# Standardy IS VZP – NIS

**UPOZORNĚNÍ:**

Tento dokument je zpracován Všeobecnou zdravotní pojišťovnou České republiky (dále též jen „VZP ČR“ nebo „VZP“). Všeobecná zdravotní pojišťovna České republiky jej uveřejňuje v rámci zadávací dokumentace jí zadávaných veřejných zakázek. Tento dokument umožňuje utvořit si představu o standardech informační architektury ICT VZP ČR. Účelem jeho uveřejnění je poskytnout informace nezbytné pro integraci dodávané komponenty se stávajícím informačním systémem v souladu se Standardy ICT- VZP- NIS.

Uveřejněním tohoto dokumentu není dotčena právní odpovědnost spojená s jeho zneužitím.

V tomto dokumentu bylo použito názvů subjektů a názvů produktů, které mohou být chráněny příslušnými právními předpisy.

**Otevřením tohoto dokumentu berete výše uvedené skutečnosti na vědomí.**

# Verze dokumentu

| Verze | Datum | Autor | Popis |
|---|---|---|---|
| 1.06 | 11. 10. 2017 | ÚICT VZP ČR | |
| 1.07 | 23. 02. 2018 | [redacted] | Úprava 3. kapitoly |
| 1.08 | 7. 9. 2018 | [redacted] | Revize integračních částí - pro účely CIS |
| 1.09 | 26. 2. 2019 | [redacted] | Revize kapitoly Bezpečnostní standardy |
| 1.10 | 11. 3. 2019 | [redacted] | Úpravy v dokumentu, upřesnění logování |
| 1.10.1 | 23. 5. 2019 | [redacted] | Sloučeny změny s revizemi od OTP |
| 1.10.2 | 12.6.2019 | [redacted] | Úprava formátu |

# Obsah

1 Úvod ... 8
2 Architektonické a QA standardy ... 9
2.1 Aplikační – obecné standardy ... 9
2.1.1 Třídy Aplikací ... 9
2.2 Integrační a komunikační standard ... 9
2.2.1 Integrace se stávajícím IS ... 10
2.3 Vývojové standardy ... 10
2.3.1 Použité vývojové nástroje pro interní vývoj aplikací: ... 10
2.3.2 Vývojová a testovací prostředí ... 10
2.4 Testovací standardy ... 11
2.5 Dokumentační standard ... 12
3 Infrastrukturní standardy ... 17
3.1 Obecné zásady ... 17
3.2 HW ... 18
3.2.1 On Premise Serverová infrastruktura ... 18
3.3 Sítě ... 19
3.3.1 VLAN ... 19
3.3.2 QoS (QUALITY OD SERVICE) ... 19
3.3.3 Datová centra ... 19
3.3.4 Perimetr ... 21
3.3.5 Síťové služby ... 21
3.4 OS ... 22
3.4.1 OS pro aplikace třídy A ... 22
3.4.2 OS pro aplikace třídy B ... 22
3.4.3 Prostředí pro virtualizaci ... 22
3.4.4 Požadavky na linuxové účty ... 22
3.5 Middleware ... 23
3.5.1 Aplikační servery ... 23
3.5.2 Webové servery ... 23
3.6 Virtualizovaná infrastruktura pro hostování aplikací ... 23

3.7 Deployment aplikací provozovaných on-Premise do prostředí v DC VZP ... 24
3.8 Datové a databázové služby ... 25
3.8.1 Databázové technologie ... 25
3.8.2 Datové a databázové standardy ... 25
4 Bezpečnostní standardy ... 27
4.1 Dodržování legislativních požadavků ... 27
4.1.1 Autorský zákon ... 27
4.1.2 ZOKB ... 27
4.1.3 GDPR ... 27
4.2 Dodržování obecných standardů a doporučení ... 27
4.3 Minimum běžících a instalovaných služeb ... 27
4.4 Nevyhovující služby nebo protokoly ... 27
4.5 Synchornizace času ... 28
4.6 Kryptografie ... 28
4.6.1 Požadavky na kryptografické algoritmy ... 28
4.6.2 Požadavky na ochranu privátního klíče ... 28
4.7 Komunikace s veřejnou sítí ... 28
4.7.1 Systémy, nebo aplikace, které publikují služby do veřejné sítě (inbound) ... 28
4.7.2 Komunikace do veřejné sítě (outbound) ... 28
4.7.3 SMTP komunikace s veřejnou sítí ... 28
4.8 Řízení přístupu ... 29
4.8.1 Interní uživatelé ... 29
4.8.2 Externí uživatelé (např. klient VZP) ... 29
4.8.3 Propagace identity uživatele ke koncovým službám ... 29
4.8.4 Ochrana hesel a politika hesel ... 29
4.8.5 Mechanismus obrany proti hádání přístupu do systému ... 29
4.8.6 Omezení přístupů ke službám ve vnitřní síti VZP ČR ... 29
4.8.7 Zobrazení varovného hlášení ... 29
4.9 Ochrana informačních aktiv ... 30
4.9.1 Klasifikační schéma informačních aktiv ... 30
4.9.2 Data v klidu ... 30
4.9.3 Data v pohybu ... 30
4.9.4 Data in use – Data v použití ... 31
4.9.5 Antimalware ochrana ... 31

4.9.6 Plán obnovy (Disaster Recovery) ... 31
4.10 Bezpečnostní testy ... 31
4.10.1 Systémy, nebo aplikace, které nepublikují služby do veřejné sítě ... 31
4.10.2 Systémy, nebo aplikace, které publikují služby do veřejné sítě ... 31
5 Logování ... 32
5.1 Požadavky ... 33
5.1.1 Formát a encoding logu ... 33
5.1.2 JSON - doporučené pojmenování klíčů a identifikace datové struktury ... 33
5.1.3 Obecně platné zásady pro logování ... 33
5.1.4 Technické zajištění logování ... 34
5.1.5 Retence logů ... 34
5.1.6 Dokumentace ... 34
5.2 Základní úroveň logování z pohledu bezpečnosti ... 34
5.2.1 Logování procesu autentizace ... 35
5.2.2 Činnosti provedené administrátorem ... 35
5.2.3 Změny přístupových oprávnění a změny údajů, které slouží k přihlášení ... 35
5.2.4 Neprovedení činnosti v důsledku nedostatku přístupových oprávnění ... 36
5.2.5 Přístupy k záznamům o činnostech ... 36
5.2.6 Operace se soubory ... 36
5.2.7 Vybrané JSON klíče pro záznam události ... 36
5.3 Logování transakcí při zpracování osobních a zvláštní kategorie osobních údajů ... 37
5.3.1 Vybrané JSON klíče pro záznam události ... 37
5.3.2 Příklad logu činnosti nahlížení ... 38
5.3.3 Příklad logu činnosti změna ... 38
5.4 Základní požadavky na logování komunikace a business logiky- Transakční log ... 38
5.4.1 Informační obsah události zaznamenávané v transakčním logu ... 38
5.4.2 Vybrané JSON klíče pro záznam události ... 39
5.4.3 Příklad transakčního logu ... 40
5.5 Provozní log ... 40
5.5.1 Základní požadavky na provozní logování – Provozní log ... 40
5.5.2 Formát logovacího souboru provozního logu ... 40
6 Provozní standardy ... 41
6.1 Monitoring ... 41
6.1.1 Rozsah monitoringu a používané nástroje ... 41

6.1.2 Používané dohledové nástroje pro On premise řešení ... 41
6.1.3 Požadavky na procesy z hlediska monitoringu ... 42
6.1.4 Požadavky na návrh monitoringu ... 42
6.1.5 Požadavky na rozhraní pro monitoring ... 42
6.2 Zálohování a archivace ... 43
6.2.1 Zálohovací systém ... 43
6.2.2 Požadavky na aplikační celky z pohledu jejich zálohování: ... 43
6.3 Definice provozních parametrů služby/aplikace (SLA) ... 44
6.4 Podmínky převzetí do rutinního prostředí a aplikační podpory ... 45
6.5 Vazba na ITIL procesy ... 45
6.5.1 Definování veškerých eskalačních procedur u aplikace - správa HelpDesku/ServiceDesku ... 45
6.5.2 Zavedení aplikace do incident managementu ... 45
6.5.3 Zavedení aplikace pod standardní řízení změn - change management ... 45
6.5.4 Zavedení aplikace do release plánů - release management ... 46
7 Seznam příloh ... 46
8 Výjimky ze standardu ... 46
8.1 Integrace se stávajícím IS ... 46

# 1 Úvod

## STANDARDY IS VZP - NIS

- **Představují -** soubor pravidel určených pro vytváření, rozvoj a využívaní IS VZP ČR.
- **Obsahují -** charakteristiky, metody, postupy a podmínky, které musí IT komponenty naplnit či dodržet, zejména pokud jde o bezpečnost a integrovatelnost s jinými informačními komponenty a systémy.
- **Jsou určeny -** pro všechny dodavatele řešení/služeb/komponent jako pravidla dodávek IS/IT a k vývoji aplikací a jejich releasů.
- **Všichni dodavatelé komponent IS do VZP** jsou povinni po akceptaci standardu ho respektovat ve znění, v jakém ho přijali.
- **Od standardu se lze odchýlit pouze na základě výjimky.** Výjimky zpracovává oddělení architektury, posuzuje je vlastník příslušného standardu VZP ČR, který je uveden u příslušné kapitoly. Schválení výjimky na základě posouzení schvaluje náměstek pro IT VZP ČR.
- **Při vydání nové verze standardu dodavatelé jsou vyzváni k přistoupení k nové verzi standardu** pro další dodávky. Pokud není poskytované řešení kompatibilní s novou verzí standardu, požádají VZP o výjimku.
- **Jejich účelem je** nasazení a následné provozování řešení/komponent v rutinním prostředí VZP s požadovanými garancemi, s požadovanými provozními parametry, s požadovanou odbornou aplikační a provozní podporou provozu IT při optimalizaci řešení IT.

# 2 Architektonické a QA standardy

## 2.1 Aplikační – obecné standardy

Vlastník kapitoly: oddělení Architektury

- Aplikace má být navržena jako vícevrstvá, tyto vrstvy musí být jasně definovány a jejich rozdělení striktně dodržováno. Obvykle se aplikace skládá z těchto vrstev:
  Webová / presentační vrstva - uživatelské rozhraní -
  - Aplikační vrstva
  - Databázová vrstva
- Aplikační řešení musí být složeno z jednotlivých komponent s definovanými a oddělenými funkčnostmi, včetně rozhraní (API) jež funkčnosti zpřístupňují, bez duplicit a distribuované funkční logiky.
- Aplikační řešení by má být tvořeno ze sady relativně nezávislých modulů, aby změna v jednom z nich neznamenala (podstatný) zásah do zbývajících modulů. Moduly jsou v ideálním případě samostatně (autonomně) nasaditelné (upgradovatelné).
- Aplikace musí mít deklarovatelným způsobem ošetřeny architektonické aspekty: škálovatelnost a flexibilita a to zejména **umožněním horizontálního škálování;**
- Součástí návrhu aplikačního řešení a realizace je požadován kapacitní a výkonnostní sizing systému s výhledem na 5 let.
- Aplikace musí splňovat požadavky na zálohování a obnovu popsané níže.
- Aplikace/ Řešení musí podporovat mechanismy pro archivaci dat a jejich případnou obnovu
- Aplikace musí respektovat již v návrhu požadavky na bezpečnost a soulad (compliance), viz kapitola 4 Bezpečnostní standardy.

### 2.1.1 Třídy Aplikací

Aplikace a aplikační řešení jsou z pohledu kritičnosti provozu kategorizovány do následujících tříd:

**Třída A**

Jedná se o business kritické a technologické aplikace, jejichž výpadek má zásadní charakter. Garantovaná dostupnost těchto aplikací je 99,4% v požadovaném režimu provozu (standardně 7x24 nebo 5x16).

**Třída B**

Jedná se o aplikace, které nepatří mezi business kritické a mají nižší nároky na zajištění jejích dostupnosti. Požadovaná dostupnost je 98,1% v požadovaném režimu provozu 5x8 nebo 5x16.

## 2.2 Integrační a komunikační standard

Vlastník kapitoly: oddělení architektury

- Komunikace mezi aplikacemi a integrace musí respektovat následující pravidla: Komunikace je v zásadě asynchronní (synchronní komunikace pouze ve výjimečných odůvodněných případech);
- Komunikace musí být odolná proti výpadku jedné strany
- Komunikace maximálně omezuje využívání mechanismů:

  - distribuovaná transakce
  - dvoufázové potvrzení transakce (two-phase- commit);
- Komunikace dodržuje zásady idempotence[1], tam kde je to možné.
- Veškeré vazby systému na ostatní systémy jsou formou volné vazby (loosely coupled), doporučeným mechanizmem aplikační komunikace je využití messagingu, případně synchronních REST služeb.
- Pro přenos souborů (MFT) a datových objektů větších než 2MB se využije souborový přenos.
- Pro datovou integraci se využijí nástroje ETL, případně nástroje pro Event Streaming .
- Pro implementaci nových veřejných rozhraní (API) upřednostňovat REST v3.0 (HATEOAS[2]).
- Spojení mezi stávajícími systémy VZP provádět přes integrační platformu (ESB).
- V maximální možné míře je nutno využívat stávajících již implementovaných aplikačních služeb nabízených v infrastruktuře VZP.
- Není povoleno využívat integraci aplikací na úrovni databází (link mezi databázemi);
- V rámci aplikace musí být zajištěna kontrola vstupů a výstupů (formátů dat), automatické přenosy obsahují kontrolní součty a zabezpečení, manuální přenosy jsou nepřípustné;
- Proces zpracování dávek (batch, ETL, MFT) musí obsahovat dílčí kontrolní body a kontrolní mechanizmy.

### 2.2.1 Integrace se stávajícím IS

Ke dni vzniku tohoto standardu VZP provozuje stávající IS řízený historickou verzí standardu. Způsob integrace s tímto IS je proto prováděn odchylně od tohoto standardu. Tato výjimka je zachycena v kapitole 8.1 Integrace se stávajícím IS.

## 2.3 Vývojové standardy

Vlastník kapitoly: OAVRZ

### 2.3.1 Použité vývojové nástroje pro interní vývoj aplikací:

- Funkční analýza a design: Enterprise Architekt, MS Word, Balsamiq Mockups
- Technický design-aplikační logika: Visual Studio 2015/2017
- Technický design-datový design: Visual Studio 2017 Database Tools (MSSQL / Oracle)
- Technický design-integrační procesy: OpenAPI / AutoRest (Enterprise Architect, MS Word)
- Správa verzí: Visual Studio Team Services (Git), Gitlab
- Vývoj aplikací: Visual Studio 2015/2017, Visual Studio Code, SQL Server Management Studio, XCode / Android Studio, SOAP UI, Postman
- Migrace a deployment aplikací: Azure DevOps

### 2.3.2 Vývojová a testovací prostředí

Vyvíjená aplikace musí mít definována minimálně prostředí:

- Samostatné prostředí určené konkrétnímu vývojáři
- prostředí určené pro ověřovací testy v rámci vývoje, preferováné je, aby nasazování na tato prostředí probíhá automaticky
- prostředí určené pro akceptační test garanty aplikací, nasazení na tato prostředí je řízeno pověřeným vedoucím testování (určeným vedoucím testovacího oddělení)
- Verzování vývoje
  - Vyvíjená aplikace bude verzována pomocí tzv. sémantického verzování[3]

[1] (https://en.wikipedia.org/wiki/Idempotence)
[2] http://restcookbook.com/Basics/hateoas/

## 2.4 Testovací standardy

Vlastník kapitoly: OTP Oddělení testování

- Součástí každého řešení/ komponenty je testovací dokumentace (viz dokumentační standard)
- Součástí každého řešení jsou provedené testy dle dokumentace příslušné aplikační komponenty
- Testování se provádí na anonymizovaných/pseudonymizovaných datech (součástí řešení jsou nástroje pro anonymizaci/pseudonymizaci testovacích dat)
- Musí být zajištěna jednotná anonymizace/pseudonymizace dat integrovaných aplikací v rámci testovacího prostředí

**Typy požadovaných testů pro předání do provozu IT**

| **Vývojové testování** | | | |
|---|---|---|---|
| **Název testu** | **Provádí** | **Vstupy** | **Výstupy** |
| unit test<br>assembly test<br>funkční test<br>test výjimek | vývojoví pracovníci a testeři dodavatele komponenty | Návrh architektury testování<br>Plán testů<br>Testovací scénáře a testovací případy<br>Specifikace testovacích dat<br>Testovací data | Odsouhlasené testovací scénáře a testovací případy<br>Odsouhlasená specifikace testovacích dat<br>Záznam výsledků testů<br>Protokol o provedení vývojových testů |
| **Systémové testování** | | | |
| **Název testu** | **Provádí** | **Vstupy** | **Výstupy** |
| smoke test<br>funkční test<br>test výjimek<br>integrační test | testeři dodavatele komponenty společně s testery VZP ČR[4] | Testovací scénáře a testovací případy<br>Specifikace testovacích dat<br>Testovací data<br>Protokol o provedení vývojových testů | Odsouhlasené testovací scénáře a testovací případy<br>Odsouhlasená specifikace testovacích dat<br>Záznam o výsledku testů<br>Protokol o provedení systémových testů |
| **Nefunkční testy** | | | |
| **Název testu** | **Provádí** | **Vstupy** | **Výstupy** |

[3] https://semver.org/lang/cs/

[4] Společně s testery VZP znamená poskytnutí přiměřené součinnosti VZP k provedení a přípravě testu tam kde je to věcně nezbytné.

| | | | |
|---|---|---|---|
| zátěžový test<br><br>stress test | testeři dodavatele komponenty společně s testery VZP ČR | Projektová dokumentace<br>Plán testů<br>Analýza pro výkonnostní test<br>Testovací data<br>Testovací scénáře<br>Protokol o provedení systémových testů | Výsledky výkonnostního testu<br>Zpráva o výkonnostním testu |
| Backup a recovery test | Administrátoři VZP ČR | Postup zálohy a postup obnovení. Testovací scénáře ověřující základní funkčnosti po záloze a obnovení | Záznam ověření provedení obnovy ze zálohy. |
| **Bezpečnostní testy** | | | |
| **Název testu** | **Provádí** | **Vstupy** | **Výstupy** |
| bezpečnostní test | testeři OBIT VZP ČR | Identifikace komponent k testování (dodavatel a VZP ČR) | Výsledky testu |
| penetrační test (u Internet facing aplikací / systémů) | penetrační testování zajišťuje nezávislý subjekt (subdodávka), náklady nese dodavatel | Identifikace komponent k testování (dodavatel a VZP ČR), návrh rozsahu penetračního testu (dodavatel, VZP ČR) | Výsledky testu |
| **Akceptační uživatelské testy - strana odběratele (VZP ČR)** | | | |
| **Název testu** | **Provádí** | **Vstupy** | **Výstupy** |
| akceptační uživatelský test | testeři VZP ČR | Protokol o provedení systémových testů<br>Testovací scénáře, testovací případy<br>Data ze systémových testů | Záznam výsledků testu<br>Akceptační protokol za testování |

## 2.5 Dokumentační standard

Vlastník kapitoly: OAVRZ

Dokumentace systému se skládá z:

- Celková – úplná dokumentace. Popisuje úplně systém v jeho aktuální podobě.
- Přírůstek dokumentace – dokumentace konkrétní změny provedené oproti celkové dokumentaci.

- Celková dokumentace k dodanému řešení musí být dodavatelem pravidelně aktualizovaná a to při významných změnách / velký release .
- Dokumentace musí být min. 1 x ročně konsolidována, všechny dílčí změny zapracovány do úplné verze a předány VZP.
- Kromě odůvodněných a schválených a smysluplných výjimek (např. zdrojový kód) je dokumentace vedena v nástroji Sparx Enterprise Architect.

