance)	Instance je oblast sdílené paměti a souhrn běžících procesů pracujících s databází.
SGA (System Global Area)	Sdílená paměť, která je součástí databázové instance.
Datafile (databázový soubor)	Soubor obsahující data, který je součástí databáze jeden nebo více datových souborů tvoří tablespace
Redo log file	Žurnálový soubor databáze. Obsahuje informace o provedených operacích s daty pro potřeby obnovy stavu databáze
Schema	Databázeové objekty (tabulky, indexy, triggery, view atd.) patřící jednomu uživateli
Tablespace	Fyzický prostor databáze skládající se z jednoho nebo více datových souborů.
Segment	Fyzický objekt sloužící pro uložení dat. Odpovídá buď indexu nebo tabulce nebo partition.
Partition	Část tabulky nebo indexu.
<ORACLE_BASE>	Proměnná prostředí definující základní adresář „Optimal Flexible Architecture“.
<ORACLE_SID>	Proměnná prostředí definující název DB instance.
<ORACLE_HOME>	Proměnná prostředí definující adresář obsahující Oracle server software.
<db_name>	Hodnota inicializačního parametru databáze určující jméno databáze.
<version>	Verze Oracle sw, například 10.2.0.5, 11.2.0.3, 12.1.0.2… .
<ver>	Zkrácená verze Oracle sw, například 10204, 11203, 12102 ,....
RAC	Oracle Real Applications Clusters.

1.2 Formátování dokumentu

Odstavce obsahující závazné pravidlo jsou orámovány černou barvou.

Odstavce obsahující doporučení jsou orámovány šedivou barvou a pro text je použita kurzíva.

2. Úvod

Provoz datového úložiště ČSSZ je komplexní úloha, ke které je nutné přistupovat systematicky a metodicky. Součástí takového přístupu je i vypracování a dodržování standardů pro vytváření a vlastní provoz databází, které jsou součástí datového úložiště.

Tento Standard se zabývá provozem databáze Oracle v návaznosti na Standard databáze Oracle.

Cílem tohoto dokumentu je stanovit jasná doporučení z pohledu standardů pro provoz a zabezpečení databází Oracle v integrovaném informačním systému ČSSZ, který je zařazen jako prvek kritické informační infrastruktury podle zákona č. 181/2014 Sb.. Tím, že jednotlivá pravidla budou k dispozici již ve fázi vzniku nových projektů, dojde nejen k celkovému zvýšení standardizace a úrovně bezpečnosti provozu databází Oracle, ale též k úsporám vyplývajícím ze skutečnosti, že jednotlivá prostředí nebude nutné později měnit.

Současně provozovaná prostředí se mohou navrhovanému standardu přizpůsobovat postupně a to zejména při vhodných příležitostech, jako např. upgrade a instalace nových verzí SW, rozšíření kapacity diskového pole apod. Cílovým stavem je splnění požadavků *vyhlášky č. 316/2014 Sb.*

Dokument zohledňuje při standardizaci Oracle platformu IBM AIX, na které je datové úložiště implementováno.

3. Základní pravidla

Tento dokument navazuje na dokument upravující Standard databáze Oracle provozované v ČSSZ.

V IIS ČSSZ je koncepčně určena struktura instancí databází podle druhu dat, která jsou do nich ukládána. Jednotlivým aplikacím je pak v příslušné instanci zřízeno schéma podle požadavků příslušného projektu.

3.1 Konvence pro tvorbu jmen databází Oracle

Podle druhu dat a užití jsou vytyčeny tři okruhy databází:

Provozní data aplikací spravujících data klientů jsou v databázi IPA (Integrovaná Podpora aplikací) a INP (Integrované nárokové Podklady)

Zpracování dokumentů je soustředěno v databázích DMS (Document Management Systém), Archive (Content Manager on Demand) a ESS (spisová služba)

Data publikovaná na ePortal CSSZ obsahuje databáze POB.

Názvy databází obsahují maximálně 8 znaků. Název databáze obsahuje jméno databáze a určení prostředí (produkční, testovací a školící a integrační).

Názvy databází se tvoří ze jména DB a znaku určujícího prostředí. Název databáze je tvořen podle pravidla:

[jméno databáze] [prostředí] přičemž "jméno database" nabývá hodnot {IPA, INP, DMS, Archive, ESS, POB, Serv} a "prostředí" nabývá hodnot {p (produkce), t (testovací), i (integrační)}.

Vzhledem k historicky vzniklým drobným odchylkám od uvedeného pravidla jsou dlouhodobě používaná jména databází uvedena výčtem:

Konkrétní názvy databází v produkčním prostředí jsou: IPA, INP, DMAP, ESS, ARCHIVE, POB, SERV

Konkrétní názvy databází v testovacím prostředí jsou: TIPA, TINP, DMAT, TESS, ARCHIVET, TPOB, TSERV

Konkrétní názvy databází v integračním prostředí jsou: IPAI, INPI, DMAI, ESSI, ARCHIVEI, POBI,

3.2 Konvence pro tvorbu jmen databázových instancí

Jméno databázové instance je tvořeno podle konvence :

[název databáze] [n] přičemž „název databáze“ je určen v předcházejícím odstavci a [n] je číslo od 1 do 9 určující číslo instance v RAC

4. Diskový subsystém

Pro jmenné konvence a konfiguraci diskového subsystému definujeme následující pravidla.

4.1 Umístění Oracle SW a databází

Oracle software ani aplikační software nesmí být instalován do systémové (rootvg) diskové skupiny (volume group) logical volume manageru. Pro provoz databází je nutné, aby diskové skupiny pro vlastní soubory databáze a diskové skupiny pro archivní redology, byly konfigurovány samostatně. (umístěné na různých diskových skupinách).

Pro potřeby uložení dat aplikace (databázová disková skupina) je možné použít více diskových skupin, pokud je to z hlediska aplikace výhodné.

Volume (disk) group	Použití
rootvg	Určena pouze pro SW
oradatavg[r]XX	Datové soubory databáze Znak „r“ je použit v případě umístění souborů na raw devices (raw devices platí pouze pro databáze do verze 10.2.0).
oraarchvg[r]YY	Archivní logy databáze (platí pouze pro databáze do verze 10.2.0)

Při vytváření diskové skupiny je její jméno tvořeno ze základu `vg resp. vgr` a dvoumístného indexu určujícího její pořadové číslo.

Pro každou provozovanou databázi je třeba mít nejméně dvě diskové skupiny

- pro datové soubory
- pro archivní logy

Pro každý server je nutné použít alespoň jednu diskovou skupinu pro instalaci Oracle SW.

Uvedená pravidla platí pro umístění databázových souborů mimo ASM. Pro Oracle ASM jsou využity standardní systémově přidělená jména diskových zařízení (`/dev/rhdisk[n]`). Logical Volume Manager Není v tomto případě využit. Oracle doporučuje používat některou z multipath technologií dodavatele OS ve spojení s Oracle ASM.

.

5. Souborové systémy

5.1 Uložení souborů Oracle

Tabulka ukazuje možné uložení jednotlivých typů souborů Oracle v ČSSZ.

Soubor	Uložení pro single instanci	Uložení pro Oracle RAC
Instalace Oracle SW	Filesystém	Filesystém
Databázové soubory	Filesystém/Raw devices/Oracle ASM	Raw devices/Oracle ASM
Password file	Filesystém	Filesystém/Oracle ASM
Spfile	Filesystém	Raw devices/Oracle ASM
Trasovací soubory	Filesystém	Filesystém
CRS a OCR soubory	N/A	Raw devices/Oracle ASM

Filesystém může být na lokálním disku resp. na příslušném diskovém poli. Pro všechny souborové systémy použité pro databáze bude použit žurnálový souborový systém JFS2. Souborové systémy určené pro databázové soubory nesmí být používány pro data jiného typu (aplikační data musí být v jiných souborových systémech).

5.2 Optimal Flexible Architecture

Oracle po dlouhou dobu (více než 10 let) používá pro provoz databází standardní způsob umístění jednotlivých souborů a adresářů v souborovém systému serverů. Tento standard je nazýván Optimal Flexible Architecture (OFA) a vznikl ze zkušeností s provozem databází u mnoha zákazníků.