Níže uvedený seznam dokumentů je volitelný. Dle předmětu specifikace zakázky na dodávku do IS VZP bude proveden výběr povinně požadovaných dokumentů od dodavatele řešení.

| **Dokumentační oblast** | **Podrobnější popis** | **Dokumenty** |
|---|---|---|
| Funkční dokumentace | Funkční dokumentace definuje funkčnosti systému a jejich chování v souvislosti s řešením služeb pro podporu business procesu. Představuje detailní popis, jak software funguje, bez vazby na konkrétní technologii či detailní architekturu systému.<br><br>Zabývá se proto business elementy, jako jsou: business entity, schopnosti, procesy, role, cíle, lokality a taky vnější omezení (např. legislativní) a jiné vlivy, které je třeba při návrhu řešení brát v potaz.<br><br>Funkční a nefunkční požadavky na řešení jsou definovány v katalogu požadavků.<br><br>Popis požadavku na změnu definuje klíčové potřeby uživatelů na IS, podporované procesy.<br><br>Při velkých změnách obsahuje funkční dokumentace i návrh nového řešení a způsob, jak nového řešení dosáhnout ve vazbě na stávající stav. | Katalog požadavků na dodané řešení do IS VZP<br><br>Účastníci řešení<br><br>Pojmy a artefakty řešení<br><br>Statický model<br><br>Doménový model<br><br>Statický model<br><br>Logická architektura<br><br>Konceptuální datový model<br><br>Procesy podporované dodaným řešením<br><br>Dynamický model<br><br>Funkční předpoklady, omezení<br><br>Katalog služeb komponenty<br><br>Postup implementace a migrace |

| | | |
|---|---|---|
| Technická dokumentace | Technická dokumentace obsahuje návrh IT řešení business problémů specifikovaných na úrovni business analýzy a obsažené ve funkční dokumentaci. Navrhuje funkčnost jednotlivých technických komponent IT systémů, místo řešení požadavků v rámci vrstev nebo jiných částí IT architektury.<br><br>Zpodrobňuje požadavky z funkční dokumentace na implementační úroveň.<br><br>Obsahuje popis aplikační architektury, front end komponenty, validace, popis business logiky, orchestrace, popis datové vrstvy, deployment, konzumované služby IS, napojení na integrační komponenty…<br><br>Provádí přiřazení funkčních služeb do IT komponent / domén.<br><br>Provádí přiřazení business objektů do IT komponent / domén.<br><br>Při velkých změnách architektury (náhrady komponent) obsahuje návrh nového řešení a způsob, jak nového řešení dosáhnout ve vazbě na stávající stav. | Aplikační architektura<br><br>Integrační architektura<br><br>Datová architektura<br><br>Technologická architektura<br><br>Technické předpoklady, omezení<br><br>Postup implementace a migrace |
| Bezpečnostní dokumentace[5] | Popis integrace do sítě VZP ČR s ohledem na umístění komponent v rámci segmentace komunikační sítě (dle DC zón a zón Perimetru). Popis potřeb a návrh řešení s ohledem na komunikaci mimo síť VZP ČR. Výčet služeb poskytovaných do veřejné a vnitřní sítě. | Síťová bezpečnost |
| | Popis mechanismu autentizace a autorizace uživatelů. Napojení na | Autentizace a Autorizace uživatelů |

[5] Pokud informace požadované bezpečnostní dokumentací uvedl zpracovatel v rámci jiné dokumentační oblasti, pak je v bezpečnostní dokumentaci řešeno odkazem.

| | | |
|---|---|---|
| | centrální autority autentizace a autorizace. Napojení na IDM/EIM. | |
| | Výčet použitých účtů a rolí (včetně účtů a rolí dodaných s aplikací nebo systémem nebo nebo vytvořených na základě zadání VZP ČR). Identifikace, zda je účet nebo role vytvořena lokálně, nebo převzata z centrální autority, zda se jedná o privilegovaný účet nebo roli, popis využití účtu nebo role. Matice rolí, která identifikuje nežádoucí kombinace systémových rolí (kombinace, které mohou zapříčinit zneužití přidělených oprávnění při kumulaci rolí) | Uživatelské a servisní účty |
| | Identifikace a popis informačních aktiv se kterými systém nebo aplikace pracuje a klasifikace informačních aktiv. V případě osobních a citlivých údajů popis kategorií subjektů údajů a kategorií osobních údajů, plánované lhůty pro výmaz jednotlivých kategorií údajů, účelu zpracování a právního důvodu zpracování. | Výčet primárních aktiv typu informace |
| | Při zpracování osobních informací je součástí bezpečnostní dokumentace analýza „Vliv zamýšlených operací zpracování na ochranu osobních údajů“, tedy analýza rizik a dopadů zpracování dat a dokumentů. | Vliv zamýšlených operací zpracování na ochranu osobních údajů |
| | Popis integračních vazeb (vazby na další komponenty IS VZP ČR nebo státní správy) z pohledu bezpečnosti a to specificky se zaměřením na využitý komunikační framework, popis a klasifikaci přenášených informačních aktiv, mechanismy autentizace, autorizace a auditu, způsobu zabezpečení vč. specifikace použitých šifrovacích mechanismů. | Integrační vazby |
| | V případě, že systém v rámci výměny informací využívá asymetrické kryptografie, pak jsou součástí dokumentace informace o uložení a zabezpečení privátních klíčů. | Uložení a zabezpečení privátních klíčů |

| | | |
|---|---|---|
| | Výčet zaznamenávaných bezpečnostních událostí, včetně popisu formátu, místa uložení a retence. | Bezpečnostní logování |
| | Podrobný plán obnovy systému. V případě, že systém využívá asymetrické kryptografie, pak jsou součástí dokumentace informace o zajištění zálohování a obnovy privátních klíčů. | Plán kontinuity činností |
| Testovací dokumentace | Dokumentuje průběh testování pro danou komponentu.<br>Rozsah povinné dokumentace se stanoví dle metodiky testování VZP v závislosti na charakteru komponenty, typu vývoje a správy systému, včetně postupů pro obnovu dat, jak z produkčního prostředí, tak mezi testovacími prostředími. Dále bude dokumentace popisovat návrhy řezů dat a možnosti pseudonymizace a anonymizace. | Testovací strategie<br>Testovací plán<br>Test scope - rozsah testů<br>Testovací scénáře<br>Testovací případy<br>Testovací skripty<br>Testovací data<br>Záznam o provedení testu<br>Postup na obnovu dat v testovacím prostředí<br>Postup pro vytváření řezů dat a anonymizaci/pseudonymizaci dat<br>Akceptační protokol |
| Provozní dokumentace | Provozní dokumentace potřebná k provozování a správě dodaného řešení v prostředí VZP. | Zálohování a archivace, odklady dat, obnova dat – provozní příručka<br>Monitoring – provozní příručka<br>Administrátorská příručka<br>Uživatelská příručka<br>Instalační postup<br>Konfigurační příručka<br>Tabulky předávání do provozu IT<br>Migrační dokumentace<br>Licenční politika, certifikáty<br>Řešení typických chyb a problémů |

| | | |
|---|---|---|
| | | Administrační nástroje<br><br>Pravidelná údržba, profylaxe<br><br>Popis Infrastruktury<br><br>Datový model<br><br>Kapacitní nároky – disky, HW<br><br>Popis síťového řešení |
| Zdrojové kódy | Obecné požadavky na kód:<br><br>- Snadná udržitelnost<br>- Vnitřní integrita<br>- Efektivita návrhu a zápisu<br>- Snadné další použití<br>Veškerý konfigurační kód musí být řádně okomentován tak, aby pro každý funkční modul bylo zřejmé:<br><br>- Název modulu<br>- Účel modulu<br>- Původní autor<br>- Provedené změny (datum, autor, účel změny)<br>Veškeré názvy použité v konfiguračním kódu musí být uvedeny tak, aby byl odborným specialistům zřejmý účel pojmenovaného prvku v daném kontextu. Názvy musí odpovídat jmenné konvenci jednotné pro veškerý konfigurační kód v rámci dodávky. VZP preferuje standardizovanou konvenci CamelCase.<br><br>Veškerý konfigurační kód musí být navržen v co nejjednodušší struktuře, která je zároveň čitelná a pochopitelná odborným specialistou.<br><br>Odborným specialistou se myslí pracovník, který může být získán na běžném pracovním trhu a po absolvování běžně dostupného odborného výcviku může pracovat na dalších úpravách a rozvoji dodaného informačního systému. | |

# 3 Infrastrukturní standardy

## 3.1 Obecné zásady

Standardem pro provoz aplikací je virtualizovaná infrastruktura. Virtualizace může být realizována formou virtuálních serverů, kontejnery či přímým hostingem funkcí.

Instalace aplikace na bare-metal HW je možná pouze po schválení výjimky ze strany OTP a Oddělení architektury.

Infrastruktura provozovaná formou služby není povolena.

## 3.2 HW

Vlastník kapitoly: OTP OSI

### 3.2.1 On Premise Serverová infrastruktura

Základem serverové infrastruktury, centralizované a provozované v rámci datových center (DC), jsou servery nebo serverovými systémy založené na architektuře procesoru x86. Serverová infrastruktura je postavena na neproprietálních základech (bez vazby na jediného konkrétního výrobce). Servery jsou certifikovány na operační systémy uvedené v kapitole 3. 3., musí být rozšířitelné, maximálně flexibilní a vysoce dostupné. Jednotlivé servery nebo serverové systémy jsou připojeny do sítě LAN a v případě komunikace s diskovými poli i do sítě SAN a vybaveny kvalitními nástroji pro správu. V případě používání virtualizace uvedené v kapitole 3. 3. je hardware management propojen s virtualizační vrstvou. Servery nebo serverové systémy jsou v provedení rackmount a v datových centrech jsou umístěny v rackových skříních velikosti 42U. Napájení rackových skříní se odvíjí od spotřeby zařízení, která jsou v něm umístěna.

Standardem pro připojení fyzických serverů do sítě LAN v datových centrech je:

- Management console konzole, 1x1GE, access
- Management interface, 2x1GE, acces, active-standby
- Datový interface, 2x10GE, trunk, active LACP

**On Premise SAN infastruktura**

V jednotlivých datových centrech jsou disková enterprise a midrange pole, která jsou zapojena do SAN infrastruktury pomocí SAN přepínačů. Potřebná kapacita diskových polí je řešena rozšířením těchto polí nikoliv nákupem dalších polí. Do této SAN infrastruktury jsou z důvodu vysoké propustnosti a kvalitního zabezpečení (využití alternativních cest) zapojeny všechny významné servery, zálohovací zařízení (páskové knihovny, B2D zařízení) a zmíněná disková pole. Tato SAN síť využívá u všech významných komponent minimálně 2 FC rozhraní pro zajištění vysoké dostupnosti.

#### 3.2.1.1 Podmínky pro on – premise infrastrukturu podle Třídy Aplikací

**Třída A**

Aplikace v této třídě pracují v režimu aktiv/pasiv mezi oběma lokalitami. Jsou provozované na infrastruktuře, která eliminuje dopady výpadků fyzických komponent HW. V případě výpadku celé primární lokality bude aplikace po dobu nutnou k přepnutí do záložní lokality dočasně nedostupná. Přepnutí může být provedeno buď automaticky, nebo poloautomaticky. V záložní lokalitě je připravena infrastruktura primárně využívána pro testovací prostředí, které bude v případě přepnutí produkčních aplikací omezeno, nebo vypnuto. Přepnutí do záložní lokality může mít vliv na výkonnost aplikace. Data jsou zrcadlena do záložní lokality prostřednictvím vhodné technologie.

**Třída B**

Aplikace nemusí být provozované na infrastruktuře, která eliminuje dopady výpadků fyzických komponent HW.

V případě nedostupnosti není počítáno s automatickým nebo poloautomatickým převodem do záložní lokality. Data nejsou zrcadlena do záložní lokality.

Veškeré nově implementované nebo upravované aplikace obou tříd musí umožňovat odklad dat a vytváření archivů a to jak z databázových objektů, tak z nedatabázových oblastí (z filesystémů).

## 3.3 Sítě

Vlastník kapitoly: OTP OSS

### 3.3.1 VLAN

VLANy jsou implementované v přístupové vrstvě. Uživatelé z různých oddělení, rozděleni do určených VLAN, mohou přistupovat do sítě určenými přístupovými přepínači, které jsou umístěny v různých podsítích. V hraniční, případně distribuční, vrstvě je nakonfigurované směrování těchto podsítí mezi sebou a také případné omezení provozu mezi VLANami pomoci ACL – Access Control List (přístupových listů).

### 3.3.2 QoS (QUALITY OD SERVICE)

QoS zajišťuje rovnoměrné vyvažování zátěže sítě s ohledem na druh přenášených dat, spravedlivě rozděluje konektivitu mezi jednotlivé aplikace dle nastavených priorit a zabraňuje přetížení sítě.

Ve VZP ČR jsou použity následující **QoS** třídy, které jsou řazeny dle priority – od nejvyšší priority po nejnižší prioritu.

- Třída – Network support
- Třída – Real time (VoIP RTP, VoIP Signalizace)
- Třída – 3B: Interaktivní provoz (terminálová třída) – (Aplikace Interaktivní)
- Třída – 3A: Web provoz (webová třída)
- Třída – 3D: Scavenger třída (DoS, P2P, ...) – Služby UDP (Bulk)
- Třída – Zbytková třída – ostatní provoz

### 3.3.3 Datová centra

Fyzická topologie síťové vrstvy v každém z datových center VZP ČR je tvořena dle architektury Spine and Leaf. Logická síťová vrstva je centrálně řízena pomocí clusteru controllerů. Jedná se o aplikačně řízenou infrastrukturu (Application Centric Infrastructure - ACI), která umožňuje integrovat do řízení síťového provozu datového centra vlastní logiku jednotlivých aplikací z pohledu jejich požadavků na síťovou konektivitu, bezpečnost a L4-L7 služby (load balancing, firewalling atd.).

VZP ČR používá technologii Cisco ACI.

#### 3.3.3.1 Architektura datových center

Z pohledu architektury se obě datová centra chovají jako jedno logické datové centrum, dále jen NDC – Nové Datové Centrum. NDC je v prostředí ACI vytvořeno několika tenanty (virtuálními prostředími). Pro zajištění sdílení infrastrukturních a společných služeb je využit tenant common.

Přehled použitých tenantů (prostředí):

- Sdílené služby (common) – služby sítě, AAA, management, dohled, ostatní společné síťové služby, propojení do uživatelské sítě VZP net.
- Administrativní/Management prostředí (ADM) – out-of-band management připojení, management rozhraní
- Produkční prostředí (PRO) – produkční aplikační celky

- Testovací prostředí (TSTxx) – testovací prostředí TST01 – TST12. Každé testovací prostředí je samostatným tenantem, tedy až 12 tenantů.

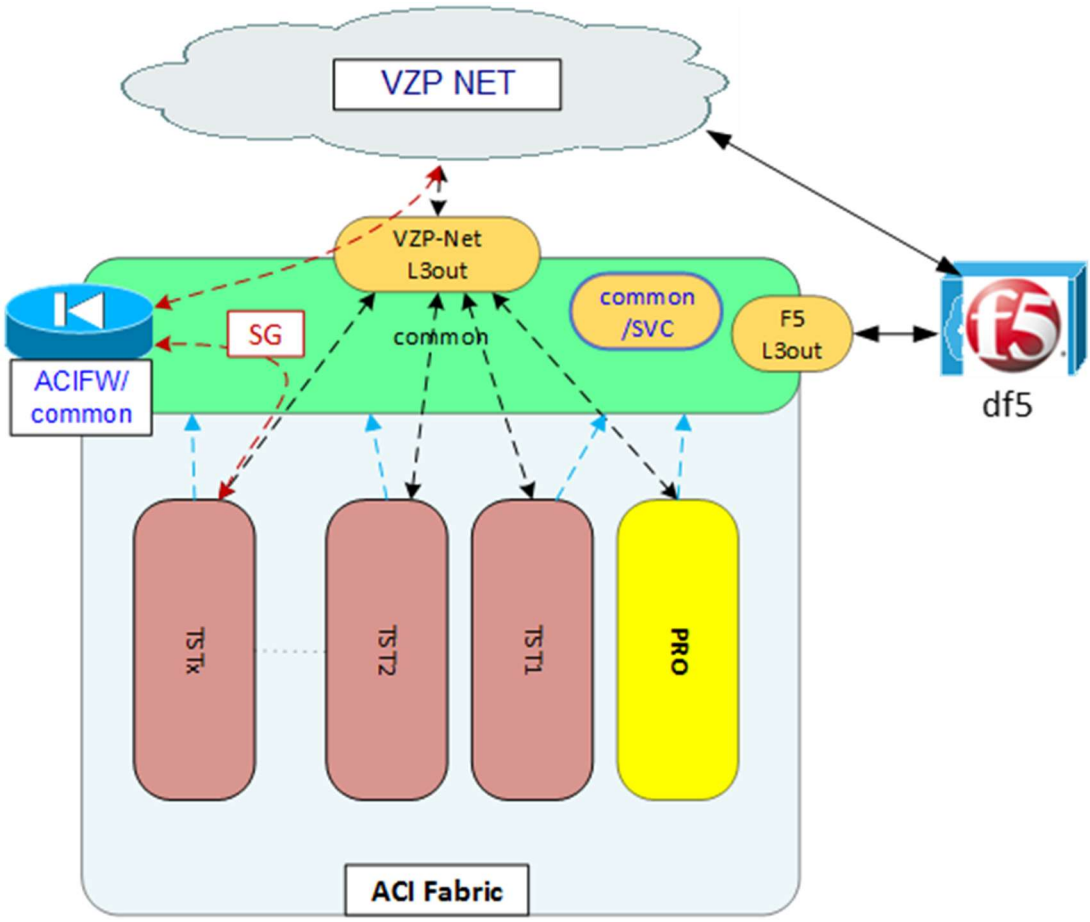
Produkční a testovací prostředí NDC je rozděleno do aplikačních celků. Každý aplikační celek je tvořen samostatným aplikačním profilem. Aplikační celek se typicky skládá z jednotlivých EPG (End Point Group) reprezentujících vrstvu aplikace:

- Webová (Prezentační) vrstva
- Aplikační vrstva (APP EPG)
- Databázová vrstva (DB EPG)
- HeartBeat vrstva

- Aplikační profil (Application Profile) je množina EPG a kontraktů/filtrů, které dohromady tvoří pravidla pro komunikaci v rámci vybrané aplikace.
- EPG je logická skupina serverů/aplikací/koncových zařízení, pro kterou jsou definovány jednotlivé politiky. V rámci EPG je standardně povolena veškerá komunikace. Mezi jednotlivými EPG je standardně veškerá komunikace zakázána a povolená komunikace je stanovena pomocí konraktů (contracts).
- Kontrakty (contracts) je skupina politik, která definuje potencionální komunikaci mezi jednotlivými EPG. Kontrakt je tvořen filtry (filters), které definují specifické protokoly a porty, které jsou povoleny v komunikaci mezi EPG.

Bezpečnostní oddělení (řízení provozu) na síťové vrstvě je zajištěno následujícími prostředky:

- East-West provoz – komunikace v rámci tenanta uvnitř ACI prostředí – je řízena pomocí standardních contractů mezi jednotlivými EPG.
- East-West provoz – komunikace mezi tenanty uvnitř ACI prostředí –probíhá výjimečně a je řízena pomocí standardních kontraktů mezi jednotlivými EPG nebo ve specifických odůvodněných případech je využit servisní graf obsahující firewall.
- North-South provoz – komunikace ze sítě VZP (administrátoři) do tenantů NDC –probíhá přes L3 out spojení, kde bude vytvořen servisní graf se zařazením firewallu pomocí PBR (Policy Based Redirect).
- North-South provoz – komunikace ze sítě VZP (uživatelé) do tenantů NDC –probíhá přes L3 out spojení přes loadbalancer F5 bez servisního grafu, tj. bez firewallu.




Obrázek: Tenanti a komunikace v ACI a mimo ACI

### 3.3.4 Perimetr

Perimetr je zabezpečená oblast podnikové sítě, která leží mezi internetem a vnitřní sítí VZP ČR. Perimetr je rozdělen pomocí bezpečnostních bran (firewallů) do několika oddělených bezpečnostních zón:

- vnější perimetr – bezpečnostní oddělení externích sítí (Internetu) od sítě VZP
- vnitřní perimetr – bezpečnostní oddělení veřejně vystavených služeb VZP od vnitřní (uživatelské) sítě VZP

Součástí řešení je i VPN přístup do VZP ČR. VPN slouží pro vzdálený přístup zaměstnanců a externích kontraktorů do sítě VZP ČR z Internetu.

### 3.3.5 Síťové služby

Síť VZP ČR poskytuje pro koncová zařízení, aplikace a uživatele následující služby:

- Časová synchronizace (NTP)
- Kvalita služby (QoS)
- DNS, DHCP, IPAM (DDI)
- Loadbalancing

## 3.4 OS

Vlastník kapitoly: OTP OSSM

V době instalace musí mít všechny implementované verze OS zajištěnu podporu ještě minimálně dalších 5 let.

### 3.4.1 OS pro aplikace třídy A

- Red Hat Enterpise Linux, Oracle Linux, CentOS (verze 7 a vyšší)
- MS Windows Server 2016

### 3.4.2 OS pro aplikace třídy B

- Red Hat Enterprise Linux, Oracle Linux, CentOS (verze 7 a vyšší)
- MS Windows Server 2016

### 3.4.3 Prostředí pro virtualizaci

Hostitelský systém je hypervizor nebo operační systém s hypervizorem , který umožní provoz Virtuálních serverů. Podporované platformy jsou a ve VZP mohou být nasazeny technologie, VMWare vSphere 6.5 Enterprise a vyšší, Oracle VM 3.4 a vyšší.

Řízení Virtuálních serverů - správa VMs na VMWare nástrojem VMWare vCenter Server 6.5 Standard a vyšší.

Pro zajištění vysoké dostupnosti aplikací třídy A pro a realizaci DRP plánu slouží technologie VMware DRS a HA cluster, případně VMware SRM.

Pro aplikace třídy A využívající softwarové produkty Oracle bude použita virtualizace Oracle VM.

U aplikací třídy B lze použít i další virtualizační technologií:

- KVM (Kernel-based Virtual Machine)

### 3.4.4 Požadavky na linuxové účty

Uvedené požadavky jsou se zdůrazněním požadavků na aplikace ve vztahu k administraci.

- Na linuxových systémech se rozlišují 2 typy účtů: uživatelské a servisní účty.
- Uživatelské účty jsou centralizované, autentizace protokolem Kerberos, autorizace protokolem LDAP. Autentifikace i autorizace je nezávislá na aplikačním IDM. Zřizovány jsou pouze za účelem správy systému, subsystémů a aplikací. Je zakázáno přidělovat uživatelské účty kvůli aplikačním přístupům (např. pro přenosy dat do/z aplikace). Na uživatelské účty se vzdáleně přistupuje protokolem ssh, autentizace heslem (možno GSSAPI).
- Servisní účty, to jsou účty dedikované pro správu, instalaci, provoz systému, subsystémů (např. Oracle db, aplikační servery, aj.) a aplikací, jsou lokální. Servisní aplikační účty (a skupiny) jsou alfabetické malými písmeny, začínají znaky ‚vzp‘, dále identifikace aplikace. Primární skupinou servisního aplikačního účtu je skupina stejného jména. S omezením na 16 znaků. UID a GID pro subsystémy a aplikace jsou přidělovány jednotně centrální autoritou VZP. Na servisní účty za účelem administrace se přistupuje pomocí sudo z běžného uživatelského účtu na základě přidělené administrátorské role (dedikovaný administrátorský LDAP). Přístup na servisní účty není povolen s autentifikací heslem.

- Instalace dané aplikace včetně tvorby unixové adresářové struktury (vlastnictví, skupiny uživatelů, práva) se provádí na základě aplikační dokumentace pomocí dodané instalační úlohy. Aplikační dokumentace musí obsahovat seznam veškerých aplikačních trustů vytvářených na úrovni systému (ssh public key trusty pro vzájemnou komunikaci, aj.). Aplikace obsahuje úlohu, která kontroluje správnost nasazení, tedy mj. i nastavení vlastnictví, skupiny uživatelů, práva v adresářových stromech aplikace. Zjištěné chyby jsou protokolovány, a pokud je to možné, automaticky opravovány.
- Veškeré aplikační struktury jsou uchovávány v dedikovaných aplikačních adresářových stromech. Pokud aplikace využívá obecné subsystémy (např. java, http server, openssl, …), musí být rovněž veškerá konfigurace a data těchto subsystémů v adresářových stromech aplikace a nezávislá na případném použití komponenty jinou souběžnou aplikací (dedikovaný port pro http server, …). Pokud nelze zajistit nezávislost použití dané komponenty, musí aplikace použít vlastní instalaci komponenty ve svém aplikačním stromě.

## 3.5 Middleware

Vlastník kapitoly: OTP OSAD

### 3.5.1 Aplikační servery

Výčet typů AS využívaných v IS VZP:

| Druh AS | Použití |
|---|---|
| Oracle Fusion Middleware WebLogic Server v nejnovější podporované verzi | Aplikace deployované v J2EE, vhodné pro aplikace třídy A |
| JBoss aplikační server v nejnovější podporované verzi | Pro J2EE aplikace třídy B nebo v odůvodněných případech, kde není vhodné použití Oracle Weblogic J2EE. |

### 3.5.2 Webové servery

Výčet typů WS využívaných v IS VZP:

- Oracle Web Tier v nejnovější podporované verzi
- Apache v nejnovější podporované verzi
- IIS

## 3.6 Virtualizovaná infrastruktura pro hostování aplikací

Vlastník kapitoly: OTP OSAD

Aplikační služby jsou hostovány na virtuálních prostředí / serverech následujících parametrů:

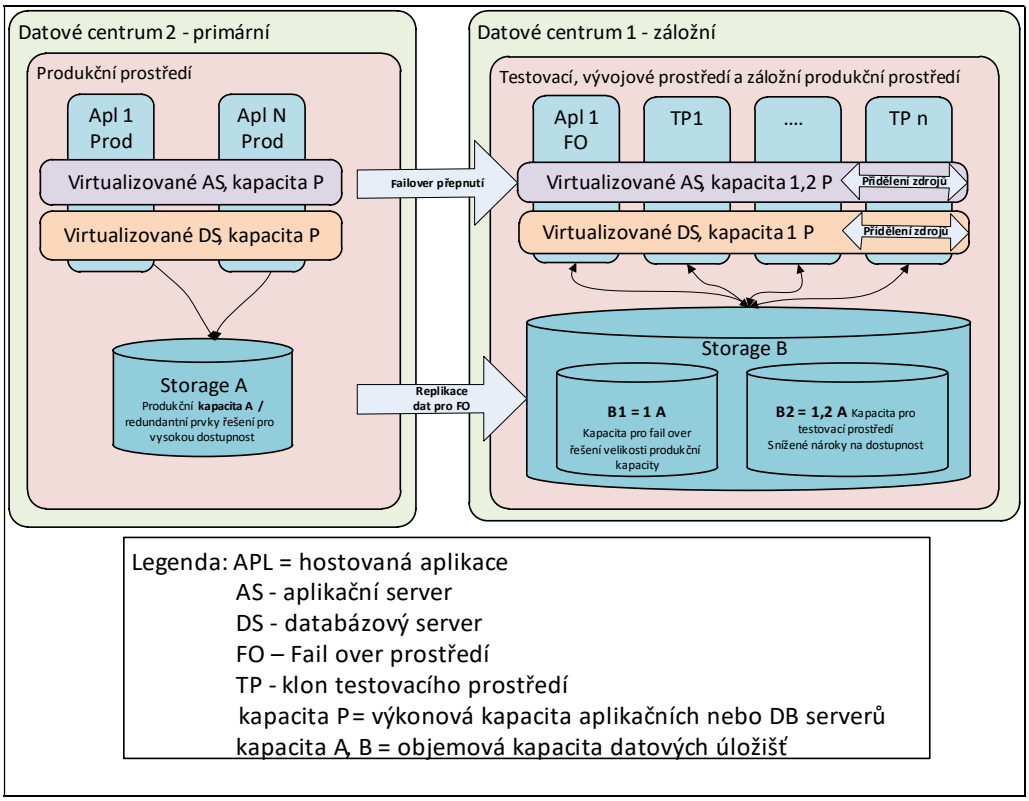
| Název služby | Popis |
|---|---|
| Server s OS | OS Windows nebo Linux (viz kap. 3.3 OS) |
| Aplikační server | OS Windows nebo Linux aplik. serveru Oracle Weblogic Suite |
| Databázový server Oracle | OS Linux, Oracle dB EE + RAC + partitioning |
| Databázový server MS SQL | OS MS Windows, MS SQL Server v edici Enterprise |

## 3.7 Deployment aplikací provozovaných on-Premise do prostředí v DC VZP

Vlastník kapitoly: OTP OSAD

Pro zabezpečení provozu aplikací v prostředí datových center je používán standardizovaný deployment aplikací:

- Produkční instance aplikací a jejich odpovídajících dat je hostována v primárním datovém centru na zařízeních s vysokou dostupností a redundancí na virtualizované infrastruktuře.
- Záložní instance aplikací je hostována ve virtualizované infrastruktuře v záložním datovém centru s dedikovanou kapacitou úložiště o velkosti produkčních dat pro fail over primárního DC.
- Virtualizovaná infrastruktura serverů záložního centra je dimenzována jako výkonový ekvivalent zařízení v primárním datovém centru. Požadavek na dostupnost je nižší, tomu odpovídá nižší redundance prvků.
- Virtualizovaná infrastruktura záložního centra je sdílena s testovacími prostředími.
- Produkční data z primárního DC jsou asynchronně replikována do záložního DC.
- Pro účely testování je v záložním DC dedikována obecně kapacita virtualizované úložné kapacity až v rozsahu 1,2 velikosti produkčních dat sdílená pro všechny instance testovacích prostředí. Tato kapacita je alokována individuálně při návrhu systému.
- Kapacita úložiště Storage B musí být 2,2 násobkem kapacity úložiště produkčního prostředí Storage A
- Kapacita HW serverů pro databázovou a aplikační vrstvu musí být výkonově dimenzována jako 1,2 násobek produkčního prostředí (měřeno součtovým počtem jader, velikostí operační paměti virtuálních serverů a diskových úložišť pro aplikační a databázovou vrstvu). Redundance komponent není nutná.



## 3.8 Datové a databázové služby

Vlastník kapitoly: OTP OSAD

### 3.8.1 Databázové technologie

| Standard | Popis |
|---|---|
| Oracle DB EE v nejnovější podporované verzi, včetně databázových options | Pro aplikace třídy A nebo B. |
| MS SQL EN/STD min. verze 2014, X64bit, standalone/cluster | Podpůrné služby a pro aplikace v třídě B. V odůvodněných případech je možné použít i pro aplikace třídy A. |

### 3.8.2 Datové a databázové standardy

| Oblast standardizace | Popis |
|---|---|
| Minimum redundancí | Data jsou uložena v jediné databázi. Redundantní databáze v rámci lokality nejsou pro core business aplikace povoleny. Replikace se provádí pouze z důvodu realizace DR plánu. |
| Jediný zdroj informací | Data jsou uložena v místě jejich vzniku, do ostatních systémů jsou poskytována prostřednictvím integrační platformy. Platí pravidlo minima duplicit. |
| Datová konzistence | Datová konzistence je zachovávána již v rámci databáze, tedy nikoliv pouze aplikačně. |
| Modelování DB pomocí ER diagramu | Jsou zachovány normálové formy. Pouze v případech, kdy je to nutné jsou možné výjimky – v dokumentaci však je explicitně uvedeno. |
| Návrh datového modelu | Návrh datového modelu DB musí být akceptován datovým architektem VZP ČR.<br>Persistentní objekty vývojář definuje bez určení:<br>• Názvu tablespace<br>• fyzických atributů segmentu (pctused, pctfree, storage params,...)<br>Databázové objekty jsou považovány za privátní součást aplikace, tzn. aplikace může přistupovat k databázovým objektům jiné aplikace pouze prostřednictvím dedikovaných služeb. |
| Jmenné konvence databázových objektů | Všechna jména základních databázových objektů (tabulky, pohledy, balíky funkcí a procedur, fronty, sekvence, indexy, triggery apod.) začínají dvouznakovým prefixem dodavatele |
| Kódování | Preferované UTF16, UTF8,<br>Definici collation – preferována Czech CI AS (case insensitive a accent sensitive)<br>Na výjimku: ISO 8859-2, Windows 1250 |
| Podpora anonymizace / pseudonymizace osobních | Datová vrstva musí podporovat možnost anonymizace a pseudonymizace osobních údajů bez nežádoucího vlivu na |

| | |
|---|---|
| údajů | chování datového engine a aplikace.<br><br>Využívá se pro účely příslušné legislativy a vytváření datového derivátu pro testování z produkčních dat.<br><br>Součástí dodávek je nástroj pro vytváření anonymizovaných derivátů produkčních dat (scrambling tool).<br><br>Toto musí být zohledněno i v dokumentaci. |
| Podpora řezů dat | Datový model musí být navržen tak, aby pro účely testování bylo možno oddělit testovací derivát – vzorek dat z produkčních dat.<br><br>Součástí dodávek je nástroj pro vytváření takových derivátů.<br><br>Toto musí být zohledněno i v dokumentaci. |
| Zakázané vazby | Data v relačních databázích nesmí být provazována technologicky přes významové klíče, povolena je relační vazba pouze přes nezávislé technologické klíče záznamů.<br><br>Nejsou dovoleny přímé datové vazby mezi datovými doménami. |

# 4 Bezpečnostní standardy

Vlastník kapitoly: OKIB

## 4.1 Dodržování legislativních požadavků

Dodávaný systém, nebo aplikace, je v souladu (po technické stránce poskytuje takové funkcionality, které VZP ČR umožní být v souladu) s níže uvedenými zákony a nařízeními:

### 4.1.1 Autorský zákon

Zákon č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů, v platném znění.

### 4.1.2 ZOKB

Zákon č. 181/2014 Sb. (Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (Zákon o Kybernetické bezpečnosti) v platném znění (zkratka ZoKB) a související Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

### 4.1.3 GDPR

„Nařízení Evropského parlamentu a Rady č. 679/2016 ze dne 27. 4. 2016“ (zkratka GDPR).

- Systém, nebo aplikace, musí umožnit splnit oprávněné požadavky subjektu údajů ve vztahu k osobním údajům, tyto údaje musí být možné vyhledat, opravit, vymazat, omezit dobu zpracování a předat ve strojově čitelné podobě jinému správci.
  - Dodavatel technický způsob zajištění uvádí v příslušné dokumentaci.
- V rámci dodávky jsou provedeny příslušné funkční testy.
- Dodavatel provede analýzu „Vliv zamýšlených operací zpracování na ochranu osobních údajů“, tedy analýzu rizik a dopadů zpracování dat a dokumentů.

## 4.2 Dodržování obecných standardů a doporučení

V rámci dodávky/vývoje je doporučeno dodržování obecně platných standardů uvedených níže. Výjimky nebo odchylky od uvedených standardů musejí být předem schváleny VZP.

- (Center for Internet Security Benchmark);
- Application Security Verification Standard;
- ISO/IEC 2700x *(ISMS)*;
- ISO/IEC 12207 *(Systems and software engineering – Software life cycle processes)*;
- ISO/IEC 15504 *(Software Process Improvement and Capability Determination (SPICE))*.

## 4.3 Minimum běžících a instalovaných služeb

Jsou nainstalovány a spuštěny pouze takové služby, které jsou pro provoz systému / aplikace nezbytné.

## 4.4 Nevyhovující služby nebo protokoly

Služby nebo protokoly, které nevyhovují bezpečnostním požadavkům pro přenos či zpracování definované kategorie citlivosti informace nesmí být pro přenos nebo zpracování informace použity.
Nevyhovuje zejména:

- použití nešifrovaných protokolů pro vzdálenou administraci (TELNET, http, atd …);
- použití nešifrovaných protokolů pro přenos dat (FTP, http, atd …);
- použití slabých a již nevyhovujících metod šifrování (SSL2, SSL3, SHA1, atd…);
- použití služeb se známou zranitelností, která není výrobcem opravena nebo je neopravitelná;
- použití služeb bez podpory výrobce (Out Of Life).

## 4.5 Synchornizace času

Systém provádí synchornizaci času s NTP servery VZP ČR (ntp1.vzp.cz, ntp2.vzp.cz, ntp3.vzp.cz) nejméně jednou za 24 hodin.

## 4.6 Kryptografie

### 4.6.1 Požadavky na kryptografické algoritmy

Kryptografické algoritmy musí splňovat doporučení NÚKIB platné ke dni 28. 11. 2018. Dokument lze získat ze stránek https://www.govcert.cz/cs/doporuceni-v-oblasti-kryptografickych-prostredku/.

### 4.6.2 Požadavky na ochranu privátního klíče

- Jakýkoliv privátní klíč uživatele musí být chráněn heslem;
- Privátní klíče musí být spolehlivě zálohovány pro případ jejich ztráty nebo poškození;
- Musí být definovány postupy pro obnovení klíče a postupy instalace nového klíče v případě nedůvěry ve starý aktuální klíč.

## 4.7 Komunikace s veřejnou sítí

### 4.7.1 Systémy, nebo aplikace, které publikují služby do veřejné sítě (inbound)

Všechny On-Premise systémy, nebo aplikace, které publikují služby do veřejné sítě (např. poskytující B2B API, webové prezentace apod.) jsou:

- umístěny ve vyhrazeném síťovém segmentu (vnitřní perimetr), který je dohledován IDS/IPS řešením a má omezené možnosti komunikace do vnitřní sítě;
- zapojeny tak, že je aplikačními firewally prováděna inspekce provozu.

### 4.7.2 Komunikace do veřejné sítě (outbound)

Všechny On-Premise systémy, nebo aplikace, které potřebují pro zajištění svého provozu komunikovat s veřejnou sítí, kromě systémů, nebo aplikací poskytujících základní infrastrukturní služby typu DNS, NTP, e-mail gw pro veřejnou síť, Proxy (vč. schválených výjimek) s veřejnou internetovou sítí nekomunikují přímo, ale pro komunikaci s veřejnou sítí využívají proxy server (proxy server zajišťuje terminaci šifrovaného kanálu a inspekci provozu).

### 4.7.3 SMTP komunikace s veřejnou sítí

- SMTP brána, která komunikuje s veřejnou sítí, musí:
- být umístěna ve vyhrazeném síťovém segmentu (vnitřní perimetr), který je dohledován IDS/IPS řešením a má omezené možnosti komunikace do vnitřní sítě;
- identifikovat nevyžádané emaily (pomocí heuristiky, RBL, reputace odesílatele, nebo kombinací těchto mechanismů) a aplikovat na ně příslušné politiky (např. odmítnutí doručení, označení zprávy jako nevyžádané apod.);
- podporovat šifrování emailové komunikace mezi emailovými servery (SMTPS);
- zabránit potenciálnímu spoofingu emailové komunikace (SPF);
- Identifikovat malware a zabránit jeho doručení (využívat sandboxingu, nebo antivirového řešení).

## 4.8 Řízení přístupu

### 4.8.1 Interní uživatelé

- Musí být zajištěno řízení přístupů k jednotlivým aktivům na základě rolí nebo profilů v nástroji pro řízení identity a autorizace přiřazené konkrétnímu identifikovanému uživateli.
- Identita interního uživatele je uchovávána v AD.
- Autentizace/ověření uživatele musí probíhat proti Active Directory.
- Autorizace interního uživatele k funkcionalitám systémů je řízena IDM (Identity Management Systém) ve kterém jsou role a profily uživatele definovány.

### 4.8.2 Externí uživatelé (např. klient VZP)

- Musí být zajištěno řízení přístupů k jednotlivým aktivům na základě rolí nebo profilů v nástroji pro řízení identity a autorizace přiřazené konkrétnímu identifikovanému uživateli.
- Identita uživatele je uchovávána v EIM (Externí Identity Management).
- Identita uživatele v systémech je řízena EIM
- Autentizace/ověření uživatele využívá EIM

### 4.8.3 Propagace identity uživatele ke koncovým službám

- Identita konkrétního uživatele je ověřena z front-endu aplikace a propagována až ke koncovým službám přes všechny technologické vrstvy IS. K tomu je využíváno předávání autorizačního tokenu mezi službami (OAuth, SAML)

### 4.8.4 Ochrana hesel a politika hesel

- Hesla nesmí být uchovávána v čitelné podobě v dávkových souborech, automatických přihlašovacích skriptech, makrech, v nechráněných souborech a všude tam, kde by mohlo dojít k jejich odhalení.
- Systém, nebo aplikace, musí zajistit ochranu hesel a vynucovat politiku hesel v souladu s požadavky ZoKB, resp. Vyhlášky 82/2018.

### 4.8.5 Mechanismus obrany proti hádání přístupu do systému

- Ve všech systémech nebo aplikacích musí být implementována kontrola proti pokusům o uhádnutí uživatelských jmen a hesel (např. prostřednictvím omezeného počtu pokusů o přihlášení a definované doby omezení přístupu do systému či aplikace).
- Po definovaném počtu neúspěšných pokusů (5 pokusů) o přístup musí dojít k automatickému uzamčení příslušného účtu. Tento požadavek se nevztahuje na systémové účty, kde by mohlo uzamčení účtu způsobit provozní problémy. Opětovné odemknutí je v kompetenci Administrátora systému nebo aplikace. Mechanismus musí být navržen tak, aby nedošlo k hromadnému zamykání a tím odepření služby.

### 4.8.6 Omezení přístupů ke službám ve vnitřní síti VZP ČR

Systémy, nebo aplikace, publikují do sítí, ze kterých k němu přistupují koncoví uživatelé, výhradně služby, které jsou koncovým uživatelům určené. Jiné služby (např. služby zajišťující integraci s jinými systémy) nesmí být nikdy ze sítí, ve kterých pracují koncoví uživatelé, dostupné.

### 4.8.7 Zobrazení varovného hlášení

V případě systému, nebo aplikace, kdy uživateli jsou pracovníci VZP a systém, nebo aplikace obsahuje chráněné informace, musí být uživatelům před dokončením procesu autentizace zobrazeno varovné hlášení, které je informuje o důsledcích jejich aktivit. Toto hlášení musí uživatele varovat, že neoprávněný pokus o přihlášení, nebo zneužití takového přístupu může vést k pracovně právnímu postihu a/nebo trestnímu stíhání a dát jim možnost proces autentizace ukončit.

Varovné hlášení musí obsahovat následující text: "Veškerá práva k systému a údajům v něm obsažených jsou vyhrazena ve prospěch VZP ČR. Vstup do tohoto systému je umožněn pouze na základě autorizovaného přístupu a při dodržování příslušných bezpečnostních pravidel. Jakékoli nakládání, přenášení nebo jiné zpracování údajů obsažených v tomto systému v rozporu s pokyny nebo souhlasem VZP ČR jsou zakázány. Aktivity v tomto systému jsou monitorovány.".

## 4.9 Ochrana informačních aktiv

Systém, nebo aplikace, musí zajistit:

- kompletnost a platnost dat při zaručeném zpracování pouze autorizovanými systémy a uživateli;
- nesmí umožnit neautorizovaný zásah do evidovaných informací / dat.

### 4.9.1 Klasifikační schéma informačních aktiv

Pro účely klasifikace informací VZP ČR je stanoveno následující klasifikační schéma informací:

- **chráněné informace** – informace, jejichž ochrana vyplývá ze zákona, nebo informace vyžadující zvýšenou úroveň ochrany na základě obchodních nebo vnitřních požadavků z hlediska dostupnosti, důvěrnosti nebo integrity,
- **interní informace** – informace související s běžným provozem VZP ČR a jednotlivých organizačních celků, které nejsou určeny ke zveřejnění a nesmějí být volně přístupné externím subjektům,
- **veřejné informace** – informace, které nevyžadují žádný zvláštní stupeň ochrany ve vztahu k zachování důvěrnosti, dostupnosti a integrity. Tyto informace mohou být volně zveřejněny i mimo VZP ČR.

Mezi **chráněné informace** patří:

- **osobní údaje** - jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.
- **zvláštní kategorie osobních údajů** - osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; do zvláštní kategorie osobních údajů spadá biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.

Tam, kde je to možné, je provedena anonymizace subjektů přiřazením jedinečného identifikátoru, který s sebou nenese žádná osobní data.

### 4.9.2 Data v klidu

- Pokud data obsahují chráněné informace, pak musí být při uložení šifrovány (v databázích a datových skladech, na souborovém systému, na páskách a dalších výměnných médiích, v mobilních zařízeních apod.).
- Pro případ zničení primárních dat musí být data zálohována a archivována. Záložní kopie musí být umístěny v geograficky vzdálené lokalitě, nebo tak, aby nehrozilo současné zničení medií a zdrojových dat.
- Zálohovaná data se musí podepisovat a používat mechanismus kontrolního součtu.
- Musí být nastaven proces pro bezpečnou likvidaci již nepotřebných dat a to tak, aby informace nešlo obnovit.

### 4.9.3 Data v pohybu

- Pokud data obsahují chráněné informace, pak musí být během přenosu po síti šifrovány.
- je doporučeno data obsahující chráněné informace podepisovat.

#### 4.9.4 Data in use – Data v použití

- Přístup k informacím musí být řízen na základě přístupových oprávnění pro jednotlivé uživatele a jednotlivá aktiva.
- Je uplatňován princip *"need to know",* do produkčních prostředí, která obsahují chráněné informace nemají např. přístup pracovníci vývoje.
- V případě, že informace obsahují osobní, nebo zvláštní kategorie osobních údajů, musí být operace (přístup a změna) nad těmito informacemi logovány.
- V neprodukčních prostředích (vývojová a testovací prostředí) nesmí být využívány chráněné informace.
- Informace v neprodukčních prostředích jsou anonymizovány, kdy Anonymizací se rozumí taková úprava, po které nelze údaje vztáhnout k určenému nebo určitelnému subjektu údajů.

#### 4.9.5 Antimalware ochrana

Ukládané dokumenty jsou testovány pomocí antiviru (systému na ochranu proti malware).

#### 4.9.6 Plán obnovy (Disaster Recovery)

Dokumentace musí obsahovat stanovení procesů, postupů a opatření pro zajištění obnovy provozu a testování DR plánů.

### 4.10 Bezpečnostní testy

#### 4.10.1 Systémy, nebo aplikace, které nepublikují služby do veřejné sítě

Systémy, nebo aplikace, které nepublikují služby do veřejné sítě, musí být ve spolupráci s dodavatelem podrobeny internímu bezpečnostnímu testování. Toto testování provádí VZP v součinnosti s dodavatelem.

#### 4.10.2 Systémy, nebo aplikace, které publikují služby do veřejné sítě

a) V případě, že je systém, nebo aplikace bude dostupná z veřejné sítě, musí dodavatel zajistit, aby byl v rámci dodávky proveden nezávislý penetrační test aplikace v rozsahu, který je v souladu s nejlepší praxí.
b) Minimálně jsou provedeny testy v těchto oblastech:

| **Oblast** | **Testy** |
|---|---|
| Brute Force Prevention | Lack of account lockout, Different login failure message, Insufficient authentication, Weak password recovery, Lack of SSL on login pages, Auto-complete enabled on pass parameters |
| Credential/Session prediction | Sequential session token, Non-Random session token, |
| Insufficient Authorization | Forcefully browse to logged in URL, Forcefully browse to high privilege URL, HTTP verb tampering, Insufficient session expiration |
| Session Fixation | Failure to generate new session ID, Permissive session management |
| Session Weaknesses | Session token passed in URL, Session cookie not set with secure attribute, Session cookie not set with HTTPOnly, Session cookie |

| | |
|---|---|
| | not sufficiently random,<br><br>Site does not force SSL connection, Site uses SSL but references insecure objects, Site supports weak SSL ciphers |
| Cross-Site Scripting | Reflected cross-site scripting, Persistent cross-site scripting, DOM-based cross-site scripting, Cross-frame scripting, HTML injection, Cross-site request forgery, Clickjacking |
| Injection Attacks | Format string attack, LDAP injection, OS command injection, SQL injection, Blind SQL injection, SSL injection, XPath injection, HTTP header injection/response splitting, Remote file includes, Local file includes, Potential malicious file uploads |
| Information Disclosure | Directory indexing, XML External Entity |
| Information Leakage | Detailed application error messages, Include file source code disclosure, Path traversal, Predictable resource location, Insecure HTTP methods enabled, WebDAV enabled, Default web server files, Testing and diagnostics pages, Internal IP address disclosure, Server-Side Request Forgery (SSRF) |

c) Do doby provedení penetračních testů a odstranění nálezů plynoucích z těchto testů nesmí být aplikace veřejně dostupná (technickými prostředky je zajištěno, že je aplikace dostupná pouze subjektu, který provádí testování). Protokol s výsledky testů předkládá dodavatel VZP ČR. Protokol obsahuje metodiku testů, výčet použitých nástrojů při provedení testů, výčet dílčích testů (dokladuje, které testy byly provedeny) a výsledky testů.