Rozmístění souborových systémů je navrženo tak, aby umožňovalo bezproblémový běh více databází v jednom operačním systému a to včetně možnosti provozovat souběžně více verzí Oracle server software.

Oracle Server software je pro každou verzi / patchset instalován do vlastního souborového systému – ORACLE_HOME . Všechny instalace mají společný souborový systém – ORACLE_BASE , ve kterém jsou umístěné společné soubory (např. oraInventory) či odkazy na ně.

Pro prostředí zákazníka verze Oracle 10.2.0 a nižší		
Adresář	**Popis**	**Mount Point**
/oh10g		
/oh10g	<ORACLE_BASE>	1x pro server
/oh10g/product	Adresář pro instalace Oracle software	
/oh10g/product/X.X.X	Adresář pro instalace Oracle software pro danou verzi	1x pro každou verzi
/oh10g/product/X.X.X/dbhome_X	<ORACLE_HOME> - instalační adresář Oracle software	
/oradataXX/oracle	Adresář pro umístění struktury databázových souborů (filesystem)	
/oradataXX/oracle/<DB_NAME>	Adresář pro databázové soubory dané databáze (filesystem)	1x pro každou databázi
/oh10g/admin	Adresář pro administrativní soubory	
/oh10g/admin/<DB_NAME>	Adresář pro administrativní soubory dané databáze	1x pro každou databázi
/archive1/<DB_NAME>/oraarch	Adresář pro archivní logy dané databáze (filesystem)	
/oh10g/admin/<DB_NAME>/adump	Adresář pro auditní logy dané databáze	
/oh10g/admin/<DB_NAME>/bdump	Adresář pro trace soubory background procesů dané databáze	

Pro prostředí zákazníka verze Oracle 10.2.0 a nižší		
Adresář	**Popis**	**Mount Point**
/oh10g/admin/<DB_NAME>/cdump	Adresář pro core dump soubory dané databáze	
/oh10g/admin/<DB_NAME>/scripts	Adresář pro skripty pro vytvoření dané databáze	
/oh10g/admin/<DB_NAME>/pfile	Adresář pro konfigurační soubory dané databáze	
/oh10g/admin/<DB_NAME>/udump	Adresář pro trace soubory uživatelskýchprocesů dané databáze	

Pro Oracle RAC prostředí zákazníka verze 11.2.0 a vyšší (uložení databázových souborů výhradně do Oracle ASM)		
Adresář	**Popis**	**Mount Point**
/oracle		
/oracle	<ORACLE_BASE>	1x pro server
/oracle/product	Adresář pro instalace Oracle software	
/oracle/product/X.X.X	Adresář pro instalace Oracle software pro danou verzi	1x pro každou verzi
/oracle/product/X.X.X/dbhome_X	<ORACLE_HOME> - instalační adresář Oracle software	
/oracle/admin	Adresář pro administrativní soubory	
/oracle/admin/<DB_NAME>	Adresář pro vytvářecí skripty a logy dané databáze	1x pro každou databázi
/oracle/admin/<DB_NAME>/scripts	Adresář pro skripty pro vytvoření dané databáze	
/oracle/diag	ADR adresář pro administrativní soubory Oracle Server software	Platí nejen pro databáze.
/oracle/diag/rdbms/{db_name}	Adresář pro administrativní soubory databáze	1x pro každou databázi

Pro Oracle Automatic Diagnostic Repository (ADR) je k dispozici ADRCI utilita, která umožňuje prohlížení i čištění [PURGE] obsahu souborového repository.

Detailní popis struktury adresářů ADR je nad rámec tohoto dokumentu. Struktura adresářů je vytvářena automaticky při spouštění dané softwarové komponenty a je popsána v dokumentaci k dané verzi Oracle Server.

5.3 Oddělení aplikace od databáze

Aplikace nesmí žádným způsobem zasahovat do souborových systémů, Oracle ASM, nebo raw devices pro provoz využívaných databází.

Soubory a programy aplikace nesmí být instalovány do souborových systémů obsahujících Oracle SW, či soubory databáze, nebo ostatní soubory nezbytné pro běh databáze (souborový systém s inicializačním souborem DB, archivní logy…) a nesmějí vyžadovat oprávnění zápisu do těchto souborových systémů.

Pokud je v databázi nastaven parametr `utl_file_dir` nesmí žádný z adresářů uvedených v tomto parametru být v souborových systémech používaných pro databázi či Oracle software.

5.3.1 Instalace nové verze Oracle SW

Instalace nové verze Oracle SW vyžaduje připojení nového souborového systému do adresáře /oracle/product/X.X.X. Před upgrade databáze/databází se musí pro každou DB provést a zkontrolovat záloha.

5.4 Adresářová struktura pro databáze

Soubory databáze jsou uloženy v jednotné struktuře umožňující efektivně využívat možností diskových polí.

Pokud databáze využívá raw devices nedoporučujeme využívat symbolické odkazy na jednotlivé raw devices.

Nedoporučujeme kombinovat datové soubory v raw devices (resp. Oracle ASM) s datovými soubory v souborovém systému v jedné databázi. (Pozn. pro Oracle RAC může mít nedodržení tohoto pravidla fatální následky vzhledem k tomu, že v architektuře není implementován sdílený cluster filesystem - jeho funkci nahrazuje Oracle ASM.)

5.5 Konvence pro pojmenovávání databázových souborů / filesystém

Databázové soubory se pojmenovávají malými písmeny shodně s jménem tabulkového prostoru databáze jehož jsou součástí, k jménu souboru se přiřazuje minimálně dvoumístný index s číslem souboru. Standardní příponou souboru je **`dbf`** pro databázové soubory, **`ctl`** pro řídící soubory, **`log`** pro online a **`arc`** pro archivní redology.

Příklady:

Tabulkový prostor / typ souboru ve filesystému	Příklad jména souboru
SYSTEM	`system01.dbf`
3. řídící soubor DB	`control03.ctl`
druhý onlile redolog ze čtvrté skupiny	`redo04_02.log`

5.6 Konvence pro pojmenovávání databázových souborů / raw devices

Logical volumes pro raw device (maximum 11 znaků):

{lv}`{identifikace_aplikace}`{tablespace_name}{index}

kde

lv: prefix pro logical volume pro primární devices

`{identifikace_aplikace}`: jednoznaková identifikace databáze projektu

{tablespace_name}: zkrácený název tablespace – maximum 6 znaků

{index} … dvouciferné pořadové číslo pro datafile 01, 02 …

Příklady:

Tabulkový prostor / typ souboru	Příklad jména souboru
SYSTEM	lvnsystem01

5.7 Konvence pro pojmenovávání archivních redologů

Pro archivní logy databáze je jmenná konvence definována inicializačním parametrem databáze `log_archive_format` jehož hodnota je tvořena z jména databáze takto:

```
<db_name>_%t_%S.arc
```

Pro databáze od verze 10g je formát obohacen o číslo inkarnace (resetlogs id):

```
<db_name>_%r_%t_%S.arc
```

5.8 Konvence pro použití ASM

ASM je preferovaný systém pro uložení databázových souborů. Pro každý server je použita jedna instance ASM. Pro každou databázi jsou v ASM definovány dvě diskové skupiny. Jedna pro datové soubory a on-line redo log soubory, druhá pro flash recovery area.

Konvence pro názvy diskových skupin ASM je následující:

XXXX_YYY

kde XXXX je název databáze a YYY je označení účelu:

- DB – datové soubory a on-line soubory
- ARCH – flash recovery area
- LOB – historická data, nestrukturovaná data

Struktura prostorů pro uložení souborů je následující:

+DG/oradata/FF

kde + je označení kořene v ASM

DG je název diskové skupiny

FF je jméno databázového souboru podle konvencí pro názvy databázových souborů.