Na základě výsledků testů VZP ČR rozhoduje o akceptaci testovaných komponent IS a jejich uvedení do provozu.

# 5 Logování

Tato kapitola definuje požadavky na logování v oblastech:

- **Bezpečnosti**:
  - Základní úroveň logování z pohledu bezpečnosti;
  - Logování transakcí při zpracování osobních a zvláštních kategorií osobních údajů.
- **Komunikace a Business logiky**:
  - Transakční logy.
- **Provozu:**
  - Provozně-aplikační logy.

Pro zalogování událostí do správného logu nebo i do více logů se použije následující logika zařazení události:

| **Událost související s:** | **Oblast logování** |
|---|---|

| | |
|---|---|
| Autentizací | Bezpečnost |
| Přístupovými oprávněními | Bezpečnost |
| Privilegované přístupy | Bezpečnost |
| Operace se soubory | Bezpečnost |
| Exporty dat | Bezpečnost |
| Operace s auditními záznamy | Bezpečnost |
| Operace s osobními daty | Bezpečnost |
| Stavem aplikace (chyby, výjimky) | Provoz |
| Stavem infrastruktury | Provoz |
| Výkonostní aplikace | Provoz |
| Komunikace s dalšími aplikacemi, použití datových rozhraní | Komunikace |

Událost může patřit do více než jednoho logu, tedy bude zalogována do více logů.

## 5.1 Požadavky

### 5.1.1 Formát a encoding logu

a) Preferovaný format logu je v případě vývoje aplikace specificky pro VZP ČR JSON (JavaScript Object Notation), **v ostatních případech je formát dán výrobcem** a jeho použití musí být schváleno VZP ČR.
b) Doporučený encoding logu je UTF-8, v ostatních případech je nutné schválení encodingu VZP ČR.

### 5.1.2 JSON - doporučené pojmenování klíčů a identifikace datové struktury

a) Každý záznam musí obsahovat klíč "`source_type`", který identifikuje datovou strukturu události (přiřazení záznamu příslušné doméně zájmu).
b) Každý záznam by měl obsahovat klíč "`event_type`", který identifikuje specifickou událost.
c) Pokud je nutno zaznamenat informace, pro které není vhodné použití žádného z uvedených klíčů, pak dodavatel vytváří vlastní klíč:
   i. Klíče jsou pojmenovávány v angličtině.
   ii. Informace o nově vzniklém klíči a jeho účelu je součástí příslušné dokumentace.

### 5.1.3 Obecně platné zásady pro logování

a) Každý záznam je označen časovým razítkem vytvoření / modifikace záznamu.
b) Logované informace musí odpovídat aktuálnímu stavu systému, interpretace logů musí proveditelná bez dodatečných datových zdrojů. Pokud je logovaná hodnota z číselníku loguje se jak klíč tak i odpovídající hodnotu, které se vždy vztahuji k danému časovému okamžiku.
c) Každá komponenta, která se podílí na zpracování transakcí (včetně volání integračních služeb a rozhraní ) bude logovat do lokálního transakčního logu. Do transakčního logu se zaznamenávají minimálně události volání a ukončení služby.

5.1.3.1 Časové razítko

a) Každý záznam obsahuje časové razítko vzniku události.
b) Preferovaný format časového razítka je: "`YYYY-MM-DD hh:mm:ss`", pokud není požadováno jinak, je uvedený čas vždy platný v zóně Europe/Prague. Příklad: "`2019-03-14 11:02:39`".
c) Další možný format časového razítka je ve formátu, ve kterém jej do logu zapisuje operační system, na kterém je aplikace spuštěna (UNIX/Linux: "`Mar 12 13:31:45`", Windows "`15.03.2019 9:31:40`").
d) Ostatní formáty zápisu časového razítka musí být v souladu s ISO 8601 a jejich použití musí být schváleno VZP ČR.

### 5.1.4 Technické zajištění logování

5.1.4.1 On-Premise

a) Logový soubor musí být lokální, tj. agent nemůže k logu přistupovat pomocí síťového protokolu na sdíleném prostředí. To nevylučuje vzdálené plnění logu. Jako nepřípustný pro automatizovaný monitoring je log v podobě průběžné databázové tabulky nebo pohledu.
b) Pokud je aplikace nasazena na OS Unix/Linux, pak musí logovat s využitím souborového systému a musí zajistit rotaci logů, nebo využívá mechanismu syslog.
c) Pokud je aplikace nasazena na OS Windows, pak musí logovat s využitím souborového systému a musí zajistit rotaci logů, nebo používá mechanismu Windows Event logu.
d) Musí být zajištěno, aby velikost jedné zprávy nepřekročila 65507 bajtů.
e) Preferovaný mechanismus pro zajištění persistence logů generovaných kontejnery Docker je využití Docker Volumes.

### 5.1.5 Retence logů

V případě, že logy nejsou předávány do Centrálního úložiště logů nebo SIEM nástroje, musí být zajištěna kapacita pro dostatečně dlouhé uložení logů, to znamená:

a) všechny logy jsou online uchovány minimálně po dobu 30 dní;
b) logy, které obsahují informace v souladu s požadavky ZoKB, resp. Vyhlášky 82/2018 jsou k dispozici minimálně po dobu 18 měsíců;
c) logy, které obsahují informace o přístupech k osobním údajům nebo k zvláštní kategorii osobních údajů, jsou k dispozici minimálně po dobu 36 měsíců.

### 5.1.6 Dokumentace

Dodavatelem je předána dokumentace, která obsahuje:

a) výčet auditovaných událostí;
b) vzorky událostí;
c) při použití JSON formátu názvy použitých klíčů vč. jejich popisu;
d) způsob uložení (místo uložení na souborovém systému);
e) zajištění retence a rotace;
f) nastavení přístupových práv.

## 5.2 Základní úroveň logování z pohledu bezpečnosti

Vlastník kapitoly: OKIB

Pokud jsou záznamy ve formátu JSON, pak každý záznam musí obsahovat následující klíč a kodnotu: "`source_type`": "`security`".

### 5.2.1 Logování procesu autentizace

Požadavek zaznamenat proce autentizace se týká všech komponent IS VZP ČR, které v jakékoli formě implementují proces autentizace (včetně API).

| Auditovaná operace | event_type | Popis |
|---|---|---|
| Přístup do systému nebo aplikace | login | Jsou zaznamenány všechny oprávněné i neoprávněné pokusy o přístup. |
| Ukončení práce v systému nebo aplikaci | logout | Je zaznamenáno, kdy byla ukončena práce se systémem - včetně situace, kdy bylo provedeno automatické odhlášení po uplynutí stanovené doby nečinnosti. |

#### 5.2.1.1 Příklad logu procesu autentizace u aplikace

Příklad logu procesu autentizace u aplikace, která implementuje vlastní logování a log ukládá do souboru:


```
{ "time_stamp": "2019-03-14 11:02:39", "host_fqdn": "server1.vzp.cz", "host_ip": "172.16.0.1", "source_type": "security", "application": "my_app1", "environment": "prod", "source_class": "VZP_USER", "source_uid": "user1", " source_host": "client1.kz.vzp", "source_host_ip": "172.16.1.1", "source_interface": "UI", "event_type": "login", "auth_method": "password", "auth_provider": "ldap", "result": "false", "error_descr": "invalid user" }
```


### 5.2.2 Činnosti provedené administrátorem

Komponenty IS VZP ČR, které zpracovávají, ukládají, nebo přenáší informace s klasifikací interní a vyšší, musí zaznamenávat:

| Auditovaná operace | event_type | Popis |
|---|---|---|
| Činnost administrátora | activity | Jsou zaznamenány činnosti administrátora. |

#### 5.2.2.1 Příklad logu činnosti provedené administrátorem

Příklad logu činnosti provedené administrátorem v systému, který implementuje vlastní logování a pro uložení logu využívá syslog:


```
Mar 14 11:02:39 server1 user1: { "time_stamp": "2019-03-14 11:02:39", "host ": "server1.vzp.cz", "host_ip": "172.16.0.1", "source_type": "security", "application": "os_linux", "source_uid": "user1", "event_type": "activity", "uid": "root", "gid": "root", "groups": "root", "pid": "17783", "shell": "bash", "activity": "tail -f /var/log/messages", "result": "true" }
```


### 5.2.3 Změny přístupových oprávnění a změny údajů, které slouží k přihlášení

Komponenty IS VZP ČR poskytující služby autentizace nebo autorizace musí zaznamenávat:

| Auditovaná operace | Popis |
|---|---|
| Změny stavu účtu | Přidání, odebrání, zneplatnění, povolení, nebo uzamčením účtu administrátorem (včetně uzamčení účtu po několika neúspěšných pokusech o autentizaci). |
| Změny rolí přiřazených účtu | Přidání, nebo odebrání role uživatelskému účtu. |
| Přidání, změna nebo odebrání *definice* role | Jsou zaznamenány všechny aktivity související s přidáním, změnou, nebo odebráním definice role. |

### 5.2.4 Neprovedení činnosti v důsledku nedostatku přístupových oprávnění

Komponenty IS VZP ČR, které zpracovávají, ukládají, nebo přenáší informace s klasifikací interní a vyšší, musí zaznamenávat:

| Auditovaná operace | Popis |
|---|---|
| Neprovedení činnosti | Je zaznamenáno, pokud aktivitu nebylo možno provést v důsledku nedostatečných přístupových oprávnění. |

### 5.2.5 Přístupy k záznamům o činnostech

Komponenty IS VZP ČR, které zpracovávají, ukládají, nebo přenáší informace s klasifikací interní a vyšší, musí zaznamenávat:

| Auditovaná operace | Popis |
|---|---|
| Operace nad auditními záznamy | Komponenty IS VZP ČR musí zaznamenávat pokusy o manipulaci s auditními záznamy a konfigurací auditní služby (v rámci logování přístupu k souborům), včetně zastavení a spuštění mechanismů sloužících pro záznam těchto činností. |

### 5.2.6 Operace se soubory

Pokud soubor obsahuje chráněné informace, pak musí být zaznamenány operace vytvoření, smazání, čtení a zápisu, včetně identifikace uživatele, který operace vykonal.

| Auditovaná operace | Popis |
|---|---|
| Operace se soubory | Jsou zaznamenány operace vytvoření, smazání, čtení a zápisu souboru včetně výsledku operace. |
| Exporty | Pokud aplikace umožňuje exportovat chráněné informace prostřednictvím UI, pak jsou zaznamenány události exportu dat (uložení dat mimo určenou aplikaci). |

### 5.2.7 Vybrané JSON klíče pro záznam události

| Název | Typ | Popis |
|---|---|---|
| time_stamp | DATETIME | Datum a čas zpracování transakce. |
| host | VARCHAR2 | FQDN zařízení, na kterém událost vznikla. |
| host_ip | VARCHAR2 | IP zařízení, na kterém událost vznikla. |
| source_type | VARCHAR2 | Identifikuje datovou strukturu události. |
| application | VARCHAR2 | Jednoznačný identifikátor aplikace, pro kterou záznam vznikl, dle katalogu aplikací (např. application = “crp”). |
| environment | VARCHAR2 | Identifikace prostředí (prod\|dev\|test). |
| source_class | VARCHAR2 | Typ původce, který inicioval transakci. Může to být například zaměstnanec VZP (VZP_USER), automatická úloha (VZP_JOB), zdravotnické zařízení (ZZ), zdravotní pojišťovna |

| | | |
|---|---|---|
| | | (ZP) atd. |
| source_uid | VARCHAR2 | V případě zaměstnance VZP ČR uživatelské jméno, v případě zdravotnického zařízení kód IČZ, v případě zdravotní pojišťovny kód ZP. |
| source_host | VARCHAR2 | Identifikace zařízení (prostředku), ze kterého byla transakce iniciována (FQDN PC nebo serveru, případně reference požadavku IPF). |
| source_host_ip | VARCHAR2 | Pokud je zařízení (prostředek) PC, nebo server, je uvedena IP adresa prostředku. |
| source_interface | VARCHAR2 | Identifikace volajícího rozhraní (např. UI, IPF, CRON). |
| event_type | VARCHAR2 | Typ události. |
| result | BOOLEAN | Výsledek operace (true == provedeno\|false == selhalo). |
| error_descr | VARCHAR2 | Upřesnění chyby v případě selhání. |

## 5.3 Logování transakcí při zpracování osobních a zvláštní kategorie osobních údajů

Vlastník kapitoly: OKIB

Pokud tranakce provádí operace, které lze vztáhnout k určenému nebo určitelnému subjektu údajů, jsou vždy zaznamenávány auditní informace, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní nebo zvláštní kategorie osobních údajů, zaznamenány nebo jinak zpracovány. Vždy je rovněž zaznamenán výčet primárních aktiv typu informace, které se transakce účastní.

Nad rámec transakcí zpracování osobních údajů a zvláštní kategorie osobních údajů údajů jsou zaznamenávány náhledy a změny zdravotní pojišťovny vzhledem k přímé vazbě na zpracování OÚ a pro možné prošetřování zejména neoprávněné přeregistrace ke zdravotní pojišťovně, případně provedené změny bez vědomí a souhlasu pojištěnce.

Záznamy transakcí při zpracování osobních údajů ve formátu JSON musí obsahovat identifikaci datové struktury `“source_type”: “data_access”` a identifikaci události `“event_type”:` s výčtovou hodnotou `“data_create” OR “ data_read” OR “data_update” OR “data_delete”` (CRUD).

a) Logování zajistí komponenta, která je původcem transakce.
b) Vždy je zajištěna jednoznačná identifikace iniciátora transakce a to i při zřetězení transakce.
c) Ze zaznamenané tranakce musí být zjevné, zda je událost vyvolána interakcí uživatele s UI, nebo zda se jedná o automatizovaný proces.
d) Pro zaznamenání, z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, je využit číselník důvodů.

### 5.3.1 Vybrané JSON klíče pro záznam události

| **Název** | **Typ** | **Popis** |
|---|---|---|
| reason | VARCHAR2 | Z jakého důvodu byly osobní údaje, nebo zvláštní kategorie osobních údajů zaznamenány, nebo jinak zpracovány. |
| subject_id | VARCHAR2[] | Identifikátor subjektu, nebo subjektů tak, jak jej využívá aplikace. |

| | | |
|---|---|---|
| subject_attr | VARCHAR2[] | Výčet konkrétních informačních aktiv, které se účastní transakce. |
| file_name | VARCHAR2 | Jméno souboru, pokud se účastní transakce. |

### 5.3.2 Příklad logu činnosti nahlížení

Příklad logu nahlížení údaje subjektu z UI aplikace:


```
{ "time_stamp": "2019-03-14 11:02:39", "host": "server1.vzp.cz", "host_ip": "172.16.0.1", "source_type": "data_access", "application": "my_app1", "environment": "prod", "source_class": "VZP_USER", "source_uid": "user1", "source_device": "client1.kz.vzp", "source_device_ip": "172.16.1.1", "source_interface": "UI", "event_type": "data_read", "result": "true", "reason": "kontrola údajů klienta, žádost klienta", "subject_id ": "54a2ca2e4f47e95870cdcd9b216588d7", "subject_attr": { "pojistenec": [ "cisloPojistence", "jmeno", "prijmeni", "datumNarozeni" ], "aktualniAdresa": [ "ulice", "obec", "psc", "stat" ] } }
```


### 5.3.3 Příklad logu činnosti změna

Příklad logu změny zdravotní pojišťovny z UI aplikace:


```
{ "time_stamp": "2019-03-14 11:02:39", "host": "server1.vzp.cz", "host_ip": "172.16.0.1", "source_type": "data_access", "application": "my_app1", "environment": "prod", "source_class": "VZP_USER", "source_uid": "user1", "source_device": "client1.kz.vzp", "source_device_ip": "172.16.1.1", "source_interface": "UI", "event_type": "data_write", "result": "true", "reason": "přeregistrace klienta k jiné ZP", "subject_id ": "54a2ca2e4f47e95870cdcd9b216588d7", "subject_attr": { "zdravotniPojistovna": [ "kod", "nazev" ] } }
```


## 5.4 Základní požadavky na logování komunikace a business logiky- Transakční log[6]

Vlastník kapitoly: OAVRZ

Každá komponenta, která se podílí na zpracování transakcí včetně volání služeb ESB bude logovat do lokálního transakčního logu. Do logu se zaznamenávají minimálně události volání a ukončení služby. Výčet zaznamenávaných událostí odpovídající business logice je povinnou součástí návrhu a dokumentace systému.

### 5.4.1 Informační obsah události zaznamenávané v transakčním logu

Pokud jsou záznamy ve formátu JSON, pak každý záznam musí obsahovat následující klíč a kodnotu: `“source_type”: “transaction”`.

| **Auditovaná událost /operace** | **Popis** |
|---|---|
| Volání rozhraní aplikační komponenty | Komponenty IS VZP ČR musí zaznamenávat volání svého aplikačního rozhraní. |
| Zápis a čtení zpráv do/z fronty zpráv | Komponenty IS VZP ČR musí zaznamenávat předávání dat pomocí front (mesagingu) |

[6] Pro vyhodnocení Transakčních logů je nezbytnou podmínkou zapnutí logování ESB, kdy vlastní vyhodnocení bude probíhat technologicky v nástroji, který propojí informace z Aplikačního auditního logu a logování ESB.

| | |
|---|---|
| Synchronizace dat pomocí rozhraní pro dávkové zpracování | Komponenty IS VZP ČR musí zaznamenávat výměnu dat pomocí dávkového zpracování dat (ETL, file sync apod.) |
| Směrování zpráv v rámci integrační platformy | Komponenty IS VZP ČR musí zaznamenávat případné podmíněné směrování zpráv, případně volání. Relevantní zejména pro integrační vrstvu (ESB, BPEL engine apod.) |
| Transformace zpráv | Komponenty IS VZP ČR musí zaznamenávat transformace zprávy na jiný formát. Relevantní zejména pro integrační a proxy komponenty. |

### 5.4.2 Vybrané JSON klíče pro záznam události

| **Název** | **Typ** | **Popis** |
|---|---|---|
| time_stamp | DATETIME | Datum a čas zápisu záznamu |
| source_type | VARCHAR2 | Identifikuje typ události. |
| host | VARCHAR2 | FQDN zařízení, na kterém událost vznikla. |
| application | VARCHAR2 | Jednoznačný identifikátor aplikace, pro kterou záznam vznikl, dle katalogu aplikací (např. application = “crp”). |
| environment | VARCHAR2 | Identifikace prostředí (prod\|dev\|test). |
| app_interface | VARCHAR2 | Identifikace použitého rozhraní, zahrnuje typ rozhraní |
| service_id | VARCHAR2 | Identifikátor použité služby – tím je myšleno ID(uri) rozhraní / ID fronty zpráv apod. |
| instance_id | VARCHAR2 | Jednoznačný identifikátor instance dané transakce/služby přidělovaný zapisující službou / aplikací |
| com_partner | VARCHAR2 | Jednoznačný identifikátor protistrany komunikace podle katalogu aplikací (pokud je znám) |
| | | |
| transaction_id | VARCHAR2 | Identifikátor primární business transakce – události předávaný přes všechna volání |

| | | |
|---|---|---|
| | | podřízených služeb |
| partner_id[7] | VARCHAR2 | Technologický identifikátor partnera, kterého se volání služby týká, předávaný přes všechna volání podřízených služeb. |
| source_uid | VARCHAR2 | Identifikace uživatele, který spustil primární službu. Předávaný přes všechna volání podřízených služeb. |
| result | BOOLEAN | Výsledek operace (true == provedeno\|false == selhalo). |
| result_code | VARCHAR2 | Výstupní stav dané instance transakce/služby kód stavu |

### 5.4.3 Příklad transakčního logu

Příklad záznamu volání aplikace přes webové rozhraní


```
{ "time_stamp": "2019-03-14 11:02:39", "host": "server1.vzp.cz", "host_ip": "172.16.0.1",
"source_type": "transaction", "application": "my_app1", "environment": "prod", "app_interface": "SOAP",
"service_id": "soa-infra/services/ZakladniRegistry/AiscCtiAifo/client", "instance_id":
"a4567gdsfx4460", "com_partner": "B2B_proxy", "transaction_id": "a02546456fd464d45s46z1x",
"partner_id": " client1.kz.vzp ", "source_uid": " user1 ", "result": "true", "result_code": "200 OK" }
```


## 5.5 Provozní log

### 5.5.1 Základní požadavky na provozní logování – Provozní log

### 5.5.2 Formát logovacího souboru provozního logu

Formát provozních logů je specifický z důvodu specifických požadavků na rychlé a automatizované zpracování:

- Formát souboru je v podobě cleartext souboru operačního systému v některém z obecně používaných formátů (Syslog, Common / Combined Log Format,…), resp. ve formátu Windows Event Log, případně lze použít dohodnutý formát.
- Oddělovačem je svislé lomítko „|“ (vertical bar, ASCII 124);
- Žádné z polí zprávy by nemělo obsahovat diakritiku, pokud to není nutné např. z důvodu přenosu textu chybové zprávy z programu a jeho prostředí.

[7] ID_PARTNER slouží k logování pro GDPR, 101/2000 Sb. a ZoKB jako zdroj informaci o žádajícím subjektu při zpracování. Vlastní logování zpracovávaných osobních údajů (subjektů), kterých se daná transakce týká zajistí komponenta, která je původcem dané transakce

Popis polí provozního logu:

| Název | Popis |
|---|---|
| time_stamp | Datum a čas zápisu záznamu ve formátu dle kapitoly 5.1.3.1 Časové razítko |
| severity | Hodnocení závažnosti události viz níže. |
| Proces | Proces, ke kterému se vztahuje událost, nepovinné |
| object | objekt, který je zdrojem zprávy (např. program, název certifikátu, apod.), nepovinné |
| text | text zprávy, obsahující popis události a případné chyby |

5.5.2.1 Závažnost provozní události podle výsledku operace

| Závažnost | Popis |
|---|---|
| Critical | Fatální chyba, např. nemožnost spustit operaci, kdy je nutný zásah v co nejkratší době. |
| Major | Výsledek operace je selhání operace, např. neúspěchu posledního z pokusů o přenos, kdy je nutný zásah, např. manuální zpracování. |
| Minor | Neúspěch běhu operace, operace bude opakována, nebo nastala dílčí chyba, která nemusí znamenat neúspěch celé akce. Je žádoucí kontrola průběhu. |
| Warning | Zjištění problémů u operace s úspěšným výsledkem nebo jiná upozornění, která vyžadují příležitostné prověření. |
| Normal | Úspěšné dokončení operace. |

# 6 Provozní standardy

## 6.1 Monitoring

Vlastník kapitoly: OTP OCD

### 6.1.1 Rozsah monitoringu a používané nástroje

Rozsah monitoringu a používané monitorovací nástroje jsou popsány v dokumentu Stav IS VZP.

### 6.1.2 Používané dohledové nástroje pro On premise řešení

Centrální systém dohledu provozu informačního systému je vybudován na platformě **HP Operations Manager** (HP OM). Do dohledového centra HP OM (centrální konzole) jsou soustřeďovány všechny důležité zprávy z ostatních monitorovacích nástrojů.

**HP OM** – agent na úrovni OS, centrální konzole
**HP OM Performance Manager (PM)** – sledování vytíženosti systémů
**Oracle Enterprise Manager Cloud Control (OEM)** – agent, integrace vybraných událostí do HP OM
**Microsoft System Center 2012 Operations Manager (SCOM)** – agent na úrovni OS, integrace vybraných událostí do HP OM
**Nagios** – bezagentní, s integrací vybraných zpráv do HP OM

**HP Business Service Management (HP BSM)** – integrace do HP OM
- **Business Process Monitor (BPM)** – aktivní aplikační monitoring

**HP Network Node Manager i (HP NNMi)** – aktivní SNMP poll, pasivní SNMP trap, je integrován s HP OM

**HP SiteScope** – bezagentní, integrace do HP OM a HP BSM

Není-li možné nasadit monitoring pomocí zavedených nástrojů, poskytne dodavatel v rámci dodávky aplikace monitorovací nástroj (například skript), jehož výstup lze integrovat do HP OM.

### 6.1.3 Požadavky na procesy z hlediska monitoringu

Aplikační monitoring musí být součástí nasazovaného systému.

Kritické a závažné chybové stavy procesů/aplikací, které brání jejich provozu, dále chyby automatizovaných a dávkových zpracování musejí být zapisovány do aplikačního logu. Formát logu je popsán v kapitole 5.5 Provozní log.

Obchodně kritické procesy by měly mít implementovánu striktně čtecí roli pro technologického uživatele monitoringu, pokud tomu nebrání samotná povaha procesu (např. plně aktivní operace). Tato role musí umožnit i odstraňování případných sestav vytvářených uživatelem.

Součástí akceptačních testů musí být ověření funkčnosti monitoringu.

### 6.1.4 Požadavky na návrh monitoringu

Každá nově dodávaná aplikace nebo komponenta infrastruktury musí být monitorována, a to před nasazením do provozu. Návrh sledování dostupnosti, resp. chybovosti, jakož i výkonnosti musí být součástí projektových dokumentů (analýzy, technického designu, funkčního designu, implementační dokumentace) a zejména administrátorské a provozní dokumentace.

Návrh monitoringu vychází z doporučení dodavatele a je vypracován v součinnosti s VZP. Musí vycházet z popisu systémů, služeb a procesů aplikace, včetně návazností na ostatní systémy, a musí obsahovat zejména:

- způsob zjišťování stavu každé důležité komponenty / služby aplikace,
- návrh prahových hodnot nebo ukazatelů stavu,
- závažnost zjištěné události,
- prioritu řešení události,
- instrukce k řešení události.

Řešení monitoringu musí být navrženo tak, aby sledovaných událostí bylo co nejméně a sledování bylo proaktivní; události musejí včas upozornit na mezní stavy, aby bylo možné s předstihem zabránit výpadku služby, avšak nikoli za cenu inflace nevýznamných zpráv.

V HA aplikacích je nutné popsat režim, v němž jsou redundantní komponenty konfigurovány (loadbalance / failover) a určit závažnosti výpadků komponent a souvislosti kombinací těchto výpadků.

### 6.1.5 Požadavky na rozhraní pro monitoring

Všechny servery musejí na úrovni operačního systému umožňovat nasazení některého z agentů používaných dohledových nástrojů; spolu s agentem budou implementovány standardizované

šablony s nastavenými prahovými hodnotami, které je možné na základě doporučení dodavatele upravit.

Všechna klíčová síťová zařízení musejí mít implementován protokol SNMP v. 3+ s možností hlášení událostí pomocí SNMP TRAP i GET, a s dostupnou MIB.

V případě monitorování pomocí logů (systémových, aplikačních apod.) musí být log vytvořen podle kapitoly 5.5 Provozní log

## 6.2 Zálohování a archivace

Vlastník aplikace: OTP OSSU

Všechna DC jsou zálohována jedním společným zálohovacím subsystémem (dále jen ZS).

### 6.2.1 Zálohovací systém

ZS je tvořen těmito komponentami:

- Řídící SW „Data Protector“.
- Cluster dvou serverů v oddělených lokalitách, na nichž je řídící SW provozován.
- HW pro ukládání zálohovaných dat, umístěný rovněž ve dvou různých lokalitách (DC), dostupný pomocí LAN a SAN infrastruktury. Jsou používány robotické páskové knihovny, které mohou být v případě potřeby doplněny o jiný HW (např. typu B2D), připojitelný pod řídící zálohovací software.

Zálohování probíhá tak, aby byla respektována bezpečnostní zásada „3-2-1“ (tj. „důležitá data musí existovat 3x, ve 2 různých datových formátech, 1 kopie ve druhé lokalitě“) dle příslušné třídy aplikace.

### 6.2.2 Požadavky na aplikační celky z pohledu jejich zálohování:

Aplikace musí být navržena tak, aby:

- SW a HW komponenty aplikačních celků byly zálohovatelné technologiemi, které má VZP ČR v době nasazení aplikace a během jejího provozování k dispozici, v souladu s bezpečnostními standardy VZP ČR. Zálohovatelné musí být všechny SW komponenty a datové objekty potřebné pro činnost aplikace, a to s ohledem na předpokládané datové objemy, případné odstávky, propustnost potřebné infrastruktury a dobu potřebnou pro provedení záloh. Součástí dodávky aplikace musí být i analýza vývoje předpokládaných zálohovaných datových objemů.
- Umožňovala a podporovala datové odklady na jiná úložiště nebo zálohovací média. Musí tedy umět připravit data určená k odkladu/archivaci (např. umístit je do dohodnuté lokace, vhodně je pojmenovat, …) a vést o nich potřebnou evidenci po provedení odkladu. Musí být také možné v případě potřeby takto odložená data po jejich obnově aplikaci opět zpřístupnit.
- Bylo možné omezit pravidelně zálohovaný datový objem (uspořádání dat do read-only datových objektů, které po jejich finální záloze sice mohou ležet na discích, ale již se dále nezálohují).
- Bylo možné identifikovat změny v datech, provedené od poslední zálohy
- Hodnoty parametrů RTO a RPO pro aplikační celky byly v souladu s platnými D+R a BC plány VZP ČR, a to i s ohledem na budoucí očekávané zálohované/obnovované datové objemy a datovou propustnost příslušné infrastruktury.

- Je-li pro tvorbu záloh třeba odstávka, součástí dodávky musí být potřebné nástroje, které umožní takové zálohy provádět automatizovaně.
- Jsou-li pro zálohování třeba nějaké další SW komponenty (přípravné scripty, programy třetích stran, …), musí být také součástí dodávky aplikace.
- Je-li pro zálohování některé části aplikačního celku potřeba příslušná zálohovací licence pro požadovaný typ zálohy (typicky pro online zálohy DB, Exchange, …), při nových dodávkách aplikačních celků ji zajišťuje VZP ČR, dodavatel aplikace však vždy musí v nabídkách a dalších dokumentech specifikovat, jaké typy záloh (s ohledem na námi používané technologie) budou požadovány.

*Vysvětlivky:*

*RTO = Recovery Time Objective … doba výpadku postižených služeb v případě obnovy*

*RPO = Recovery Point Objective … k jakému času lze data obnovit, která data bude třeba po obnově nahradit (datové změny od poslední zálohy), případně která nahradit nepůjdou*

## 6.3 Definice provozních parametrů služby/aplikace (SLA)

Vlastník kapitoly: OTP OSAD

SLA a provozní parametry příslušné aplikace/domény budou součástí v technické specifikace příslušné komponenty (definované smluvně).

Využívané hodnoty:

**Provozní doba aplikace** – doba, kdy běží servery a aplikace

Režim provozní doby (7x24, 7x16, 5x16, 5x8)

**Podporovaná provozní doba** - doba, kdy provozní oddělení IT VZP zajišťuje personálně provoz aplikace

Režimy podporované provozní doby: 7x24, 7x16, 5x16, 5x8

**Doba podpory externím dodavatelem** - doba, po kterou je dostupná podpora dodavatele

Režim doby podpory externím dodavatelem (7x24, 7x16, 5x16,5x10, 5x8)

**Servisní okno -** servisním oknem se rozumí vymezený časový rámec mimo provozní dobu služby na údržbu systému.

Režim servisních oken

- Po 18:00 - 24:00 HW údržba
- Út 18:00 - 24:00 SW údržba
- St 18:00 - 24:00 HW údržba
- Čt 18:00 - 24:00 SW údržba

**Podpora Helpdesk** - standardní doba Helpdesku pro uživatele a řešitele -

Režim podpory Helpdesku

- Po – Čt 07:00 - 17:00
- Pá - 07:00 – 15:00

**Požadovaná dostupnost aplikace –** Dostupnost aplikace/služby koncovým uživatelům v procentech.

**Požadovaná doba odezvy -** časový interval mezi akcí uživatele a odezvou systému.

**Požadovaná spolehlivost** - střední doba mezi výpadky
Střední doba mezi obnovením služby po výpadku a vznikem nového výpadku dané služby. Uvádí se ve dnech.

## 6.4 Podmínky převzetí do rutinního prostředí a aplikační podpory

- Aplikace/služba je řádně otestovaná s příslušnou testovací dokumentací a akceptačními protokoly za jednotlivé druhy testů.
- Rutinní operace jsou plně automatizované (vyžadují pouze prvotní nastavení a následnou pravidelnou kontrolu), manuální operace jsou max. eliminovány (např. manuální kopírování dat v případě provozní chyby).
- Aplikace/služba je připravena k monitoringu všech funkcionalit, veškerého HW, SW a DB a je připravena k využití stávajících monitorovacích nástrojů.
- Aplikace/služba musí být předána dle standardního procesu předání aplikací do provozu včetně kompletní provozní dokumentace dle požadované struktury
- Aplikace/služba je dodána s kompletní dokumentací provozní i uživatelskou, včetně „Předávacích tabulek“ (přílohou standardů). K aplikaci/službě je dodán instalační postup a konfigurační příručka, podle kterých je možné jednoznačně aplikaci/službu instalovat a konfigurovat, bez jakýchkoliv manuálních zásahů.
- Po provedení instalace aplikace/služby dle dokumentace a instalačních postupů je stav aplikace/služby plně funkční, dle požadavků odběratele.
- Aplikace/služba je v době 1 měsíce od nasazení do produkčního prostředí v pilotním provozu, kdy se vyžaduje zvýšená podpora dodavatele
- Aplikaci/službu je po splnění a dodání výše uvedených bodů možné převzít do plného rutinního prostředí a následné aplikační podpory.

viz přílohy:

P5_předávací_Tabulky_produkčního prostředí

P5a_předávací_Tabulky_testovací_prostředí

## 6.5 Vazba na ITIL procesy

Vlastník kapitoly: OKP

Aplikace musí být zařazena ve VZP do standardních ITIL procesů.

### 6.5.1 Definování veškerých eskalačních procedur u aplikace - správa HelpDesku/ServiceDesku

- Kritičnost aplikace
- Obnovení provozu
- Rozpoznání nestandardní situace
- Eskalační procedura

### 6.5.2 Zavedení aplikace do incident managementu

Aplikace musí být zavedena do procesu Incident Managementu.

### 6.5.3 Zavedení aplikace pod standardní řízení změn - change management

Aplikace musí být zavedena do procesu Change Managementu, který má následující části:

- Požadavek a zadání změny
- Schvalovací proces změny

- Realizace změny a předání úpravy aplikačního softwarového vybavení (dále zkratkou ASW) podle pravidel release managementu (uvedeno v následující kapitole)
- Nasazení změny ASW a akceptace v rámci procesu test managementu
- Podle objemu a závažnosti zakázky je může být celý proces projektově řízen.

#### 6.5.4 Zavedení aplikace do release plánů - release management

Aplikace musí být zavedena do procesu Release Managementu.

Ve VZP používáme toto rozdělení release:

- malý - malé změny, bez dopadu do integrace
- velký - velké funkční změny
- mimořádný – mimo termín release plánu – např. legislativou vynucené změny…

Pro každou komponentu ASW se v rámci dohody mezi dodavatelem a ICT VZP ČR nastaví release plán.

# 7 Seznam příloh

Příloha 1: Vzor_Predavaci_tabulky_PP (produkční prostředí)
Příloha 2: Vzor_Predavaci_tabulky_TP (testovací prostředí)
Příloha 3: Integrace aplikace do IDM (Identity management)
Příloha 4: Integrace aplikace s CSČ (Centrální správa číselníků)
Příloha 5: Popis integračních vazeb prostřednictvím IPF a metodika realizace integračních vazeb

# 8 Výjimky ze standardu

## 8.1 Integrace se stávajícím IS

Příloha 3: Integrace aplikace do IDM (Identity management)
Příloha 4: Integrace aplikace s CSČ (Centrální správa číselníků)
Příloha 5: Popis integračních vazeb prostřednictvím IPF a metodika realizace integračních vazeb

# Stav IS VZP

**UPOZORNĚNÍ:**

Tento dokument je zpracován Všeobecnou zdravotní pojišťovnou České republiky (dále též jen „VZP ČR“ nebo „VZP“). Všeobecná zdravotní pojišťovna České republiky jej uveřejňuje v rámci zadávací dokumentace jí zadávaných veřejných zakázek. Tento dokument umožňuje utvořit si představu o standardech informační architektury ICT VZP ČR. Účelem jeho uveřejnění je poskytnout informace nezbytné pro integraci dodávané komponenty se stávajícím informačním systémem v souladu se Standardy ICT- VZP- NIS.

Uveřejněním tohoto dokumentu není dotčena právní odpovědnost spojená s jeho zneužitím.

V tomto dokumentu bylo použito názvů subjektů a názvů produktů, které mohou být chráněny příslušnými právními předpisy.

**Otevřením tohoto dokumentu berete výše uvedené skutečnosti na vědomí.**

# Verze dokumentu

| Verze | Datum | Autor | Popis |
|---|---|---|---|
| 0.9 | 11.3.2019 | Juraj Boldiš | Založení dokumentu ze Standardu verze 1.09 |
| 1.0 | 22.5.2019 | Roman Palkovič (OTP) | Připomínkování a zapracování úprav dokumentu |
| 1.0.1 | 14.6.2019 | Juraj Boldiš | Zapracovány připomínky M. Škopa |
| | | | |
| | | | |

# Obsah

1. ÚVOD ..... 6
2. APLIKAČNÍ KOMPONENTY ..... 7
2.1.1. Integrace se stávajícím IS ..... 7
3. INFRASTRUKTURA VZP ..... 8
3.1. HW ..... 8
3.1.1. On Premise Serverová infrastruktura ..... 8
3.1.2. Cloudová infrastruktura ..... 8
3.1.2.1. IAAS - využívané služby ..... 8
3.1.2.2. PAAS využívané služby ..... 8
3.2. Sítě ..... 9
3.2.1. Celkové schéma sítě VZP ČR ..... 9
3.2.2. LAN RP a KLIPRů ..... 10
3.2.3. Bezdrátová síť (WIFI) ..... 11
3.2.5. Datová centra On premise ..... 12
3.2.6. Perimetr ..... 13
3.2.7. Síťové služby ..... 14
3.2.8. Sjednocená komunikace ..... 14
3.3. OS ..... 14
3.3.1. OS pro aplikace třídy A ..... 14
3.3.2. OS pro aplikace třídy B ..... 14
3.3.3. Prostředí pro virtualizaci ..... 14
3.4. Middleware ..... 15
3.4.1. Integrační platforma ..... 15
3.4.2. Aplikační servery ..... 15
3.4.3. Webové servery ..... 15
3.5. Virtualizovaná infrastruktura pro hostování aplikací ..... 16
3.6. Deployment aplikací provozovaných on-Premise do prostředí v DC ..... 16
3.7. Datové a databázové služby ..... 17
3.6. Popis standardního koncového zařízení ..... 18
3.7. Elektronická pošta ..... 19
3.8. Active Directory ..... 20
3.9. PKI ..... 20
6. PROVOZNÍ PROSTŘEDÍ ..... 21
6.1. Monitoring ..... 21
6.1.1. Rozsah monitoringu ..... 21
6.1.2. Používané dohledové nástroje pro On premise řešení ..... 21

**6.2. Zálohování a archivace ..... 22**

**6.2.1. Zálohovací systém ..... 22**

**6.2.2. Zálohovací architektura ..... 22**

# Seznam obrázků

Obrázek 1 - Celkové schéma sítě VZP ČR ..... 10
Obrázek 2 - Schéma propojení datových center ..... 12
Obrázek 3 – Schéma deploymentu datových center ..... 17
Obrázek 4 - Schéma zálohovacího sytému VZP ČR ..... 22

## 1. Úvod

# STAV IS VZP

- **Shrnuje aktuální stav aplikačních komponent –** poskytuje přehled o aplikačních komponentách, které jsou možné využít pro, rozvoj a budování IS VZP ČR.

- **Popisuje aktuální stav infrastruktury –** dává přehled o infrastruktuře, kterou v současnosti VZP využívá

# 2. Aplikační komponenty

### 2.1.1. Integrace se stávajícím IS

Ke dni vzniku tohoto dokumentu VZP provozuje stávající IS řízený historickou verzí standardu. Způsob integrace s tímto IS je proto prováděn dle původního standardu, stav je popsán v následujících přílohách.

Příloha 3: Integrace aplikace do IDM (Identity management)
Příloha 4: Integrace aplikace s CSČ (Centrální správa číselníků)
Příloha 5: Popis integračních vazeb prostřednictvím IPF a metodika realizace integračních vazeb

# 3. Infrastruktura VZP

## 3.1. HW

### 3.1.1. On Premise Serverová infrastruktura

Základem serverové infrastruktury, centralizované a provozované v rámci datových center (DC), jsou servery nebo serverovými systémy založené na architektuře procesoru Intel Itanium a x86. Servery jsou certifikovány na operační systémy uvedené v kapitole 3. 3., jsou rozšířitelné, maximálně flexibilní a vysoce dostupné. Jednotlivé servery nebo serverové systémy jsou připojeny do sítě LAN a v případě komunikace s diskovými poli i do sítě SAN a vybaveny kvalitními nástroji pro správu. V případě používání virtualizace uvedené v kapitole 3. 3. je hardware management propojen s virtualizační vrstvou. Servery nebo serverové systémy jsou v provedení blade nebo rackmount a v datových centrech jsou umístěny v rackových skříních velikosti 42U. Napájení rackových skříní se odvíjí od spotřeby zařízení, která jsou v něm umístěna.

Standardem pro připojení fyzických serverů do sítě LAN v datových centrech je:

- Management konzole, 1x1GE, access
- Management interface, 2x1GE, acces, active-standby
- Datový interface, 2x10GE, trunk, active LACP

**On Premise SAN infastruktura**

V jednotlivých datových centrech jsou disková enterprise a midrange pole, která jsou zapojena do SAN infrastruktury pomocí SAN přepínačů. Potřebná kapacita diskových polí je řešena rozšířením těchto polí nikoliv nákupem dalších polí. Do této SAN infrastruktury jsou z důvodu vysoké propustnosti a kvalitního zabezpečení (využití alternativních cest) zapojeny všechny významné servery, zálohovací knihovny a zmíněná disková pole. Tato SAN síť využívá u všech významných komponent minimálně 2 FC rozhraní pro zajištění vysoké dostupnosti.

### 3.1.2. Cloudová infrastruktura

Je využíván jeden cloudový poskytovatel - Microsoft a tedy spravujeme a využíváme jedno cloudové prostředí - Azure. Do listopadu 2019 můžeme využívat pouze služby, které jsou definovány smlouvou, není tedy možné využít jakoukoliv službu, následně bude možné využívat vše. Níže jsou vyjmenovány služby, které využíváme pro provoz e-VZP aplikací a veřejného webu.