5.9 Velikosti souborů

Pro soubory databáze nesmí být překročena maximální velikost souboru (platformě specifická pro jednotlivé typy fs) `maxfsize - 2*db_block_size`. Při definici velikosti databázových souborů, které mají povoleno se zvětšovat (`autoextend on`) musí být definován také parametr určující maximální velikost souboru (`maxsize`).

Součet maximálních velikostí datových souborů musí být menší než je velikost souborového systému na kterém se datové soubory nacházejí.

6. Neprodukční prostředí

Pro kvalitní provoz jakéhokoliv systému je nutné zabezpečit velké množství činností, které nemají přímou souvislost s vlastním provozem. Jedná se především o vývoj nových aplikací a modulů, opravy stávajících aplikací, školení uživatelů, testování vyvinutých kódů, testování provozních postupů, pilotní provoz. Pro uvedené činnosti je nutné zajistit odpovídající prostředky.

Z výše uvedeného vyplývá jasné doporučení na realizaci jak vývojového a testovacího, tak školícího prostředí. Tato prostředí se vždy od produkčního prostředí liší. Dále jsou uvedena obecná pravidla pro realizaci zmiňovaných prostředí.

6.1.1 Pravidla pro realizaci neprodukčních prostředí

6.1.1.1 Vývojové prostředí

- Vývoj by měl probíhat na stejné platformě jaká je použita na produkčním prostředí
- Je potřeba používat stejné verze software jako na produkčním prostředí. Jedná se zejména o verze:
    - Databáze
    - Aplikačního serveru
    - Operačního systému

6.1.1.2 Testovací prostředí a Integrační prostředí

Testovací prostředí může být určeno k různým účelům a proto může být jeho realizace různá.

Pro realizaci testovacího prostředí je potřeba vždy dodržet následující pravidla:

- Testovací prostředí musí být realizované na stejné platformě jako produkční prostředí
- Je potřeba používat stejné verze software jako na produkčním prostředí. Jedná se zejména o verze:
    - Databáze
    - Aplikačního serveru
    - Operačního systému

Dle účelu prostředí je nutné zachovat následující charakteristiky:

- Pro technické testovací prostředí je nutná shoda řešení:

- Vysoké dostupnosti
- Zálohování
- Disaster Recovery

- Pro integrační testovací prostředí je nutná shoda řešení:
  - Vysoké dostupnosti
- Pro systémové testovací prostředí je nutná shoda řešení:
  - Vysoké dostupnosti
  - Zálohování
  - Disaster Recovery
- Pro akceptační testovací prostředí je nutná shoda řešení:
  - Vysoké dostupnosti

Testovací prostředí může mít nižší kapacitní charakteristiky. Důležité je, aby bylo snadné aproximovat kapacitní charakteristiky produkčního prostředí z charakteristik testovacího prostředí.

6.1.1.3 Školící prostředí

Pro realizaci školícího prostředí je potřeba dodržet následující pravidla:

- Školící prostředí musí být realizované na stejné platformě jako produkční prostředí
- Je potřeba používat stejné verze software jako na produkčním prostředí. Jedná se zejména o verze:
  - Databáze
  - Aplikačního serveru
  - Operačního systému
- Školící prostředí nemusí mít stejnou architekturu jako produkční prostředí. Především se může lišit v řešení (nebo nemusí být vůbec řešeno):
  - Vysoké dostupnosti
  - Zálohování
  - Disaster Recovery

6.1.1.4 Realizace neprodukčních prostředí v ČSSZ

V současné době je v ČSSZ standardně v provozu Testovací prostředí a Integrační prostředí. Vývojové prostředí pro dodavatele ČSSZ neprovozuje. Samostatné prostředí pro systémové testování a akceptační testování ČSSZ neprovozuje.

Testovací prostředí (technické) je realizováno samostatně podle prostředí produkčního. Testovací prostředí plní současně i funkci prostředí Školícího.

Integrační prostředí je realizováno samostatně podle produkčního a testovacího prostředí. Integrační prostředí plní současně i funkci prostředí pro systémové testování.

.

7. Bezpečnostní standardy

Tato kapitola rozšiřuje standardy databází Oracle o problematiku zabezpečení databází.

Závazná pravidla jsou normou, kterou je třeba implementovat pro všechna prostředí. *Obsah bezpečnostních opatření, rozsah a jejich zavedení musí být v souladu s vyhláškou č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)***.** Doporučení se vztahují shodně na provoz databází v primárním i záložním středisku.

Pravidla bezpečnosti včetně opatření pro zajištění identifikace interního koncového uživatele jsou dále rozpracována v kapitole 8.

7.1 Výjimky z pravidel

V případě žádosti o výjimku je třeba vypracovat zdůvodnění s příslušnou dokumentací zaměřující se především na řešení nevýhod, které z dané výjimky vyplývají a návrhem jejich eliminace a podléhají schválení bezpečnostních útvarů ČSSZ

7.2 Provozované databáze

7.2.1 Podporované verze

V současné době je nejnovější verzí databázového serveru Oracle, který je k dispozici verze 12c Release 1. Z hlediska bezpečnosti, správy a zajištění podpory je vhodné, aby provozované databáze nižších verzí byly postupně migrovány na poslední prověřenou verzi. Před případnou migrací je třeba vzít do úvahy certifikace aplikace pro jednotlivé verze databázového serveru. V případech kdy certifikace není k dispozici, případně dosud o migraci nebylo rozhodnuto z jiných důvodů, je možné použít i dřívější verze. Volba konkrétní verze ovšem musí respektovat zájem v co největší míře sjednotit provozované databáze z hlediska verzí.

V ČSSZ jsou v datovém úložišti provozované následující verze databázového serveru Oracle:

Oracle 10g Release 2 – 10.2.0

Oracle 11g Release 2 - 11.2.0

Oracle 12c Release 1 - 12.1.0

7.2.2 *Aktualizace*

Aktuální informace o procesu aktualizací lze nalézt na internetových stránkách společnosti Oracle http://metalink.oracle.com v sekci Certify podsekci Certifications a Desupport Notices.

8. Základní kritéria zabezpečení databáze Oracle

8.1 Uživatel oracle operačního systému

8.1.1 UID a GID uživatele oracle

UID a GID pro uživatele Oracle musí být jednotné pro všechny U*NIX platformy. Obvyklé nastavení je `uid=102(oracle) gid=102(dba)` .

8.1.2 Domovský adresář uživatele oracle

Uživatel oracle – vlastník Oracle software je `/home/oracle`, tedy stejně jako pro ostatní neprivilegované uživatele operačního systému. Jako domovský adresář se **nepoužívá** adresář definovaný proměnnou `ORACLE_BASE`.

8.1.3 Nezávislost aplikace na nastavení prostředí uživatele oracle

Aplikace nesmí být závislá na nastavení prostředí uživatele oracle (prostředí definované v souboru `/home/oracle/.profile` a dalších souborech definujících prostředí, například standardní shell, `.profile.ora` , `.shrc`). Aplikační programy a skripty si musí zajistit nastavení prostředí potřebného pro jejich běh nezávisle na nastavení uživatele oracle.

8.1.4 Využití uživatele oracle operačního systému v aplikacích

Aplikační programy a skripty (s výjimkou skriptů řešících zálohování databáze) **nesmí žádným způsobem využívat uživatelský účet oracle**, nebo jeho ekvivalent, například převzetím identity pomocí příkazu `su - oracle`, také **nesmějí vyžadovat oprávnění dba** (členství ve skupině dba operačního systému, nebo jejím ekvivalentu).

8.1.5 Integrita

8.1.5.1 Certifikace

RDBMS Oracle musí být certifikován pro použití na daném operačním systému

Nejnižší povolená verze pro nově zaváděné nebo vytvářené aplikace je verze uvedená jako nejvyšší povolená pro provoz produkčních databází.