#### 3.1.2.1. IAAS - využívané služby

Azure Virtual machine

Azure Virtual machine scale set

#### 3.1.2.2. PAAS využívané služby

Azure Storage – blob, queue, table, files

Azure SQL database

Azure Appservice

Azure CDN

Redis Cache

Service Bus

Key Vault

Notification HUB

Log Analytics

Service Fabric

Sendgrid

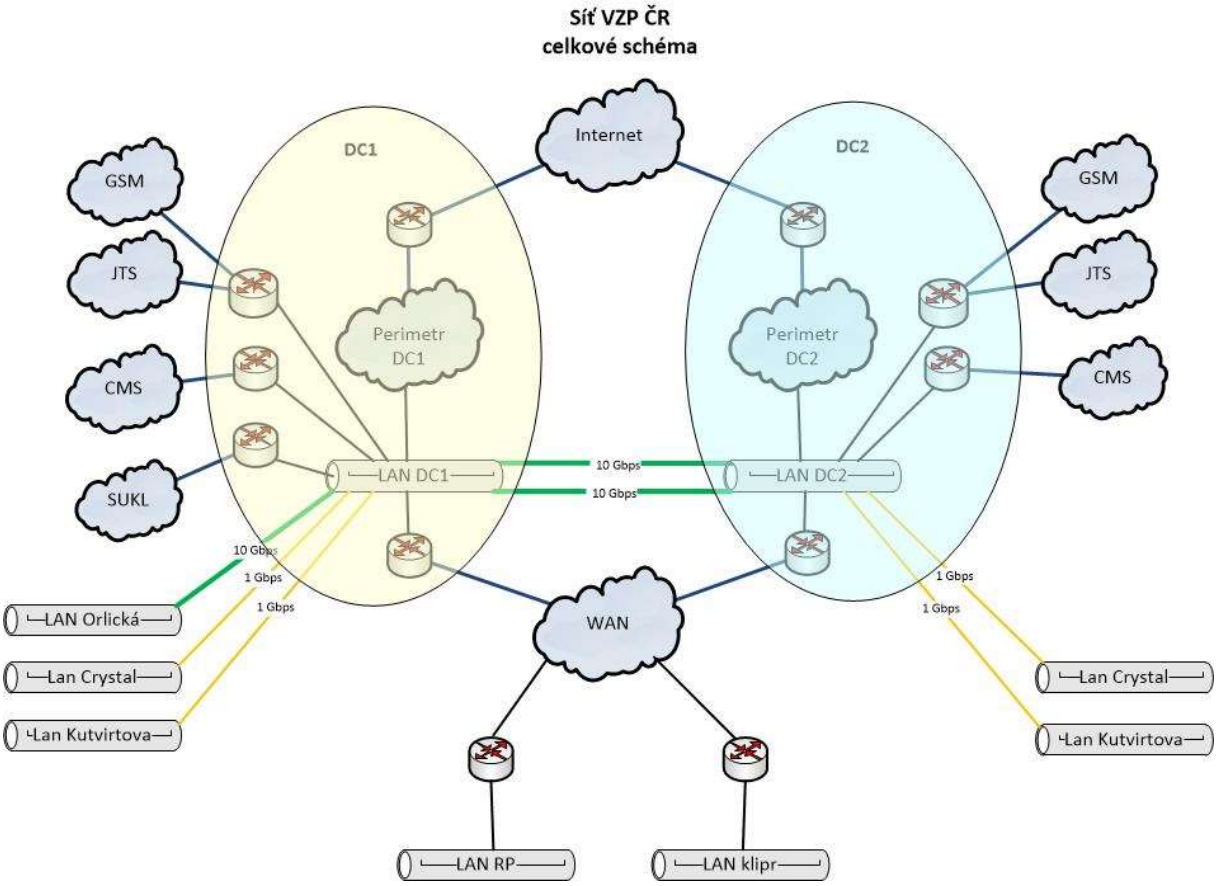
## 3.2. Sítě

### 3.2.1. Celkové schéma sítě VZP ČR

Z hlediska vztahu k uživatelům a k okolnímu světu je možné počítačovou síť VZP ČR rozdělit do několika funkčních celků:

- **Perimetr**
- **Datová centra**
- **WAN síť**
- **LAN sítě ústředí, regionálních poboček a kliprů(klientských pracovišť)**

Schematicky je síť VZP ČR znázorněna na následujícím obrázku:




*Obrázek 1 - Celkové schéma sítě VZP ČR*

| | |
|---|---|
| **CMS** | Centrální místo služeb |
| **GSM** | Globální Systém pro Mobilní komunikaci |
| **JTS** | Jednotná telefonní síť |
| **SUKL** | Státní úřad pro kontrolu léčiv |
| **RP** | Regionální pobočka |
| **KLIPR** | Klientské pracoviště |
| **DC1** | Datové centrum 1 na adrese Orlická 4/2020, 130 00 Praha 3 |
| **DC2** | Datové centrum 2 na adrese ČD Telematika, Pod Táborem 369/8a, 190 00 Praha 9 |
| **LAN Orlická** | Ústředí na adrese Orlická 4/2020, 130 00 Praha 3 |
| **LAN Crystal** | budova Crystal na adrese, Vinohradská 2577/178, 130 00 Praha 3 |
| **LAN Kutvirtova** | Call Centrum a klipr na adrese Kutvirtova 339/5, 150 00 Praha 5 |

### 3.2.2. LAN RP a KLIPRů

LAN ve VZP ČR je rozdělena do vrstev podle hierarchického modelu:

- **Access (přístupová) vrstva** – zajišťující konektivitu koncových uživatelů
- **Distribution (distribuční) vrstva** – zajišťující vysokou dostupnost
- **Edge (hraniční) vrstva** – slouží pro připojení LAN do WAN

**SLUŽBY A TECHNOLOGIE LAN**

- VLAN
- QoS

**VLAN**

VLANy jsou implementované v přístupové vrstvě. Uživatelé z různých oddělení, rozděleni do určených VLAN, mohou přistupovat do sítě určenými přístupovými přepínači, které jsou umístěny v různých podsítích. V hraniční, případně distribuční, vrstvě je nakonfigurované směrování těchto podsítí mezi sebou a také případné omezení provozu mezi VLANami pomoci ACL – Access Control List (přístupových listů).

**QoS (QUALITY OF SERVICE)**

QoS zajišťuje rovnoměrné vyvažování zátěže sítě s ohledem na druh přenášených dat, spravedlivě rozděluje konektivitu mezi jednotlivé aplikace dle nastavených priorit a zabraňuje přetížení sítě.

Ve VZP ČR jsou použity následující **QoS** třídy, které jsou řazeny dle priority – od nejvyšší priority po nejnižší prioritu.

- Třída – Network support
- Třída – Real time (VoIP RTP, VoIP Signalizace)
- Třída – 3B: Interaktivní provoz (terminálová třída) – (Aplikace Interaktivní)
- Třída – 3A: Web provoz (webová třída)
- Třída – 3D: Scavenger třída (DoS, P2P, ...) – Služby UDP (Bulk)
- Třída – Zbytková třída – ostatní provoz

### 3.2.3. Bezdrátová síť (WIFI)

Bezdrátová síť ve VZP ČR je provozována na standardních zařízeních a technologii firmy Cisco. Bezdrátová síť poskytuje několik variant připojení:

- **WLAN_DATA** – síť určená pro standardní uživatele interní sítě VZP, je veřejně inzerovaná. Tato síť je určená pro běžného uživatele a jsou na ni implementována bezpečnostní omezení.
- **WLAN_ADMIN** – síť určená pouze pro administrátory sítě. Síť není veřejně inzerovaná (má vypnuto vysílání SSID).
- **WLAN_PHONE** – síť určená pro připojení mobilních telefonů a pro volání po bezdrátové síti. Síť není veřejně inzerovaná (má vypnuto vysílání SSID). Přístup do sítě je ověřen pomocí MAC adresy zařízení.
- **WLAN_GUEST** – síť určená pro připojení externích uživatelů s přístupem pouze do Internetu pomocí protokolu HTTP (S). Tato síť je veřejně inzerovaná.
- **WiredGuest** – jedná se o drátovou síť, která je řízená prostředky bezdrátové sítě a funguje obdobně jako síť WLAN_GUEST s tím rozdílem, že klient se místo k bezdrátové síti připojuje do portu přepínače.
  Tuto síť je možno využívat pouze v centrálních lokalitách – Orlická, Perštýn.
  Tato síť určená pro připojení externích uživatelů s přístupem pouze na Internet.

### 3.2.4. WAN

VZP ČR provozuje privátní datovou síť WAN na přenosových prostředcích poskytovatele datového připojení pomocí technologie MPLS. Pro zajištění bezpečnosti přenášených dat je použito šifrování na

síťové vrstvě mezi koncovými zařízeními pomocí protokolu IPSec. Pro navazování šifrované komunikace mezi směrovači v síti VZP ČR je použita technologie GET (Group Encrypted Transport) VPN.

**Šířka pásma**

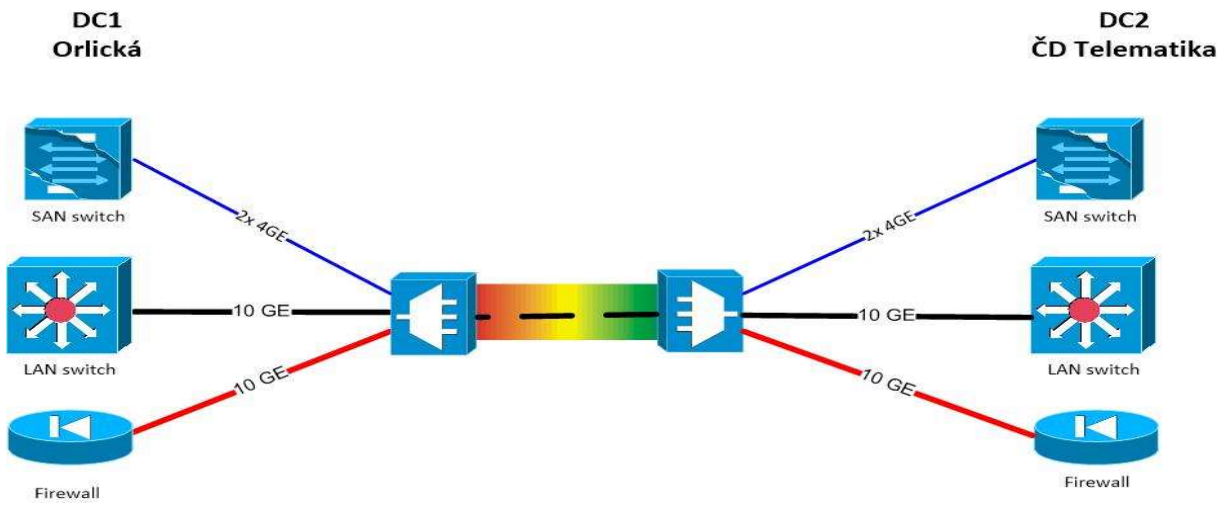
| Typ pobočky | Počet uživatelů | Šířka pásma |
|---|---|---|
| 1 | 1-5 | 0,5 Mbps |
| 2 | 6 -50 | 4 Mbps |
| 3 | 51 a více | 8 Mbps |

### 3.2.5. Datová centra On premise

VZP ČR provozuje dvě geograficky oddělená datová centra:

- DC1 na adrese Orlická 4/2020, 130 00 Praha 3
- DC2 na adrese ČD Telematika a.s., Pod Táborem 369/8a, 190 00 Praha 9

Obě datová centra jsou propojena dvěma nezávislými optickými trasami technologií DWDM. Jedna vlnová délka o kapacitě 10 Gbps je použita pro LAN provoz a druhá 10 Gbps pro propojení firewall clusteru. Pro propojení SAN přepínačů jsou multiplexovány dva kanály, každý o kapacitě 4 Gbps.




*Obrázek 2 - Schéma propojení datových center*

Každé z datových center VZP ČR je vytvořeno na technologii firmy Cisco Nexus dle architektury Spine and Leave a patří mezi tzv. aplikačně řízené infrastruktury (Application Centric Infrastructure ACI), které umožňují integrovat do řízení síťového provozu datového centra vlastní logiku jednotlivých aplikací z pohledu jejich požadavků na síťovou konektivitu, bezpečnost a L4-L7 služby (load balancing, firewalling atd.). Fyzické nebo virtuální aplikační servery sdílející stejnou bezpečnostní a síťovou politiku jsou konsolidovány do logických skupin a současně je definována jejich vzájemná komunikace (která aplikační komunikace je povolená, jaké vyžaduje QoS parametry a jaké vyžaduje L4-L7 služby).

Veškeré aplikační politiky jsou definovány na centrálním kontroleru (Application Policy Infrastructure Controller - APIC), který je s využitím otevřených aplikačních rozhraní automaticky distribuuje na jednotlivé komunikační prvky a systémy, které následně podle těchto aplikačních politik řídí síťový provoz.

**Logická infrastruktura**

Provoz datového centra je z pohledu toku dat směrem od uživatele k vlastním datům rozdělen do jednotlivých funkčních modulů neboli zón. Rozhodujícím hlediskem pro sledování toku dat je „kdo inicializuje komunikaci“.

Zóny představují zpravidla několik L3/L2 segmentů, která mají podobná bezpečnostní pravidla. Zóny jsou IP adresací příslušné k lokalitě DC. Výjimku tvoří zóna DC-DB, ta je L2 geograficky rozprostřena mezi lokalitami DC1 a DC2.

**Rozdělení DC zón:**

- **Síť VZP ČR (VZP NET)**

Zóna označuje síť VZP, která není součástí DC – tj. infrastrukturní část LAN/WAN včetně části koncových uživatelů.

- **Demilitarizovaná zóna (DC-DMZ )**

Zóna je dostupná z obou stran jak pro VZP, tak pro DC. Slouží k zabezpečení a poskytování služeb. Typicky Management, DNS, MS AD DC nebo LDAP, ACS. Do této zóny patří vrstva správy a administrace a vrstva infrastrukturních serverů.

- **Prezentační vrstva (DC-VIP)**

Jedná se o vrstvu, v které jsou umístěné servery zajišťující komunikaci s uživateli. Patří sem i virtuální IP adresy, které reprezentují jednotlivé aplikace pro přístup jak z VZP NET, tak z ostatních aplikací DC.

- **Aplikační vrstva (DC-APP )**

Zde jsou umístěny aplikační servery zajišťující business logiku jednotlivých aplikací.

- **Databázová vrstva DC (DC-DB)**

Umístění DB serverů. L2 vrstva rozprostřená geograficky mezi lokalitami DC1 a DC2. V databázové vrstvě je možné vytvářet clustery se společnou IP adresou mezi jednotlivými lokalitami.

- **Servisní zóna (DC-SERVIS)**

Zóna slouží jako prostředník pro výměnu dat mezi ostatními zónami a mezi prostředími produkce a test.

Zóny DC-APP a DC-DB nejsou přímo dostupné z VZP NET a obráceně. Komunikace musí být zprostřed-kována přes některou ze zón DC-DMZ, DC-VIP, DC-SERVIS .

**Komunikační matice zobrazuje podporované komunikace mezi jednotlivými zónami.**

| | Komunikace do zóny → | | | | | |
|---|---|---|---|---|---|---|
| Komunikace ze zóny ↓ | VZP NET | DC-DMZ | DC-VIP | DC-APP | DC-DB | DC-SERVIS |
| VZP NET | ANO | ANO | ANO | ⊖ | ⊖ | ANO |
| DC-DMZ | ANO | ANO | ANO | ANO | ANO | ANO |
| DC-VIP | ⊖ | ⊖ | ⊖ | ANO | ⊖ | ⊖ |
| DC-APP | ⊖ | ANO | ANO | ⊖ | ANO | ANO |
| DC-DB | ⊖ | ANO | ⊖ | možné | možné | ANO |
| DC-SERVIS | ANO | ANO | ⊖ | ANO | ANO | ANO |

### 3.2.6. Perimetr

Perimetr je zabezpečená oblast podnikové sítě, která leží mezi internetem a vnitřní sítí VZP ČR. Perimetr je rozdělen pomocí bezpečnostních bran (firewallů) do několika oddělených bezpečnostních zón:

- vnější perimetr – bezpečnostní oddělení externích sítí (Internetu) od sítě VZP
- vnitřní perimetr – bezpečnostní oddělení veřejně vystavených služeb VZP od vnitřní (uživatelské) sítě VZP

Součástí řešení je i VPN přístup do VZP ČR. VPN slouží pro vzdálený přístup zaměstnanců a externích kontraktorů do sítě VZP ČR z Internetu.

### 3.2.7. Síťové služby

Síť VZP ČR poskytuje pro koncová zařízení, aplikace a uživatele následující služby:

- Časová synchronizace (NTP)
- Kvalita služby (QoS)
- DNS, DHCP, IPAM (DDI)
- Loadbalancing

### 3.2.8. Sjednocená komunikace

Sjednocená komunikace je ve VZP ČR tvořena následujícími součástmi:

- **Hlasová komunikace**
  - IP Telefonie
  - Integrované nadstavbové funkcionality
  - Spolupracující systémy
    - Call Centrum Atlantis
    - Cisco Paging
- **Elektronická komunikace**
  - Instant messaging - Cisco Jabber
  - Webová konference – Cisco WebEx

## 3.3. OS

### 3.3.1. OS pro aplikace třídy A

- HP-UX 11.31, Red Hat Enterpise Linux, Oracle Linux, CentOS (verze 6.x a 7.x)
- MS Windows Server 2012R2 EN a novější

### 3.3.2. OS pro aplikace třídy B

HP-UX 11.31, Red Hat Enterprise Linux, Oracle Linux, CentOS (verze 6.x a 7.x)

MS Windows Server 2012R2 EN a novější

### 3.3.3. Prostředí pro virtualizaci

Hostitelský systém je hypervizor nebo operační systém s hypervizorem , který umožní provoz Virtuálních serverů. Podporované platformy jsou a ve VZP mohou být nasazeny technologie, VMWare vSphere 5.5 Enterprise a vyšší, HPVM, Oracle VM 3.4 a vyšší a MS Hyper-V 2012R2 a vyšší.

Řízení Virtuálních serverů - správa VMs na VMWare nástrojem VMWare vCenter Server 5.5 Standard a vyšší. Správa VMs na Hyper-V je realizována nástrojem SCVMM 2012R2 a vyšší.

Pro zajištění vysoké dostupnosti aplikací třídy A pro a realizaci DRP plánu slouží technologie VMware DRS a HA cluster, případně VMware SRM, VMware vSAN nebo MS Hyper-V Clustering, MS Storage Spaces Direct v aktuálních verzích.

Pro aplikace třídy A využívající softwarové produkty Oracle bude použita virtualizace Oracle VM.

U aplikací třídy B lze použít i další virtualizační technologií:

KVM (Kernel-based Virtual Machine)

## 3.4. Middleware

### 3.4.1. Integrační platforma

- je založená na koncepci ESB (Enterprise Service Bus) jako podnikové sběrnice služeb
- pro realizaci integrace aplikací a služeb
- využívá centrální business rule repozitory a Business rule engine
- využívá principy servisně orientované architektury (SOA)
- využívá MOM architekturu (Message Oriented Middleware) jako podmnožinu ESB kde prostřednictvím Message brokera zajišťuje spolehlivé doručení zprávy nesoucí informaci (Message) mezi jednotlivými systémy (prostřednictvím front).
- využívá model řízení událostmi

**Integrační platforma poskytuje tyto typy služeb:**

- centrální řízení komunikaci mezi systémy realizované prostřednictvím ESB služeb,
- kompozice vlastních služeb a jejich publikace konzumentům
- zprostředkování a publikace sdílených služeb konzumentům,
- orchestraci služeb vnitřních i vnějších s ostatními integračními technologiemi (BPEL)
- směrování a předávání dat mezi jednotlivými službami
- transformaci formátů dat,
- konverze protokolů mezi jednotlivými službami,
- centrální business rule repozitory
- centrální repozitory služeb

### 3.4.2. Aplikační servery

Výčet typů AS využívaných v IS VZP:

| Druh AS | Použití |
|---|---|
| Oracle Fusion Middleware WebLogic Server v nejnovější podporované verzi | Aplikace deployované v J2EE, vhodné pro aplikace třídy A |
| JBoss aplikační server v nejnovější podporované verzi | Pro J2EE aplikace třídy B nebo v odůvodněných případech, kde není vhodné použití Oracle Weblogic J2EE. |

### 3.4.3. Webové servery

Výčet typů WS využívaných v IS VZP:

- Oracle Web Tier v nejnovější podporované verzi

- Apache v nejnovější podporované verzi
- IIS

### 3.5. Virtualizovaná infrastruktura pro hostování aplikací

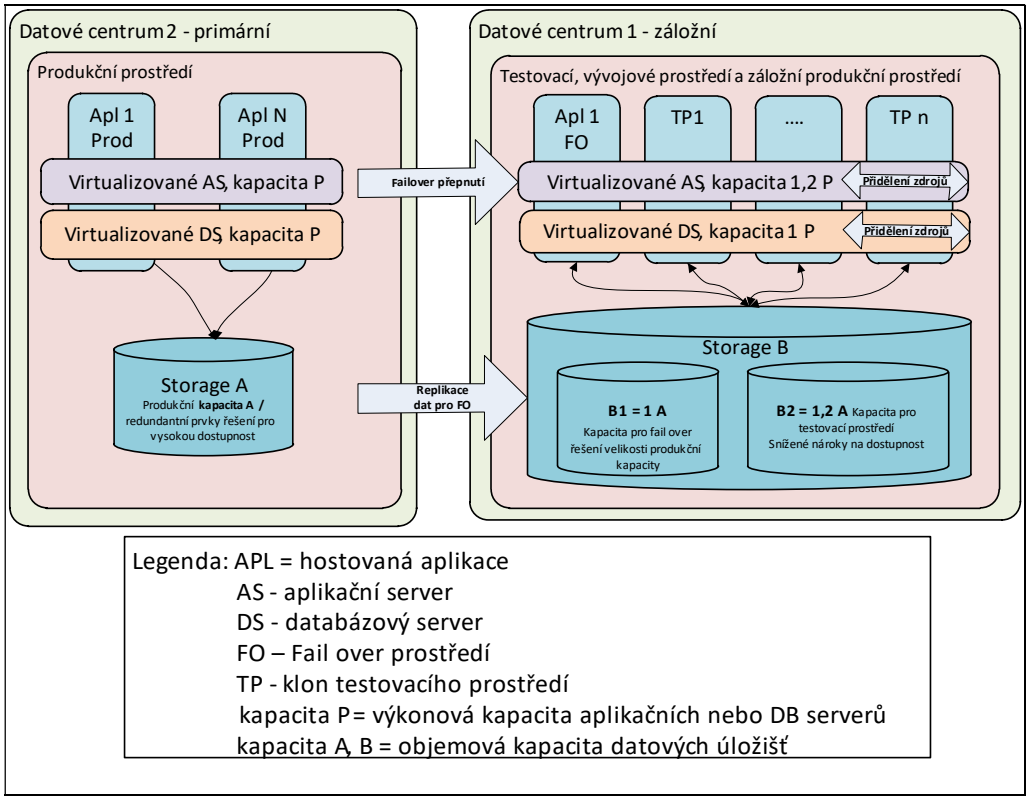
Aplikační služby jsou hostovány na virtuálních prostředí / serverech následujících parametrů:

| Název služby | Popis |
|---|---|
| Server s OS | OS Windows nebo Linux (viz kap. 3.3 OS) |
| Aplikační server | OS Windows nebo Linux aplik. serveru Oracle Weblogic Suite |
| Databázový server Oracle | OS Linux, Oracle dB EE + RAC + partitioning |
| Databázový server MS SQL | OS MS Windows, MS SQL Server v edici Enterprise |

### 3.6. Deployment aplikací provozovaných on-Premise do prostředí v DC

Pro zabezpečení provozu aplikací v prostředí datových center je používán standardizovaný deployment aplikací :

- Produkční instance aplikací a jejich odpovídajících dat je hostována v primárním datovém centru na zařízeních s vysokou dostupností a redundancí na virtualizované infrastruktuře.
- Záložní instance aplikací je hostována ve virtualizované infrastruktuře v záložním datovém centru s dedikovanou kapacitou úložiště o velkosti produkčních dat pro fail over primárního DC.
- Virtualizovaná infrastruktura serverů záložního centra je dimenzována jako výkonový ekvivalent zařízení v primárním datovém centru. Požadavek na dostupnost je nižší, tomu odpovídá nižší redundance prvků.
- Virtualizovaná infrastruktura záložního centra je sdílena s testovacími prostředími.
- Produkční data z primárního DC jsou asynchronně replikována do záložního DC.
- Pro účely testování je v záložním DC dedikována obecně kapacita virtualizované úložné kapacity až v rozsahu 1,2 velikosti produkčních dat sdílená pro všechny instance testovacích prostředí. Tato kapacita je alokována individuálně při návrhu systému.
- Kapacita úložiště Storage B musí být 2,2 násobkem kapacity úložiště produkčního prostředí Storage A
- Kapacita HW serverů pro databázovou a aplikační vrstvu musí být výkonově dimenzována jako 1,2 násobek produkčního prostředí (měřeno součtovým počtem jader, velikostí operační paměti virtuálních serverů a diskových úložišť pro aplikační a databázovou vrstvu). Redundance komponent není nutná.