8.1.5.2 Instalace

- Instalovány jsou vždy pouze komponenty nutné pro provoz aplikace. Nepoužívané komponenty jsou odinstalovány. Aplikační dokumentace musí obsahovat seznam vyžadovaných komponent.
- O provedené instalaci a počáteční konfiguraci je vždy vytvořen protokol.
- Pro instalace nové verze Oracle SW je vytvářeno nové repository pro Oracle Installer. Instalace opravných patches a patch setů je prováděna do příslušného repository. Před instalací je vždy nutné provést zálohu Repository OUI.
- Jmenná konvence OUI a záloh se řídí dokumentem Standard Oracle10g v prostředí ČSSZ v aktuálně platné verzi.

8.1.5.3 Vytvoření databáze

- Zakládání databází je možné pouze pomocí SQL skriptů, nebo Oracle nástrojů pro vytváření databáze (DBCA). Do provozních prostředí ČSSZ nelze přenášet databáze v binární formě databázových souborů.

8.1.5.4 Aplikační schémata

- Zakládání aplikačních schémat a přidělení oprávnění k nim je možné pouze pomocí SQL skriptů.

8.1.5.5 Nezávislost databázové a aplikační vrstvy

- Dodavatel musí implementovat řešení tak, aby neexistovala závislost mezi databázovou a aplikační vrstvou.
- Databázovým administrátorům (DBA) musí být umožněno používat standardní nástroje a příkazy RDBMS Oracle pro správu databáze nezávisle na chování aplikační vrstvy.

8.1.5.6 Aplikace opravných programů

Oracle pravidelně vydává bezpečnostní opravy na databázový server.

8.1.5.6.1 Critical Patch Updates

- Uvolňování bezpečnostních balíčků v pravidelných intervalech je hlavní metodou zvyšování bezpečnosti produktů Oracle. Bezpečnostní balíčky jsou vydávány vždy v nejbližší úterní termín po 15.lednu, dubnu, červenci a říjnu. Aktuální informace lze nalézt na adrese http://www.oracle.com/technology/deploy/security/alerts.htm

8.1.5.6.2 Proces implementace bezpečnostních opravných balíčků

- Součástí dokumentace každé do provozu předávané databáze musí být způsob implementace Oracle CPU v rámci životního cyklu DB a aplikace.

Aplikace Critical Patch Updates do databázového prostředí je nutné zahájit bezprostředně po jejich zveřejnění. Na základě publikovaných datumů pro Critical Patch Updates lze proces implementace plánovat dopředu. Součástí tohoto procesu je též odstávka testovacího a provozního prostředí.

Doporučený harmonogram implementace Oracle CPU:

a) instalace patche do testovacího prostředí bude provedena nejpozději v termínu 60 dní po uvolnění Critical Patch Update

b) testování funkcionality v testovacím prostředí. Konkrétní rozsah testování doporučujeme vyhodnotit ve spolupráci s konzultanty Oracle. Obecně je třeba otestovat veškerou funkcionalitu.

c) vyhodnocení provozní způsobilosti v termínu nejpozději do 90 dní po uvolnění patche

d) instalace patche do produkčního prostředí nejpozději do 4 měsíců od vydání

- *Bezpečnostní patches – CPU –by měl být instalován do produkčního prostředí do 4 měsíců od vydání opravy.*

8.1.5.6.3 Implementace Patchsets

- Součástí dokumentace každé do provozu předávané databáze musí být způsob implementace Oracle patchsets v rámci životního cyklu DB a aplikace.

Doporučený harmonogram implementace Oracle patchsets:

a) pracovníci podpory Oracle v ČSSZ provedou vyhodnocení implementačního postupu včetně doporučení dodatečných one-off patches po 60 dnech od uvolnění patchsetu

b) instalace patches doporučených podle bodu a) do testovacího prostředí bude provedena v termínu 120 dní po uvolnění patchsetu

c) testování funkcionality v testovacím prostředí. Obecně je třeba otestovat veškerou funkcionalitu.

d) vyhodnocení provozní způsobilosti v termínu do 6 měsíců po uvolnění patchsetu

de) instalace patche do produkčního prostředí do 7 měsíců od vydání

- *Patchset – musí být instalován do produkčního prostředí do 7 měsíců od jeho vydání, pokud bude v průběhu testování uznán za způsobilý.*

8.1.5.7 Integrita Oracle SW

- Přístupová oprávnění v operačním systému na Oracle software musí být nastavena tak, aby zamezovala neoprávněným změnám Oracle SW.

- V případě potřeby instalovat na databázový server software třetích stran, musí být instalace odděleny, aby bylo možné odděleně řídit přístupová oprávnění.
- Funkčnost SW třetích stran nesmí být závislá na nastavení prostředí (.profile, apod.) vlastníka SW Oracle.
- Adresáře a soubory s instalací Oracle nesmí mít povolenu změnu pro uživatele others, tzn. maximální akceptovatelné oprávnění je „r-x". Modifikovat soubory Oracle SW včetně konfiguračních souborů serveru i databáze, Oracle Net (tnsnames.ora, sqlnet.ora, listener.ora, atd.), mohou pouze databázoví administrátoři.
- Adresáře a soubory s instalací Oracle vlastní oracle:dba. Výjimkou jsou soubory jejichž vlastníkem se při instalaci v rámci běhu skriptu root.sh stává uživatel root.

8.1.5.8 Bezpečnost skriptů

- Všechny skripty spouštěné mimo přímou kontrolu vlastníka Oracle SW, například prostřednictvím cronu, zálohovacích programů apod., musí být ve vlastnictví uživatele oracle a nesmí být zapisovatelné pro others.
- V případech kdy nelze vyloučit uložení hesla do skriptu musí mít takový skript odebrána jakákoli oprávnění pro others.

8.1.5.9 Bezpečnost práce na sdílených unixových serverech

- Z bezpečnostních důvodů je nepřijatelné připojovat se k instancím databází pomocí nástroje sqlplus případně staršího svrmgrl na sdílených unixových serverech s uvedením hesla účtu v čitelné podobě.
- Příklady nepřijatelného připojování
  - sqlplus <user>/<password>@<connect_identifier>
  - svrmgrl "connect <user>/<password>@<connect_identifier>":

- *Příklady doporučeného připojování*
  sqlplus /nolog
  sqlplus / as sysdba
  svrmgrl
- *V dialogovém řádku spuštěného nástroje se pak lze připojit k instanci databáze např. příkazem connect <user>/<password>@<connect_identifier>*

8.1.5.10 Bezpečnost log a trace souborů

- Adresáře použité pro background_dump_dest, user_dump_dest a core_dump_dest musí mít oprávnění nastavena podle schématu „oracle:dba rwxr-x---"
- log_archive_dest_* musí mít oprávnění nastavena podle schématu „oracle:dba rwxr-x---"

- Aplikace nesmí pracovat (čtení, zápis) se standardními logy vytvářenými databázovým serverem; například není dovoleno provádět zápis do alert log souboru databáze.

8.1.5.11 Zálohování Oracle SW

- Pro Oracle SW musí být implementována záloha na média mimo databázový server s minimální periodou 14 dní. Mimořádnou zálohu je třeba vždy provést před všemi změnami Oracle SW, například při implementaci patchsetu.
- Zálohy musí být zabezpečeny dle platného standardu pro OS.

8.1.5.12 Integrita databázových souborů Oracle

- Databázové soubory jsou vždy umístěny do samostatného umístění tvořeného
  - filesystémem
  - raw devices
  - ASM instancí
- Oprávnění pro dané umístění musí umožňovat čtení a modifikaci pouze vlastníku databázového SW a čtení pouze skupině dba. Ostatní uživatelé nesmí mít k databázovým souborům přístup.

8.1.5.12.1 Zálohování databází Oracle

- Přístup do zálohovacího software, a to jak pro zálohování, tak i pro obnovu dat, mají pouze oprávněné osoby. Jedná se o skupinu vybraných osob z databázových administrátorů a administrátorů OS.

- *Testování integrity databázových souborů standardně zabezpečuje Oracle Recovery Manager*

8.1.5.13 Oddělení „testovacích, vývojových a produkčních prostředí“

- Vývoj a testování aplikací musí probíhat odděleně od produkčního prostředí, a to tak, aby byl zcela vyloučen přístup na produkční prostředí.
  - Vývoj a testování nesmí být prováděn na serveru, na kterém je v provozu produkční prostředí.