*Obrázek 3 – Schéma deploymentu datových center*

### 3.7. Datové a databázové služby

#### 3.5.1. Databázové technologie

| Standard | Popis |
|---|---|
| Oracle DB EE v nejnovější podporované verzi, včetně databázových options | Pro aplikace třídy A nebo B. |
| MS SQL EN v nejnovější podporované verzi,X64bit | Podpůrné služby a pro aplikace v třídě B. V odůvodněných případech je možné použít i pro aplikace třídy A. |

#### 3.5.2. Datové a databázové standardy

| Oblast standardizace | Popis |
|---|---|
| Minimum redundancí | Data jsou uložena v jediné databázi. Redundantní databáze v rámci lokality nejsou pro core business aplikace povoleny. Replikace se provádí pouze z důvodu realizace DR plánu.. |
| Jediný zdroj informací | Data jsou uložena v místě jejich vzniku, do ostatních systémů jsou poskytována prostřednictvím integrační platformy. Platí pravidlo minima duplicit. |
| Datová konzistence | Datová konzistence je zachovávána již v rámci databáze, tedy nikoliv pouze aplikačně. |
| Modelování DB pomocí ER diagramu | Jsou zachovány normálové formy. Pouze v případech, kdy je to nutné jsou možné výjimky – v dokumentaci však je explicitně uvedeno. |

| | |
|---|---|
| Návrh datového modelu | Návrh datového modelu DB musí být akceptován datovým architektem VZP ČR.<br>Persistentní objekty vývojář definuje bez určení:<br>• Názvu tablespace<br>• fyzických atributů segmentu (pctused, pctfree, storage params,...)<br>Databázové objekty jsou považovány za privátní součást aplikace, tzn. aplikace může přistupovat k databázovým objektům jiné aplikace pouze prostřednictvím dedikovaných služeb. |
| Jmenné konvence databázových objektů | Všechna jména základních databázových objektů (tabulky, pohledy, balíky funkcí a procedur, fronty, sekvence, indexy, triggery apod.) začínají dvouznakovým prefixem dodavatele |
| Kódování | Preferované UTF16, UTF8,<br>Definici collation – preferována Czech CI AS (case insensitive a accent sensitive)<br>Na výjimku: ISO 8859-2, Windows 1250 |
| Podpora anonymizace / pseudonymizace osobních údajů | Datová vrstva musí podporovat možnost anonymizace a pseudonymizace osobních údajů bez nežádoucí vlivu na chování datového engine a aplikace.<br>Využívá se pro účely příslušné legislativy a vytváření datového derivátu pro testování z produkčních dat.<br>Součástí dodávek je nástroj pro vytváření anonymizovaných derivátů produkčních dat (scrambling tool).<br>Toto musí být zohledněno i v dokumentaci. |
| Podpora řezů dat | Datový model musí být navržen tak, aby pro účely testování bylo možno oddělit testovací derivát – vzorek dat z produkčních dat.<br>Součástí dodávek je nástroj pro vytváření takových derivátů.<br>Toto musí být zohledněno i v dokumentaci. |
| Zakázané vazby | Data v relačních databázích nesmí být provazována technologicky přes významové klíče, povolena je relační vazba pouze přes nezávislé technologické klíče záznamů.<br>Nejsou dovoleny přímé datové vazby mezi datovými doménami. |

### 3.6. Popis standardního koncového zařízení

- Koncová pracovní zařízení počítače a notebooky
  - Instalován OS Windows enterprise 7 x32 /Windows 10 enterprise x64
  - Nastavení OS systému a uživatelského prostředí řízeno centrálně doménovou politikou.
  - Uživatel nemá na koncové zařízení administrátorské práva
  - Vzdálený přístup je zajištěn Remote Desktop, Support Assistant
  - Bezpečnostní aktualizace OS v 6 měsíčním cyklu

- Programové vybavení koncových pracovních zařízení
  - MS Office 2010/2016 /2019 Profesionál plus
  - Google Chrome, nastavení řízené centrální doménovou politikou

- IE aktuální verze 11, nastavení řízené centrální doménovou politikou
- 7ZIP
- Cisco AnyConnect Secure Mobility Client (Notebooky)
- Adobe Reader 11/DC

- Centrální distribuce programového vybavení na pracovní stanice
  - Distribuce SW je použitím SCCM

- Zabezpečení koncových pracovních zařízení
  - Endpoint Protection , Antivirová ochrana Kaspersky Endpoint Securit (centrálně řízený)
    - AntiMalware, IDS/IPS,
    - Firewall,
    - Application control,
    - Device control,
    - Antispam

- Jednotná adresářová struktura
    - Root:
      APPL
      Archiv
      Data
      Nezalohovano
      Program Files
      Temp
      TMP
      Users
      Windows
  - Pro Root, Program Files, Windows má běžný uživatel práva pouze pro čtení

- Ostatní programové vybavení
  - JAVA 1.6.045 ,1.7.51 , 1.8. a vyšší
  - NET Framework ver. 4.0 a vyšší

- Tisková koncová zařízení
  - Tisková a multifunkční zařízení připojená přes tiskový server, výjimečně lokální připojení
  - Follow me printing se zabezpečeným tiskem.
  - Ověřování pomocí bezkontaktních karet
  - (embeded čtečka v MFDnebo externí terminál, možnost ověření PINem).
  - Scan to me (možnost naskenovat z jakékoli MFD a obdržet sken v personální složce nebo emailem).

- Ostatní koncová zřízení
  - Mobilní telefony s OS : Android 5.0 a vyšší, Windows 10 mobile

### 3.7. Elektronická pošta

- Elektronická pošta ve VZP ČR je realizována prostřednictvím Microsoft Exchange server 2016. enterprise. Příjem elektronické pošty z Internetu zajišťují dedikované SMTP brány v perimetru, před předáním zpráv do interního poštovního systému je provedena jejich antivirová a antispamová kontrola. Odesílání pošty mimo lokální poštovní doménu probíhá pomocí SMTP protokolu s využitím poštovních bran.

- Klientský přístup k poštovnímu systému je zajištěn pomocí MS Outlook verze 2010 nebo vyšší, případně prostřednictvím internetového prohlížeče (Outlook Web App). Poštovní systém podporuje kromě SMTP i protokoly POP3 a IMAP.

Poštovní systém je využíván pro strategické řízení firmy, a proto je implementován jako vysoce dostupný.

### 3.8. Active Directory

VZP ČR využívá pro ověřování uživatelů a pracovních stanic Microsoft Active Directory (dále AD). Služby AD jsou realizovány na serverech s MS Windows Server 2012 R2. V AD má každý uživatel i každá pracovní stanice svůj účet. Účty uživatelů jsou spravovány prostřednictvím Identity Managementu na základě údajů uložených v personálním systému. AD zajišťuje pomocí skupinových politik i nastavení pracovních stanic v souladu s platnými bezpečnostními standardy.

### 3.9. PKI

VZP ČR využívá systém interních certifikačních autorit (PKI) založený na Microsoft Windows Server 2016. Vystavované certifikáty slouží pro identifikaci pracovních stanic a serverů v interní síti VZP ČR a dále pro podpis a šifrování elektronické pošty a pro vzdálený VPN přístup uživatelů do VZP ČR.

# 6. Provozní prostředí

## 6.1. Monitoring

### 6.1.1. Rozsah monitoringu

Služba dohledu provozu informačního systému je centralizovaná a je zajišťována dohledovým centrem s dvousměnným provozem v pracovních dnech od 6:00 do 22:00 hod. (v režimu 5x16). V těchto časových úsecích jsou drženy pohotovosti řešitelských skupin pro síťovou infrastrukturu, operační systémy Unix, operační systémy Windows, Oracle infrastrukturu (databáze a middleware), provoz aplikací, Exchange, a pro dohledové nástroje.

Z hlediska teorie spolehlivosti IT systémů a služeb jsou sledovány a vyhodnocovány:

- chybovost, resp. dostupnost systémů a služeb (Availability) a jejich vytížení (Utilization),
- výkonnost služeb (Performance).

Z technicko-provozního hlediska je monitoring provozován ve dvou hlavních úrovních – infrastrukturní a aplikační.

- Infrastrukturní monitoring pokrývá všechny prvky produkční IT infrastruktury ZIS od síťových prvků přes servery, databáze až po middleware. Je vyhodnocována dostupnost, resp. chybovost, jakož i vytíženost sledovaných prvků.
- Aplikační monitoring je zaměřen na sledování klíčových služeb produkčních aplikací. Probíhá aktivně pravidelným spouštěním aplikačních úloh, simulujícím uživatelské akce. Zároveň jsou pasivně vyhodnocovány vybrané úlohy reálných uživatelů. Je vyhodnocována dostupnost úloh a služeb, a současně jsou zaznamenávány a vyhodnocovány odezvy takto měřených transakcí, tedy výkonost aplikací. Výstupy pasivního monitoringu jsou využitelné pro sledování vytíženosti sledovaných oblastí.

### 6.1.2. Používané dohledové nástroje pro On premise řešení

Centrální systém dohledu provozu informačního systému je vybudován na platformě **HP Operations Manager** (HP OM). Do dohledového centra HP OM (centrální konzole) jsou soustřeďovány všechny důležité zprávy z ostatních monitorovacích nástrojů.

**HP OM** – agent na úrovni OS, centrální konzole
**HP OM Performance Manager (PM)** – sledování vytíženosti systémů
**Oracle Enterprise Manager Cloud Control (OEM)** – agent, integrace vybraných událostí do HP OM
**Microsoft System Center 2012 Operations Manager (SCOM)** – agent na úrovni OS, integrace vybraných událostí do HP OM
**Nagios** – bezagentní, s integrací vybraných zpráv do HP OM
**HP Business Service Management (HP BSM)** – integrace do HP OM
- **Business Process Monitor (BPM)** – aktivní aplikační monitoring

**HP Network Node Manager i (HP NNMi)** – aktivní SNMP poll, pasivní SNMP trap, je integrován s HP OM
**HP SiteScope** – bezagentní, integrace do HP OM a HP BSM

Není-li možné nasadit monitoring pomocí zavedených nástrojů, poskytne dodavatel v rámci dodávky aplikace monitorovací nástroj (například skript), jehož výstup lze integrovat do HP OM.

## 6.2. Zálohování a archivace

Všechna DC jsou zálohována jedním společným zálohovacím subsystémem (dále jen ZS).

### 6.2.1. Zálohovací systém

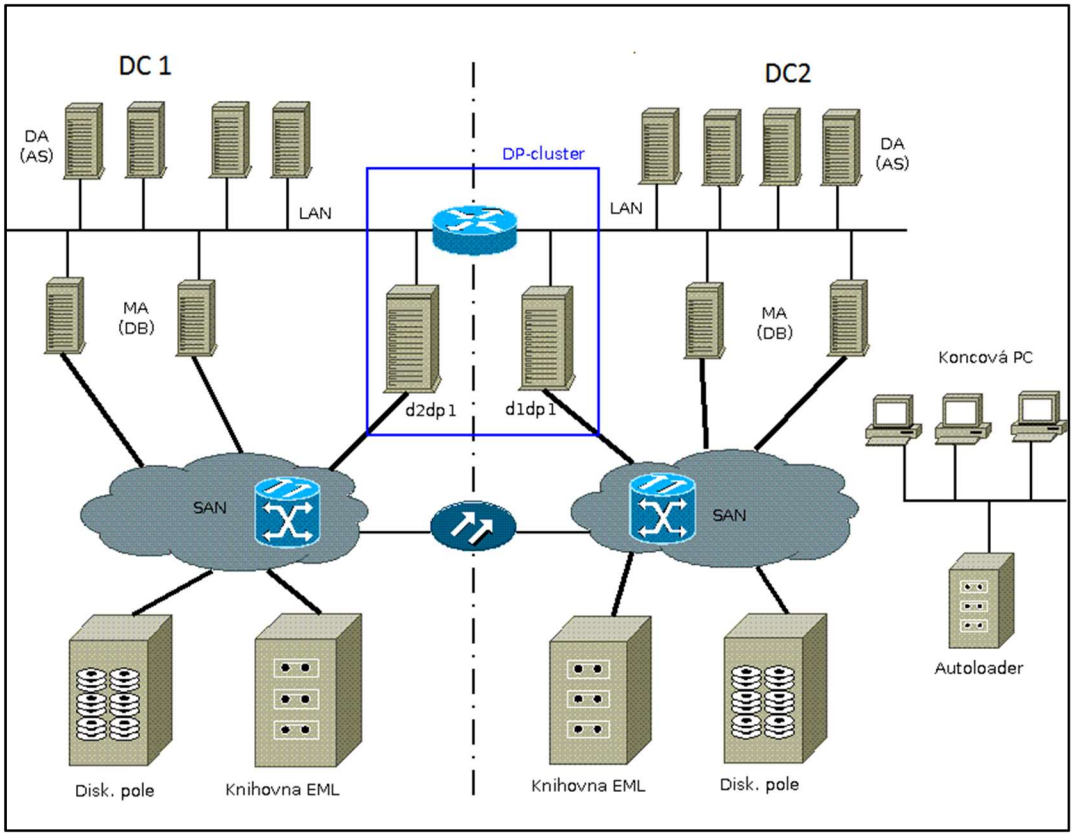
ZS je tvořen těmito komponentami:

- Řídící SW „Data Protector“.
- Cluster dvou serverů v oddělených lokalitách, na nichž je řídící SW provozován.
- HW pro ukládání zálohovaných dat, umístěný rovněž ve dvou různých lokalitách (DC), dostupný pomocí LAN a SAN infrastruktury. Jsou používány robotické páskové knihovny, které mohou být v případě potřeby doplněny o jiný HW (např. typu B2D), připojitelný pod řídící zálohovací software

Zálohování probíhá tak, aby byla respektována bezpečnostní zásada „3-2-1“ (tj. „důležitá data musí existovat 3x, ve 2 různých datových formátech, 1 kopie ve druhé lokalitě“) dle příslušné třídy aplikace.

### 6.2.2. Zálohovací architektura

Pro zálohování IS má VZP ČR k dispozici vysoce dostupný zálohovací systém s řídícím SW Micro Focus Data Protector. V každém datovém centru je k dispozici jedna pásková knihovna. Obě páskové knihovny jsou osazeny 8 kusy páskových mechanik (4x LTO4 + 4x LTO5, v budoucnu předpokládáme LTO7 a LTO8 a využití technologie B2D).




*Obrázek 4 - Schéma zálohovacího sytému VZP ČR*

# Integrace aplikace do IDM

## Příloha standardů a podmínek dodávek informačního systému VZP ČR

## UPOZORNĚNÍ:

Tento dokument je zpracován Všeobecnou zdravotní pojišťovnou České republiky (dále též jen „VZP ČR“ nebo „VZP“). Všeobecná zdravotní pojišťovna České republiky jej uveřejňuje v rámci zadávací dokumentace jí zadávaných veřejných zakázek. Tento dokument umožňuje utvořit si představu o standardech informační architektury ICT VZP ČR. Účelem jeho uveřejnění je poskytnout informace nezbytné pro integraci dodávané komponenty se stávajícím informačním systémem v souladu se Standardy ICT- VZP- NIS.

Uveřejněním tohoto dokumentu není dotčena právní odpovědnost spojená s jeho zneužitím.

V tomto dokumentu bylo použito názvů subjektů a názvů produktů, které mohou být chráněny příslušnými právními předpisy.

**Otevřením tohoto dokumentu berete výše uvedené skutečnosti na vědomí.**

# Obsah

1. Úvod ... 7
2. Integrace aplikace ... 7
2.1 Varianty integrace s IDM/OIM ... 9
2.1.1 Externí úložiště uživatelských dat (integrace s ADB nebo AD) ... 9
2.1.2 Vlastní úložiště uživatelských dat ... 10
2.2 OIM ... 12
2.3 ADB ... 13
2.3.1 Výhody použití ADB ... 14
2.3.2 Knihovna ... 15
2.3.3 Role ... 16
2.3.4 Lokality ... 16
2.4 Role ... 16
2.4.1 Metodika definování rolí ... 18
2.4.2 Kombinace „Role“ a „Pracovní úsek“ ... 19
2.5 ESSO LM ... 20
2.5.1 Spolupráce systémů OIM a eSSO ... 21
2.6 RAP ... 22
2.6.1 Integrace aplikace s RAP ... 23
2.7 GMUSERS – Katalog uživatelů ... 23
3. Fáze integrace aplikace ... 23
3.1 Kroky a zodpovědnosti během integrace aplikace do IDM řešení ... 25
4. PL/SQL API – komunikační rozhraní ... 26
4.1 Procedura Create User ... 26
4.2 Procedura UpdateUser ... 27
4.3 Procedura ChangePassword ... 27
4.4 Procedura LockUser ... 28
4.5 Procedura UnlockUser ... 28
4.6 Procedura DeleteUser ... 28
4.7 Procedura AddRole ... 29
4.8 Procedura RemoveRole ... 29
4.9 Návratové kódy ... 29
5. Reference ... 30

# Seznam obrázků

Obrázek 1 - Přehled IDM komponent ..... 9
Obrázek 2 – Integrace aplikace - externí úložiště ..... 10
Obrázek 3 – Integrace aplikace - vlastní úložiště ..... 11
Obrázek 4 - Schéma správy identity pomocí OIM ..... 12
Obrázek 5 - Relační model ADB ..... 13
Obrázek 6 - Řešení ADB ..... 14
Obrázek 7 - Ukázka GUI ADB aplikace - seznam uživatelů ..... 15
Obrázek 8 - Schéma využití knihovny ADBLib ..... 16
Obrázek 9 - Pyramida rolí ..... 17
Obrázek 10 – Role v nepřímé integraci ..... 18
Obrázek 11 - Role v přímé integraci ..... 18
Obrázek 12Příklad Business role a vazby na typové role ..... 19
Obrázek 13Princip Oracle eSSO LM ..... 21
Obrázek 14 - Schéma zobrazení aplikace RAP ..... 22

# Historie dokumentu

| Verze | Datum | Autor | Popis |
|---|---|---|---|
| 1.06 | 17.10.2017 | ÚICT VZP ČR | Vytvoření dokumentu |

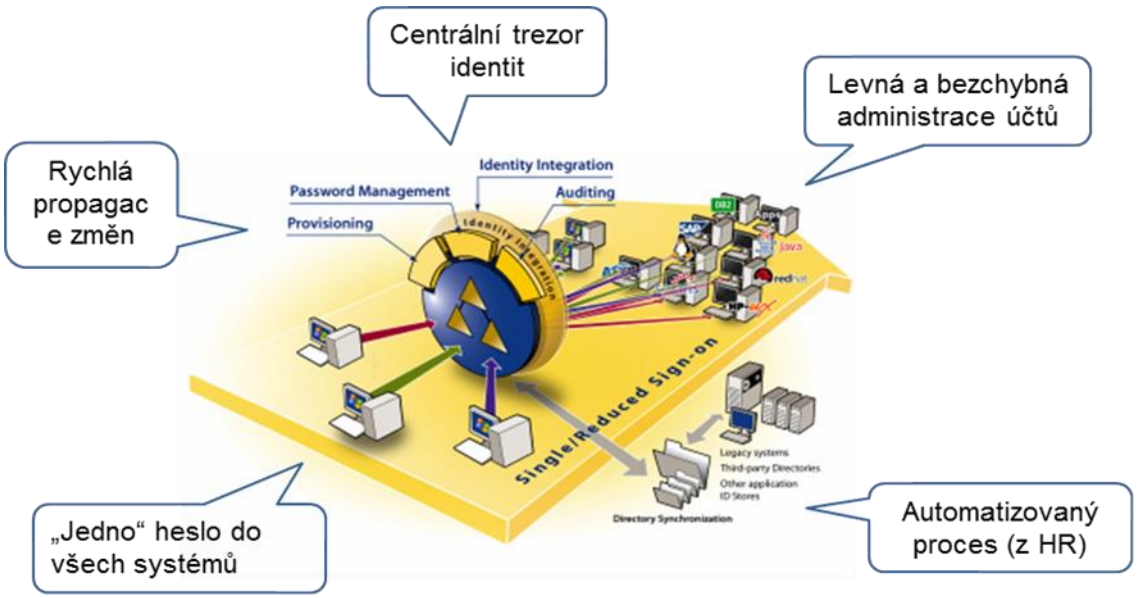
# 1. Úvod

Dokument obsahuje sadu standardů pro vybudování integračních vazeb nově dodávaných komponent informačního systému se stávajícími komponentami prostřednictvím integrační platformy v souladu se Standardy ICT VZP ČR. Vytvořené standardy jsou základem pro další rozšiřování systému zaváděním nových komponent a to jak „standardních“, tak i vytvářených dle specifických požadavků VZP ČR. Tento dokument je součástí výše uvedených Standardů ICT.

V případě specifikace rozšíření informačního systému zaváděním nových komponent ve smlouvě s dodavatelem, má specifikace uváděná v této smlouvě přednost před Standardy.