- Aplikace resp. databáze s účelem „vývoj“ nebo „test“ nesmí přistupovat k produkčním databázím. Existence databázových linků mezi jednotlivými prostředími není povolena.

8.1.5.14 Klonování pro účely testů nebo vývoje

Pro vývojové nebo testovací databáze, které vzniknou jako klon databází produkčních je nutné zabezpečit:

a) změnu hesel u všech neuzamčených systémových účtů - odpovídá DBA. Seznam systémových uživatelů je v tabulce **Chyba! Nenalezen zdroj odkazů.**

b) změnu hesel aplikačních účtů

c)

Tabulka 8.1-1

Seznam systémových uživatelů
SYS
SYSTEM
OUTLN
TSMSYS
DIP
DBSNMP[1]
WMSYS
EXFSYS

8.1.5.15 Ad-hoc dotazy

Přístup do produčního prostředí pomocí ad-hoc dotazů mimo aplikační mechanismus není pro produční prostředí povolen vzhledem k riziku ovlivnění ostatních uživatelů.

8.1.6 Řízení přístupových oprávnění

K zabezpečení proti neoprávněnému přístupu k datům uloženým v databázi jsou přednostně určeny bezpečnostní prostředky databáze.

- Aplikace musí při své činnosti využívat určené prostředky tak, aby na úrovni databáze bylo možné identifikovat interního koncového uživatele a přiřadit mu odpovídající auditní záznamy.

Pro účely identifikace interního koncového uživatele je určen nástroj IBM Guardium

[1] Není-li využit pro služby OEM.

Identifikace aplikačního uživatele pomocí Application Event API

Tato metoda využívá Guardium Application Event API, které umožňuje definovat hranice mezi aplikačními uživateli v jednom spojení do DB (session). Toto API reaguje na specifické no-op (bez účinku) SQL dotazy do tabulky dual. Pomocí těchto SQL dotazů a parametru „GuardAppEvent„ aplikace ohraničí začátek a konec DB operací jednoho konkrétního uživatele. Parametr „GuardAppEvent:Start" zajistí spuštění příslušného programu přes Guardium API, který zaznamená průběh celé komunikace až po její ukončení pomocí parametru „GuardAppEvent:Released", nebo do ukončení spojení (session). Parametr „GuardAppEventUserName" obsahuje identifikátor uživatele a parametr „GuardAppEventType" obsahuje tříznakový kód aplikace ČSSZ.

Příklad syntaxe nastavení uživatele:

SELECT 'GuardAppEvent:Start', 'GuardAppEventUserName:uzivatel', 'GuardAppEventType:APP' FROM dual;

Pokud aktuálně ohlášený uživatel již nebude původcem následujících DB příkazů, je nutné kontext uživatele zrušit pomocí SQL dotazu:

SELECT 'GuardAppEvent:Released' FROM dual;

Pokud po ukončení uživatele okamžitě navazuje činnost nového uživatele lze kontext přenastavit bez spouštění 'GuardAppEvent:Released'.

Příklad DB komunikace jednoho aplikačního uživatele v jednom spojení (session) tedy může vypadat takto:

SELECT 'GuardAppEvent:Start', 'GuardAppEventUserName:xxuzivatel1','GuardAppEventType:POJ' FROM dual;

-- SQL dotazy aplikace POJ v kontextu uživatele xxuzivatel1

SELECT 'GuardAppEvent:Released' FROM dual;

DB příkazy mezi 'Start' a 'Released' budou v IBM Guardium logovány s textem "xxuzivatel1" v atributu "Event User Name" a textem "POJ" v atributu "Event Type" v entitě "Application Events". Hodnota z atributu "Event User Name" se též propíše do atributu "App User Name"

Při změně aplikačního uživatele využívajícího dané spojení do DB, se nejdříve spustí 'GuardAppEvent:Released' nebo 'GuardAppEvent:Start' s loginem nového uživatele.

Při změně spojení využívaného aplikačním uživatelem (přívlastek) se na starém spojení spustí příkaz 'GuardAppEvent:Released', nebo 'GuardAppEvent:Start' s novým uživatelem starého spojení a na novém spojení se spustí příkaz 'GuardAppEvent:Start'

Identifikace aplikačního uživatele pomocí volání uložených procedur (stored procedure)

Tato metoda ohlášení uživatele aplikačního serveru je obdobou Application Event API. Místo noop SQL dotazu je identita uživatele aplikačního serveru vložena jako parametr do volání uložených procedur.

Komunikace může probíhat například takto:

BEGIN set_application_property('user_name', 'xxuzivatel1', 'POJ'); END;

-- SQL dotazy aplikace POJ v kontextu uživatele xxuzivatel1

BEGIN del_application_property('user_name', 'xxuzivatel2', 'POJ'); END;

DB příkazy mezi 'set_application_property' a 'del_application_property' budou v IBM Guardium logovány s textem "xxuzivatel1" v atributu "Event User Name" a "POJ" v atributu "Event Type" v entitě "Application Events". Hodnota z atributu "Event User Name" se též propíše do atributu "App User Name"

Tato metoda je vhodná zejména pro aplikace, které nejsou dostatečně flexibilní pro nasazení Application Event API, a již obsahují volání procedur s uživatelským jménem. Například aplikace PSL spouští proceduru DBMS_SESSION.SET_IDENTIFIER s identitou uživatele před každým databázovým dotazem. Informaci o ukončení činnosti uživatele neposílá.

- S výjimkou speciálních aplikačních vlastníků není sdílení jednoho přístupového účtu více uživateli dovoleno.

8.1.6.1 Databázové účty

8.1.6.1.1 Kategorie účtů

Databázové účty rozdělíme na následující kategorie:

a) Účty DBA a systémové účty databáze Oracle

b) Aplikační účty

   a. Účty uživatelů

   b. Účty aplikační podpory/technologické podpory

   c. Servisní účty aplikací

   d. Aplikační schémata

- Schválení vytvoření uživatele a jeho zařazení do kategorie zajistí pověřený pracovník ČSSZ odboru provozu centrálních informačních technologií.

- Pro jednotlivé kategorie uživatelů budou vytvořeny profily s níže uvedenými charakteristikami. Uživateli bude přiřazen jemu odpovídající profil.

8.1.6.1.2 *Účty DBA a systémové účty databáze Oracle*

Pouze DBA mají možnost připojit se k databázi s oprávněním SYSDBA. Práce uživatele SYS je vždy logována nastavením

AUDIT_SYS_OPERATIONS = TRUE

- Každý DBA má přiřazen svůj osobní účet s potřebnými oprávněními; obvykle v rozsahu role DBA, případně též SYSDBA. Účet je určen pouze pro administraci databáze, musí být vždy chráněn odpovídajícím heslem a nesmí být používán k jiným aktivitám.
- Každý účet musí být v souladu s vyhláškou č. 316/2014 Sb
- Vlastnosti profilu PROF_DBA musí být *v souladu zejména s §18 vyhlášky č. 316/2014 Sb*.

Seznam systémových účtů, které mají účet ve stavu OPEN s heslem ve správě databázových administrátorů
SYS
systém
DBSNMP – je-li využit pro služby OEM

Vlastnosti profilu PROF_DBA: Uzamčení účtu po třech neúspěšných pokusech, změna hesla povinná po 270 dnech se 60 denním varováním, 12 verzí hesel před opětovným použitím.

```
CREATE PROFILE "PROF_DBA"
    FAILED_LOGIN_ATTEMPTS 3 PASSWORD_LOCK_TIME DEFAULT
    PASSWORD_GRACE_TIME 60 PASSWORD_LIFE_TIME 270
    PASSWORD_REUSE_MAX 12 PASSWORD_REUSE_TIME UNLIMITED
    PASSWORD_VERIFY_FUNCTION CSSZ_PWD_VERIFY;
```

8.1.6.1.3 *Účty uživatelů*

Každý účet uživatelů musí být v souladu s vyhláškou č. 316/2014 Sb.

Profile PROF_USER

Vlastnosti: Čas nečinnosti 1 hodina, 4 přihlášení na uživatele, uzamčení účtu po třech neúspěšných pokusech, změna hesla povinná po 30 dnech se 7 denním varováním, 12 verzí hesel před opětovným použitím

```
CREATE PROFILE "PROF_USER"
    IDLE_TIME 60 SESSIONS_PER_USER 4
    FAILED_LOGIN_ATTEMPTS 3 PASSWORD_LOCK_TIME DEFAULT
    PASSWORD_GRACE_TIME 7 PASSWORD_LIFE_TIME 30
    PASSWORD_REUSE_MAX 12 PASSWORD_REUSE_TIME UNLIMITED
    PASSWORD_VERIFY_FUNCTION CSSZ_PWD_VERIFY;
```

8.1.6.1.4 *Účty aplikační podpory/technologické podpory*

Každý účet aplikační nebo technologické podpory musí být v souladu s vyhláškou č. 316/2014 Sb.

Profil PROF_SUPP

Vlastnosti: Čas nečinnosti 1 hodina, 4 přihlášení na uživatele, uzamčení účtu po třech neúspěšných pokusech, změna hesla povinná po 30 dnech se 7 denním varováním, 12 verzí hesel před opětovným použitím.

```
CREATE PROFILE "PROF_SUPP"
    IDLE_TIME 60 SESSIONS_PER_USER 4
    FAILED_LOGIN_ATTEMPTS 3 PASSWORD_LOCK_TIME DEFAULT
    PASSWORD_GRACE_TIME 7 PASSWORD_LIFE_TIME 30
    PASSWORD_REUSE_MAX 12 PASSWORD_REUSE_TIME DEFAULT
    PASSWORD_VERIFY_FUNCTION CSSZ_PWD_VERIFY;
```

8.1.6.1.5 Účty aplikací

Každý účet aplikace musí být v souladu s vyhláškou č. 316/2014 Sb.

Účtům aplikací (účty pro spojení z aplikačních serverů, apod.) je standardně přiřazen profile

Profil PROF_APPL

Vlastnosti: Uzamčení účtu po třech neúspěšných pokusech, změna hesla povinná po 380 dnech se 7 denním varováním, 12 verzí hesel před opětovným použitím

```
CREATE PROFILE "PROF_APPL"
    FAILED_LOGIN_ATTEMPTS 3 PASSWORD_LOCK_TIME DEFAULT
    PASSWORD_GRACE_TIME 7 PASSWORD_LIFE_TIME 380
    PASSWORD_REUSE_MAX 12 PASSWORD_REUSE_TIME UNLIMITED
    PASSWORD_VERIFY_FUNCTION CSSZ_PWD_VERIFY;
```

8.1.6.1.6 Servisní účty aplikací

Každý servisní účet aplikací musí být v souladu s vyhláškou č. 316/2014 Sb.

Servisním účtům aplikací (účty pro dávkové úlohy, apod.) je standardně přiřazen profile

Profil PROF_BATCH

Vlastnosti: Uzamčení účtu po třech neúspěšných pokusech, změna hesla povinná po 380 dnech se 7 denním varováním, 12 verzí hesel před opětovným použitím

```
CREATE PROFILE "PROF_BATCH"
    FAILED_LOGIN_ATTEMPTS 3 PASSWORD_LOCK_TIME DEFAULT
    PASSWORD_GRACE_TIME 7 PASSWORD_LIFE_TIME 380
    PASSWORD_REUSE_MAX 12 PASSWORD_REUSE_TIME UNLIMITED
    PASSWORD_VERIFY_FUNCTION CSSZ_PWD_VERIFY;
```

Pokud je to možné je také omezena doba (denní/noční/hodiny), kdy je možné servisní účet využívat.

- Ve zvláštních případech, kdy nevyhovuje žádný z výše uvedených profilů je potřeba navrhnout vhodný profil, uvést jej v dokumentaci včetně zdůvodnění jednotlivých parametrů profilu.

8.1.6.1.7 Aplikační schémata

- Pro hesla aplikačních účtů musí platit podmínky v souladu s vyhláškou č. 316/2014 Sb.
- Aplikační schémata (vlastníci dat) jsou za provozu ve stavu LOCKED.
- Jako aplikační schéma nesmí sloužit žádný z defaultních účtů databáze Oracle. Objekty aplikačních schémat nesmí být uloženy v systémových tabulkových prostorech. Účet vlastníka aplikace je používán pouze pro servisní práce typu instalace, upgrade, patches, import/export. Export/import aplikačních dat je prováděn výhradně pod účtem aplikačního schématu.
- V aplikaci musí existovat zdokumentovaný postup pro změnu hesla aplikačního účtu. Heslo aplikačního účtu musí být změněno alespoň jednou za 12 měsíců.

- *Pro zvýšení bezpečnosti se doporučuje aplikační schémata nastavit do stavu EXPIRED & LOCKED*

8.1.6.1.8 Standardní tablespaces

- *Pro* všechny aplikační účty musí být nastaven výchozí (default) tablespace **na jiný než systémový tablespace** (tj. nepoužívejte SYSTEM, SYSAUX, atd.). Viz též Standard Oracle10g v prostředí ČSSZ v aktuálně platné verzi.
- U standardních systémových účtů je default tablespace ponechán dle nastavení po instalaci, nevyžaduje-li a/nebo nepovoluje Oracle dokumentace změnu.
- Jako default temporary tablespace se používá k tomu určený tablespace s obsahem TEMPORARY.

8.1.6.2 Autentizace uživatelů

Preferovaný způsob autentizace je Oracle password based autentizace.

- Inicializační parametr databázové instance remote_os_authent musí být nastaven na hodnotu false.

- *Inicializační parametr databázové instance os_authent_prefix je vhodné mít nastaven na hodnotu různou od prázdného řetězce.*

8.1.6.2.1 Pravidla pro nastavení hesla

Pravidla pro nastavení hesel jednotlivých kategorií účtů definuje úsek IKT ČSSZ v úzké spolupráci s architektem kybernetické bezpečnosti IIS ČSSZ.

Hesla musí splňovat složitost definovanou vyhláškou 316/2014 Sb. pro odpovídající kategorie uživatelů.

- Standardní hesla musí být změněna neprodleně po instalaci.
- Heslo uživatele nesmí být nikdy shodné s jménem uživatele. Pro databáze se zavedenou verifikační funkcí musí tato funkce kontrolovat splnění tohoto kritéria.
- Standardní databázové účty, vyjma SYS, SYSTEM a případně DBSNMP, musí být po instalaci nastaveny do stavu EXPIRED & LOCKED.

Ke standardním databázovým účtům, které mají být uzamčeny patří účty uvedené v tabulce Tabulka 8.1-2;

Odstraněno: Tabulka 8.1-3

Seznam uživatelů, kteří musí být po instalaci nastaveni do stavu EXPIRED & LOCKED
OUTLN
TSMSYS
DIP
DBSNMP[2]
WMSYS
EXFSYS

Tabulka 8.1-2

Odstraněno: 3

8.1.6.3 Autentizace střední vrstvy

Problematika autentizace na střední vrstvě s propagací do databáze musí odpovídat předcházejícím bodům 8.1.6.1 a 8.1.6.2.

8.1.6.4 Databázová oprávnění

Každému aplikačnímu účtu databáze je preferováno přidělování oprávnění pomocí specifických aplikačních databázových rolí. Dodržováno je pravidlo nejmenších nutných oprávnění. Veškerá přidělená oprávnění jsou zdokumentována.

8.1.6.4.1 Databázové role

Databázové role obsahují objektová oprávnění pokud není z povahy práce nutné použít oprávnění systémové.

- Oprávnění k roli WITH ADMIN OPTION nelze přidělit.

8.1.6.4.2 Objektová oprávnění

- Objektová oprávnění nejsou přidělována přímo jednotlivým uživatelským účtům.

[2] Není-li využit pro služby OEM – Grid Control.

- Aplikační objektová oprávnění nesmí být přidělena roli PUBLIC.
- Standardní role CONNECT má odlišně přidělená oprávnění v Oracle 9i a Oracle 10g. Od verze 10g obsahuje pouze systémové oprávnění CREATE SESSION, které přímo odpovídá možnosti realizovat připojení do databáze. Z hlediska administrace v ČSSZ je proto vyžadováno:

➢ aplikační role nesmí obsahovat právo CREATE SESSION, neboť toto právo musí být schopné samostatného odebrání vybranému uživateli pro řešení administrace uživatelů

- Nepřidělovat standardní roli RESOURCE, která v sobě obsahuje značně široké oprávnění unlimited tablespace.
- Po vytvoření databáze je vyžadováno odebrat oprávnění ke spuštění pro PUBLIC k následujícím balíčkům: DBMS_JOB, DBMS_LOB, UTL_FILE, UTL_HTTP, UTL_INADDR, UTL_SMTP, UTL_TCP. Odeberte právo select pro PUBLIC z pohledu ALL_SOURCE. Po aplikaci patchsetu proveďte kontrolu, zda nedošlo k opětovnému přidělení oprávnění a v případě potřeby je odeberte.

8.1.6.4.3 Systémová oprávnění

- Použití systémových oprávnění a rolí vyjmenovaných v tabulce Tabulka 8.1-3 není dovoleno s výjimkou databázových administrátorů.

Odstraněno: Tabulka 8.1-5

Seznam systémových oprávnění s omezeným použitím
oprávnění typu ANY
ALTER DATABASE
ALTER SYSTEM
AUDIT SYSTEM[3]
BECOME USER
CREATE DATABASE LINK
CREATE LIBRARY
CREATE PUBLIC DATABASE LINK
DROP PUBLIC DATABASE LINK
CREATE PROFILE
ALTER PROFILE
DROP PROFILE
UNLIMITED TABLESPACE
ADMINISTER DATABASE TRIGGER
CREATE USER
ALTER USER
DROP USER
EXEMPT ACCESS POLICY
SYSDBA
SYSOPER
RESOURCE
DBA
DELETE_CATALOG_ROLE
EXECUTE_CATALOG_ROLE
SELECT_CATALOG_ROLE
EXP_FULL_DATABASE
IMP_FULL_DATABASE
SNMPAGENT

[3] Toto oprávnění mohou obdržet kromě DBA také bezpečnostní administrátoři.

RECOVERY_CATALOG_OWNER
HS_ADMIN_ROLE
SCHEDULER_ADMIN

Tabulka 8.1-3

Odstraněno: 5

Odstraněno: Tabulka 8.1-5

Vybraná systémová oprávnění uvedená v tabulce Tabulka 8.1-3 není dovoleno přidělovat přímo jednotlivým uživatelským účtům. Systémová oprávnění nesmí být přidělena roli PUBLIC. Ve výjimečných případech nutnosti použití některého z těchto systémových oprávnění je nutné

- vytvořit samostatné aplikační schéma, které má příslušné oprávnění
- toto schéma „publikuje“ PL/SQL rozhraní pro aplikační využití
- používaný kód nesmí být wrapován
- schéma nastavit do stavu EXPIRED & LOCKED
- rozsah použitých oprávnění musí být součástí dokumentace
- použití takovéhoto schématu musí být schváleno úsekem IKT ve spolupráci s odborem 11.

8.1.6.4.4 Data dictionary

- Přístup k data dictionary (fixní i dynamické pohledy a base tabulky) je omezen na databázové administrátory. Parametr O7_DICTIONARY_ACCESIBILITY je nastaven na FALSE.

Význam parametru O7_DICTIONARY_ACCESIBILITY: Jestliže je parametr O7_DICTIONARY_ACCESIBILITY nastaven na false, pak standardní uživatelé nemají přístup k data dictionary objektům ve schématu uživatele SYS.

- Jestliže některý uživatel/role vyžaduje přístup k objektům data dictionary bude v odůvodněných případech přednostně přidělováno příslušné objektové oprávnění.

Obecně lze přístup k objektům ve schématu SYS řešit též pomocí rolí:

- SELECT_CATALOG_ROLE, (dovoluje uživatelům provádět dotazy do data dictionary pohledů)
- EXECUTE_CATALOG_ROLE (dovoluje spouštět balíčky a procedury v data dictionary),
- DELETE_CATALOG_ROLE (dovoluje mazat záznamy ze systémové auditní tabulky AUD$) a
- SELECT ANY DICTIONARY (dovoluje dotaz na objekty ve schématu SYS včetně tabulek.)

- *Přidělení oprávnění EXECUTE/DELETE_CATALOG_ROLE, jakož i role SELECT ANY DICTIONARY není povoleno.*
- *Přidělení oprávnění SELECT _CATALOG_ROLE není bez jasného vymezení důvodů povoleno.*

- Každé přidělení oprávnění SELECT _CATALOG_ROLE musí být součástí aplikační dokumentace.

8.1.6.4.5 Role DBA

- Použití role DBA v produkčním prostředí je omezeno pouze na účty databázových administrátorů.

8.1.6.5 Databázové objekty a sdílené atributy

8.1.6.5.1 Public synonyma

- *Vytváření public synonym se nedoporučuje. V případě potřeby aplikace vytvořit synonyma se předpokládá vytvoření privátních synonym.*

8.1.6.5.2 Databázový link

- Použití public databázového linku není povoleno.

- *Komunikaci pomocí databázových linků je možné použít pouze pro specifické účely jako migrace apod. Pro detailní informace o doporučených způsobech komunikace viz standardy CSSZ*

8.1.6.5.3 Vazba na operační systém

- *Přístup aplikace k operačnímu systému databázového serveru není povolen.*

- *Použití directories je preferováno před použitím utl_file_dir.*
- *Použití parametru utl_file_dir není doporučeno.*

- Directories a utl_file_dir nesmí být směrovány do:
  - volume group s OS
  - volume group s Oracle SW
  - volume group s databázovými soubory
  - hodnota parametru utl_file_dir nesmí být nastavena na hodnotu *

- Adresářům použitým pro directories (utl_file) musí mít přidělena na úrovni filesystému minimální oprávnění nutná k provozu aplikace. Požadované oprávnění musí být součástí dokumentace.
- Přístup k directories je na úrovni databáze řízen pro schémata různá od vlastníka directory přidělením práva READ nebo WRITE. Každé přidělení takového oprávnění musí být součástí aplikační dokumentace.

- Aplikační data (včetně dočasných souborů) a SW nesmí být umístěny na databázovém serveru, zejména ne do:
  - volume group s OS
  - volume group s Oracle SW
  - volume group s databázovými soubory

- Extproc a CREATE LIBRARY nejsou povoleny.

8.1.6.6 Ochrana sensitivních dat

- *Pro ochranu citlivých dat je preferováno použití Label Security.*

- *Pro ochranu citlivých dat je možno využít šifrování poskytované nativními prostředky databáze.*

- Logon trigger nesmí být wrapován a nesmí ovlivnit přihlášení uživatelů s oprávněním DBA.

8.1.6.7 Oprávnění k systémovým funkcím

- Pokud aplikace vyžadují přidělení oprávnění ke standardním packages je vyžadováno, aby odpovídající uživatelé obdrželi potřebná oprávnění v průběhu zakládání aplikačního schématu explicitně i v případech, kdy příslušné packages jsou standardně přístupné pro uživatele public.
- Oprávnění k systémovým databázovým funkcím nesmí být přidělovány vlastníkům aplikačních schémat ani aplikačním uživatelům.
- Aplikace nejsou oprávněny používat nedokumentované funkce databázového serveru pro zabezpečení standardních provozních funkcionalit.

Nastavení databázových instancí

- Povinné nastavení pro databázové instance:
  - remote_os_authent = false
  - požadavky na nastavení parametru utl_file_dir včetně souvisejících adresářů viz kapitola 3.2.5.3 Vazba na operační systém

- *Doporučené nastavení pro databázové instance:*
  - *sql92_security = true*[4]
  - *os_authent_prefix nastavte na hodnotu různou od prázdného řetězce*
  - *os_roles = false*
  - *remote_os_roles = false*
  -
  - *audit_sys_operations = true*

Oracle Network

8.1.6.7.1 Oracle Listener

- Oracle listener musí mít zapnuté admin restrictions.

- *V případě databází, ke kterým se přistupuje pouze z několika málo vybraných pevných IP adres je doporučeno provést omezení přístupu na tyto vybrané IP adresy.*

8.1.6.7.2 Jmenné služby

- *Informace nutné pro připojení k databázím jako jsou hostname, port listeneru, jméno servisní služby, jméno instance jsou považovány za neveřejné.*

[4] SQL92 standard specifikuje, že uživatel musí mít oprávnění SELECT na tabulku, jestliže má provést operaci UPDATE nebo DELETE, které odkazují na sloupec v klauzuli where nebo set.

8.1.6.7.3 Šifrování dat přenášených po síti

- *Zvýšenou ochranu dat je možné zabezpečit kryptováním dat při přenosu.*

Pro přenos dat, která nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy např. osobní údaje podle zákona č. 101/2000 Sb. musí být při jejich přenosu vnější komunikační sítí zabezpečena ochrana pomocí kryptografických prostředků.

Pro přenos dat, která nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany např. citlivé osobní údaje podle zákona č. 101/2000 Sb. musí být při jejich přenosy chráněny pomocí kryptografických prostředků.

8.2 Izolace provozu aplikací

Dále jsou uvedena základní pravidla pro umístění schemat do databází a databází na server v pořadí podle jejich důležitosti:

1. Důsledné vzájemné oddělení produkčního, testovacího a integračního prostředí. Především není možné provozovat jakékoliv jiné než produkční prostředí na produkčním serveru. V případě, že by toto pravidlo nebylo dodrženo, je zde velké riziko, že dojde k negativnímu ovlivnění provozu při testování nových verzí či aplikací.

2. Oddělení dat podle typu zpracování – transakční, dávkové, analytické. Především oddělení analytických a transakčních úloh na datové úrovni je vhodné, neboť je obvyklé, že pro tyto typy úloh se používá diametrálně odlišný datový model a charakter provozu je též rozdílný.

3. Oddělení dat pro aplikace s různým provozním režimem – 16x5, 24x7 apod. Cílem je realizace „malé“ databáze pro provoz kritických aplikací v režimu 24x7 a „velké“ databáze pro aplikace s režimem odlišným.

4. Oddělení dat podle stupně zabezpečení (diskové pole, zrcadlené diskové pole, DataGuard, cluster, RAC apod.). Cílem tohoto pravidla je zajistit maximální zajištění kritických dat při zachování nízkých nákladů. Toho se dosáhne oddělením kritických a nekritických dat.

5. Vzájemně provázaná schemata (např. referenční integrita) je nutné umístit do stejné databáze.

6. Využití dat stejnou aplikací – umístění schemat využívaných shodnou aplikací omezí nutnost spojení aplikace do více databází, čímž se šetří zdroje (paměť)

7. Požadavky na zdroje – CPU, paměť

8. Logické členění dat je vhodné/nutné přenést i na úroveň fyzickou. Toto pravidlo je dále rozpracováno v následující kapitole.

Na základě těchto pravidel by mělo dojít ke kategorizaci serverů a databází. To následně vede k snadnému rozhodování o umístění nových datových schemat. Následně bude vhodné provést analýzu současného umístění schemat a databází. V případě zjištění zásadních rozporů s pravidly (především pravidlem

1. a 2.) doporučujeme postupně přesunout schemata či databáze tak, aby umístění těmto pravidlům vyhovovalo.

Příklad kategorií serverů:

- Testovací
- Integrační
- Provozní s provozem 24x7 zabezpečený clusterem
- Provozní s provozem 24x7 zabezpečený clusterem a daty zabezpečenými zrcadlením diskového pole
- Provozní s provozem 16x5 pro analytické aplikace

Příklad kategorií databází:

- Vývojová
- Testovací
- Školící
- Integrační
- Provozní s provozem 24x7 zabezpečená clusterem, data životního pojištění
- Provozní s provozem 24x7 zabezpečená clusterem, data neživotního pojištění
- Provozní s provozem 24x7 zabezpečená clusterem a daty zabezpečenými zrcadlením diskového pole, kmenová data klientů a data pojištění,
- Provozní s provozem 16x5 pro analytické aplikace

Výše uvedené příklady nejsou kompletním přehledem kategorií, které by měly být zavedené. Též je možné, že některé z uvedených příkladů nebude ČSSZ definovat.

V současné době jsou provozovány druhy databází

- rodukční 24x7 zabezpečená clusterem a daty zabezpečenými zrcadlením diskového pole
- testovací a současně školící
- integrační

Kromě fyzického oddělení dat je možné vzájemně izolovat jednotlivé uživatele nebo skupiny uživatelů z hlediska využívání zdrojů systému. Tímto oddělením lze odstranit především ovlivnění způsobených nadměrným zatížením databáze určitým procesem nebo aplikací, případně je možné zvýšit prioritu pro určité aplikace nebo skupiny uživatelů. Předpokladem pro takovéto oddělení je:

- Databáze verze 10 a výše
- Možnost rozlišení uživatelů nebo skupin uživatelů na úrovni databáze

- Možnost rozlišení aplikací na úrovni databáze

Po splnění těchto podmínek následuje kategorizace aplikací, aplikačních modulů a uživatelů podle potřeby zdrojů a důležitosti.

9. Pravidla pro fyzickou strukturu databáze

Provoz databáze vždy přináší požadavky na práci s daty. Jedná se obvykle ve velké míře o čtení, ale velmi důležitá je vkládání, úpravy a mazání. Tyto operace mají velký vliv na organizaci dat uložených v databázi. Především operace změn existujících záznamů a operace mazání přinášejí problémy s uložením dat. S novými verzemi databáze přicházejí stále nové možnosti a prostředky pro řešení těchto problémů. Přesto je vhodné organizovat data v databázi tak, aby k uvedeným problémům nedocházelo, nebo byly výrazně omezeny. Proto je při návrhu fyzické struktury databáze vhodné dodržovat následující pravidla:

1. Pro variantu uložení dat ve filesystému nebo rawdevices: oddělení indexů od dat – fyzické uspořádání indexů je odlišné od uspořádání tabulek a tím se liší i jejich životní cyklus. Též z hlediska optimalizace provozu databáze je výhodné, aby toto oddělení bylo dodrženo. Pro variantu uložení dat v Oracle ASM: oddělení platí na úrovni tablespaces, architektura Oracle ASM zaměřená především na výkonnost a spolehlivost uložení databázových souborů dovoluje ukládat databázové soubory určené pro indexy do jedné ASM diskové skupiny společně s databázové soubory určené pro tabulky.

2. Umístění největších tabulek do vyhrazených tablespaců. V případě partitioningu obsazují největší tabulky více tablespaců.

3. Kategorizace dat na:

    a. Rostoucí – data, která v čase přibývají, vložená data se mění minimálně a minimálně nebo vůbec jsou data odmazávána

    b. Stabilní – data, která se v čase prakticky nemění

    c. Dynamická – data měnící se v čase – data se vkládají, mění i odmazávají

    d. Pomocná – data specifická pro určitou operaci, existence je časově omezená

4. Pro tyto kategorie zavést oddělené tablespace. To umožní optimalizovat uložení dat na disku výrazně jednodušeji a výrazně se tím sníží možnost fragmentace prostoru.

5. Je žádoucí, aby logické členění dat bylo promítnuto i do fyzické struktury. To znamená, že data, která spolu nesouvisí (obvykle z různých schemat), by neměla ležet ve stejném tablespace. To umožní především snadnou údržbu databáze, snadnou identifikaci aplikací pro dané fyzické struktury a usnadní případnou reorganizaci databází.

10. Open and Closed Issues

10.1.1 Open Issues

ID	Issue	Resolution	Responsibility	Target Date	Impact Date

10.1.2 Closed Issues

ID	Issue	Resolution	Responsibility	Target Date	Impact Date