# 2. Integrace aplikace

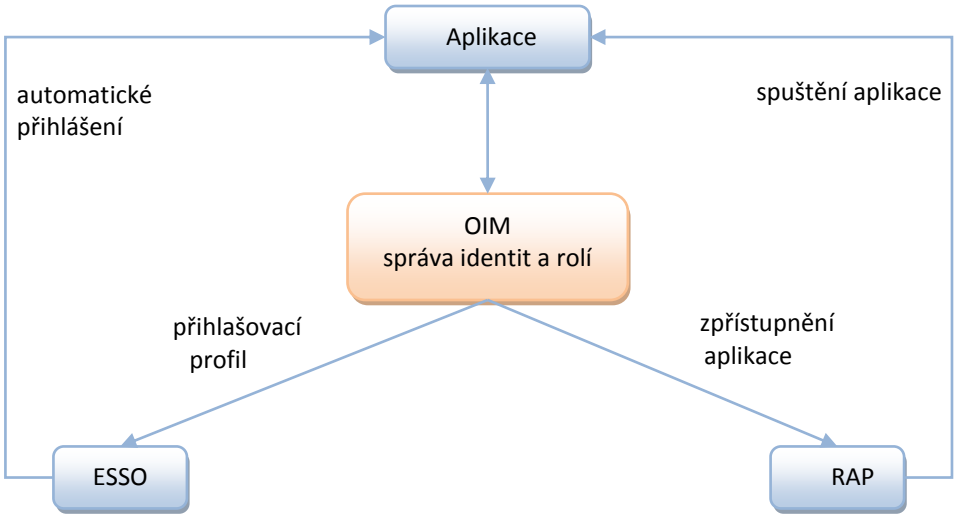
Dokument si klade za cíl seznámení s principy integrace aplikace do řešení IDM (Identity Management). Detailní informace o IDM řešení lze získat z dokumentace, která je uvedena v kapitole Refernce.




Co nabízí integrace aplikace s řešením IDM?

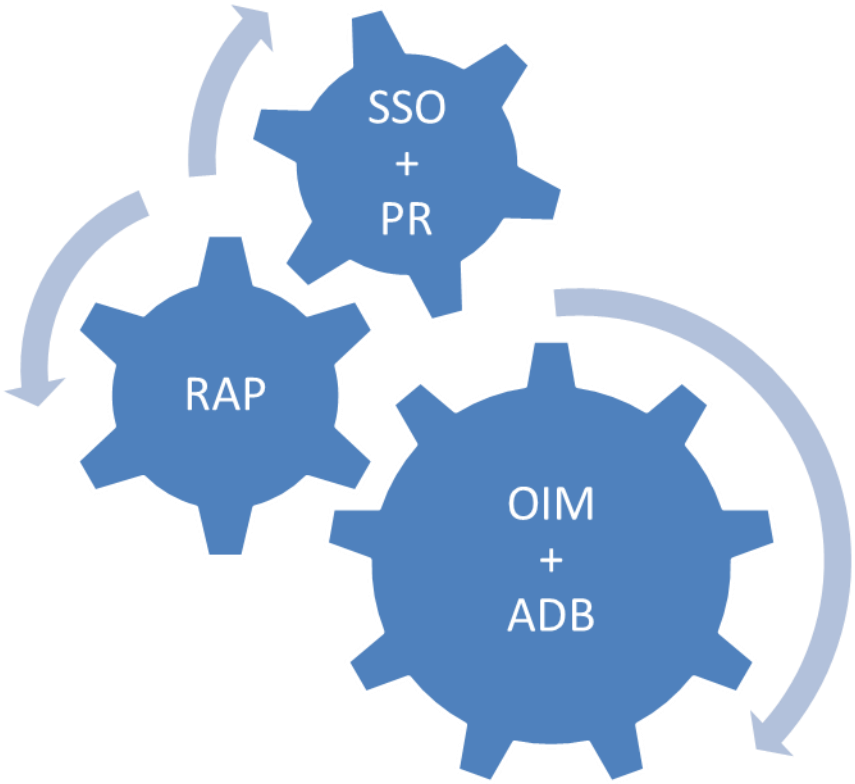
- Centrální správa uživatelských účtů a rolí pomocí Oracle Identity Manager (viz kapitola 2.1)
  - Správa identit uživatelů (jméno / heslo)
  - Správa oprávnění uživatelů pro přístup do aplikace (role, práva)
- Metodicky řešená podpora řízení oprávnění na základě rolí resp. hierarchie rolí
- Externí, konsolidované repozitory autentizačních a autorizačních dat s podporou specifik VZP – komponenta ADB (Autorizační Databáze)
- Řízené zpřístupnění aplikace (odkazu) cílovým uživatelům pomocí Rozcestníku aplikací (viz kapitola 2.6)

- Podporu Single Sign On (SSO) - automatické přihlášení cílových uživatelů do aplikace pomocí produktu Oracle Enterprise Single Sign-On Logon Manager (viz kapitola 2.5). Přihlašovací údaje do integrovaných aplikací pak spravuje OIM a vlastní přihlašování provádí Oracle eSSO LM.




Další kapitoly jsou členěny dle nabízených funkčností IDM řešení:

- Volba formy integrace s IDM (OIM)
- OIM – správa identit
- Řízení oprávnění na základě rolí
- ADB - externí, konsolidované úložiště uživatelských oprávnění
- eSSO – automatické přihlášení uživatele
- RAP – rozcestník aplikací




*Obrázek 1 - Přehled IDM komponent*

## 2.1 Varianty integrace s IDM/OIM

Aby bylo možné připojit aplikaci OIM a vyžívat tak všech možností z toho plynoucích, je nejdříve nutné zvolit způsob integrace.

Způsob se volí dle druhu úložiště dat o uživatelích a jejich rolích:

1. **Externí úložiště dat** – jedná se o preferovaný způsob integrace. Aplikace využívá externí úložiště uživatelů aplikace a jejich rolí. Úložištěm dat je Autorizační databáze ADB, která je již s OIM integrována a zajišťuje tedy plnou spolupráci s OIM. Z pohledu OIM se jedná o nepřímou integraci.
2. **Vlastní úložiště dat** – pokud aplikace buď neumožňuje použít externí úložiště dat, nebo je tento způsob z nějakého důvodu nevhodný, lze nadále využívat vlastní úložiště dat provést takzvanou přímou integraci s OIM.

### 2.1.1 Externí úložiště uživatelských dat (integrace s ADB nebo AD)

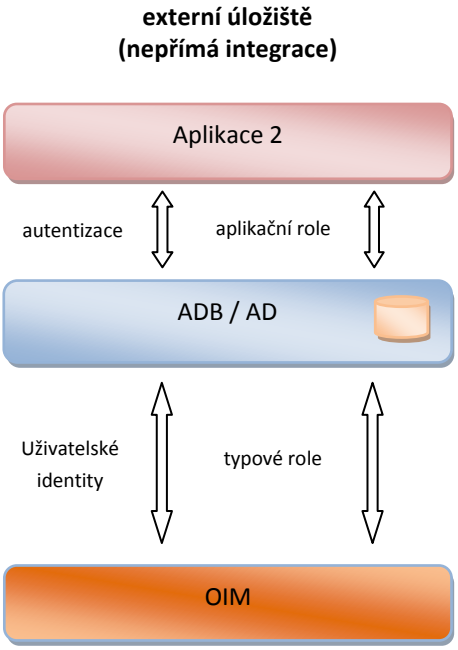
V rámci nepřímé integrace je třeba připravit aplikaci pro oddělení svého úložiště autentizačních a autorizačních dat a jeho nahrazení autorizační databází ADB pomocí ADBLib knihovny (podrobné informace viz dokumentace ADB API uvedená v kapitole Reference. Podle typu aplikace se zvolí formát dodané knihovny ADB.

- Knihovna „jar“ – aplikace využívající technologii java
- Knihovna „pll“ – aplikace vytvořené v technologii Oracle Forms

Dále je třeba připravit seznam aplikačních rolí a jmenování zástupce, který se bude účastnit jednání o mapování typových a business rolích.

Pro vývojáře je k dispozici:

- Dokumentace ADB knihovny
- Knihovna ADB pro vývoj (verze XML) a integrační testy v TVS (verze WS)
- Podpora knihovny ADB ze strany dodavatele ADB




*Obrázek 2 – Integrace aplikace - externí úložiště*

## 2.1.2 Vlastní úložiště uživatelských dat

V případě, že aplikace preferuje použití vlastního úložiště dat, je nutné implementovat přímou integraci se systémem OIM – Oracle Identity Manager. Integrační rozhraní dovoluje obousměrnou komunikaci, v terminologií OIM / IDM se jedná o tzv.:

- Provisioning – poskytování údajů z IDM do integrované aplikace, tj. směr komunikace je z OIM do integrované aplikace
- Reconciliation – sjednocení údajů v IDM dle stavu dat v integrované aplikaci, tj. směr komunikace je z integrované aplikace do OIM

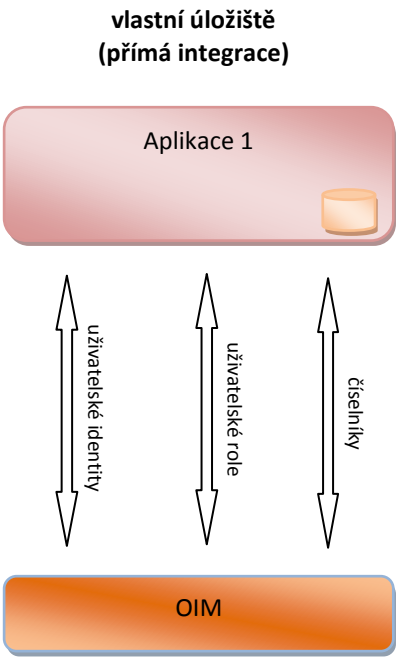
Pro implementaci integrace je nutné provést následující:

- Implementovat PL/SQL rozhraní na straně integrované aplikace (viz příloha), které slouží pro účely „provisioningu“

- Připravit tabulky/view na straně integrované aplikace pro účely „reconciliation“. Tabulky obsahují následující typy dat:
    - tabulka uživatelů (identit)
    - tabulka rolí přiřazených k uživatelům
    - tabulky číselníky, mezi které například patří číselník rolí

Pro možnost inkrementální „rekonciliace“, tj. přenosu pouze části dat, u kterých nastala změna od poslední „rekonciliace“, je nutné, aby tabulky (view) obsahovaly sloupec s datem poslední aktualizace.

Pro integrační testy je nutné předat IDM týmu přihlašovací údaje k databázi, tj. IP adresa a port, verze DB, SID DB, username, heslo atd.




*Obrázek 3 – Integrace aplikace - vlastní úložiště*

### 2.1.2.1 Přenosu dat z aplikace do OIM

Pro umožnění přenosu z aplikace do OIM stačí v databázi definovat tabulku nebo view. Každá taková tabulka nebo view by měly obsahovat sloupec určující datum a čas poslední změny daného řádku. OIM se pak snadno do takového databázového objektu podívá a získá údaje o posledních provedených změnách.

Přenášená data:

- Uživatelské identity (například přihlašovací jméno, heslo, jméno, příjmení, telefon, …)
- Uživatelské typové role (například administrátor aplikace, evidence uživatelů, …)
- Číselníky (například seznam pracovišť, seznam skupin, …)

#### 2.1.2.2 Přenos dat z OIM do aplikace

Pro zajištění funkcionality OIM vzhledem k uživatelům a jejich rolím v aplikaci, je definováno komunikační rozhraní PL/SQL API, které umožňuje základní operace s uživatelskými účty a jejich rolemi:

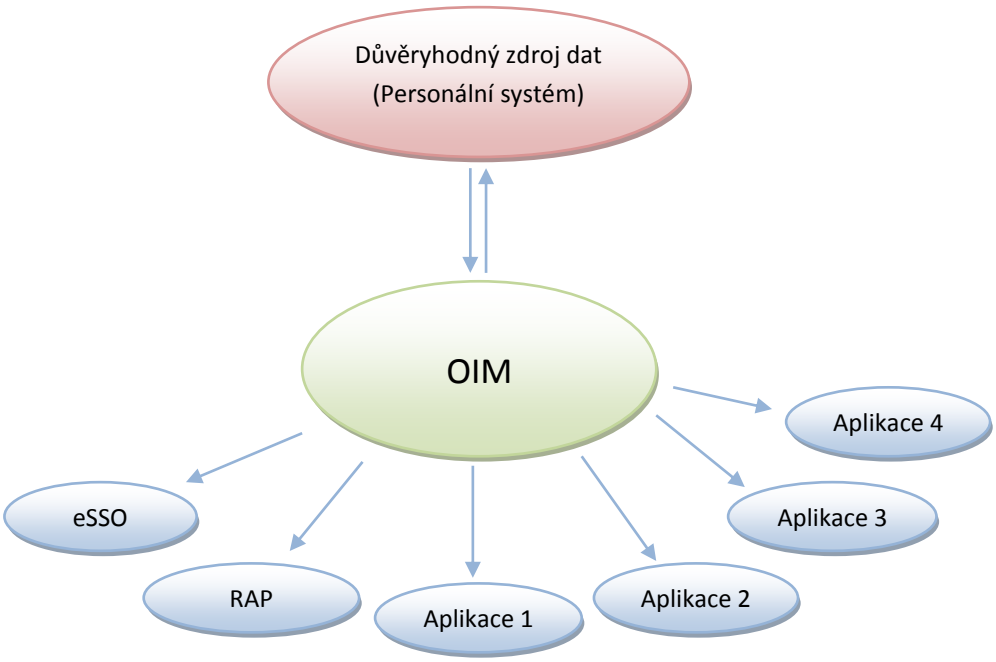
- **CreateUser** – Vložit uživatelský účet
- **UpdateUser** – Aktualizovat údaje o uživatelském účtu
- **LockUser** – Pozastavení uživatelského účtu
- **UnlockUser** – Obnovení uživatelského účtu
- **DeleteUser** – Smazání uživatelského účtu
- **ChangePassword** – Změna hesla uživatelského účtu
- **AddRole** – Přidání role
- **RemoveRole** – Odebrání role

Podrobnější informace o komunikačním rozhraní viz příloha PL/SQL API.

## 2.2 OIM

Oracle Identity Manager (OIM) zajišťuje centralizaci správy identit integrovaných aplikací a práv identit (rolí). Informace o uživateli jsou uložené na jednom místě a odtud automaticky propagovány do integrovaných aplikací (viz Obrázek 4 - Schéma správy identity pomocí OIM). Například pokud se uživatelka vdá a změní příjmení, je tato změna propagována do všech integrovaných aplikací. Zároveň OIM může z integrovaných aplikací získávat aktuální data (například změny v číselnících) a případně je propagovat dále.

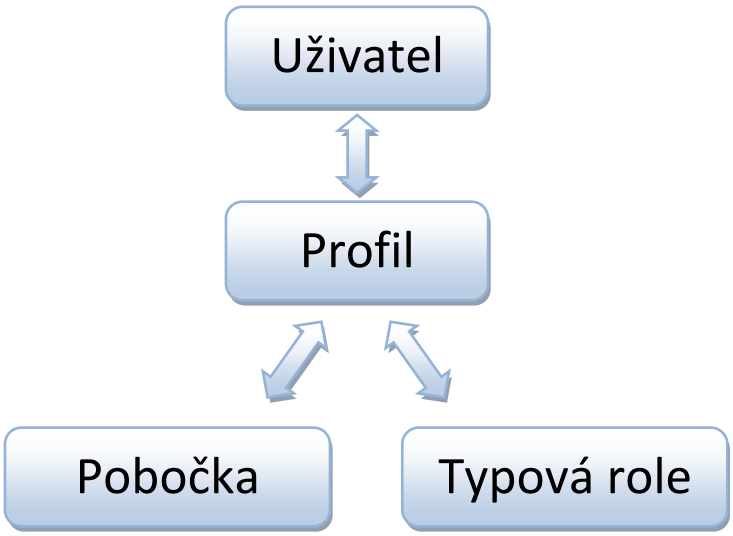
V rámci celé společnosti je tedy uživatel vždy zastoupen jednou identitou v OIM. Tato identita obsahuje všechny potřebné údaje o uživateli (v případě VZP jsou získávané z personálního systému VEMA). OIM řídí, do kterých aplikací má daná identita přístup a jaké má oprávnění (role) v aplikaci.




*Obrázek 4 - Schéma správy identity pomocí OIM*

## 2.3 ADB

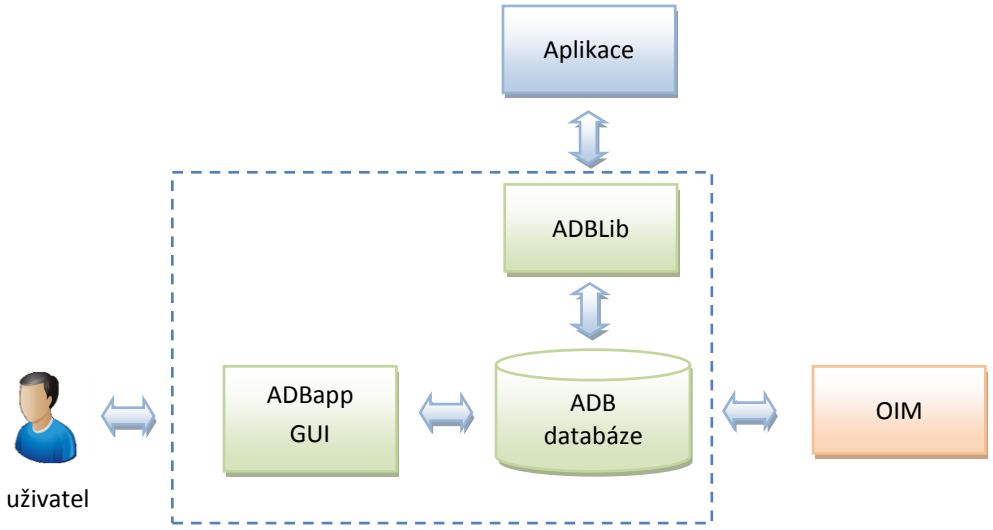
Autorizační databáze (ADB) je centrálním a konsolidovaným úložištěm dat určeným pro správu uživatelů a jejich rolí vzhledem k aplikacím. K vytvoření ADB vedly specifické požadavky v prostředí VZP. Každý uživatel ve VZP má přiřazeny své typové role (každá typová role může obsahovat jednu a více aplikačních rolí), které jsou ale zároveň vázány na konkrétní pracoviště. Vzhledem k velkému množství uživatelů, pracovišť a rolí tak vznikla ADB, která ukládá tyto údaje v jednoduchém relačním modelu (viz Obrázek 5 - Relační model ADB).




*Obrázek 5 - Relační model ADB*

Následující schéma zobrazuje komponentový pohled na ADB řešení. ADB data jsou přístupná 3 způsoby:

1. Uživatelským rozhraním (GUI), které dovoluje plnou kontrolu na ADB daty.
2. Aplikace využívající ADB jako externího úložiště – pomocí API (ADBLib) dovolují číst data z ADB.
3. Řídící IDM systém (OIM) má plnou kontrolu nad ADB daty. Přístup je realizován skrze dedikované API pro OIM.

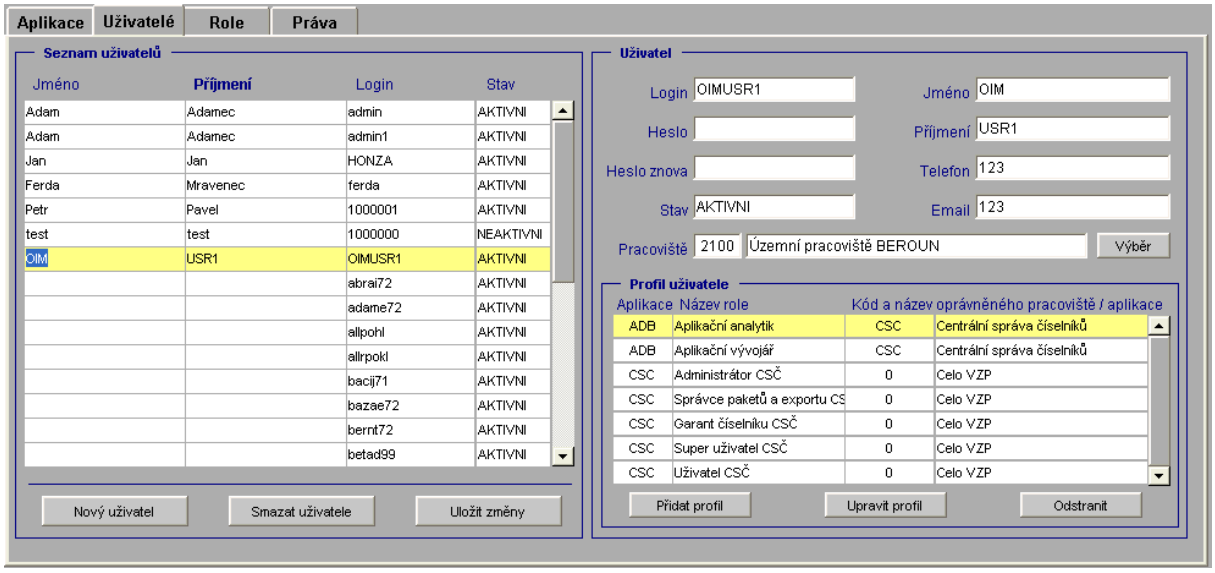



*Obrázek 6 - Řešení ADB*

## 2.3.1 Výhody použití ADB

Externí úložiště uživatelských dat v podobě ADB má následující výhody:

- Již vytvořená aplikace pro kompletní správu údajů, vytvořená v technologii Oracle Forms. Odpadá tedy nutnost vytváření vlastní správy uživatelů a jejich oprávnění v aplikaci.
- K dispozici jsou různé verze knihoven s jednotným rozhraním pro komunikaci s ADB. Stačí tedy odladit aplikaci, například s použitím XML verze knihovny, bez potřeby mít přístup k celé ADB, a po dokončení úprav jen vyměnit knihovnu a připojení s ADB bude fungovat.
    - Knihovna určená primárně pro vývoj, která umožňuje používat XML zdroj dat.
    - Knihovna určená pro komunikace s ADB prostřednictvím webových služeb.
    - V dohledné době bude k dispozici verze knihovny pro komunikaci s ADB prostřednictvím LDAP protokolu.
- Možnost zjednodušení práce s aplikačními rolemi pomocí typových rolí, které sdružují více aplikačních rolí dohromady, podle typu práce s aplikací. Typové role se pak snadněji u uživatelů spravují a mapují na business role.
- Aplikace nepotřebuje provádět žádnou správu svých uživatelů. To obstará ADB. Aplikace se pouze ptá (nepotřebuje provádět žádný zápis do oprávnění):
    - Existuje přihlašovaný uživatel?
    - Je heslo přihlašovaného uživatele správné?
    - Jaká oprávnění (aplikační role) má daný uživatel v aplikaci?
- Jednotný / konsolidovaný systém evidence uživatelů a oprávnění.
- Připravené GUI pro práci s ADB daty.



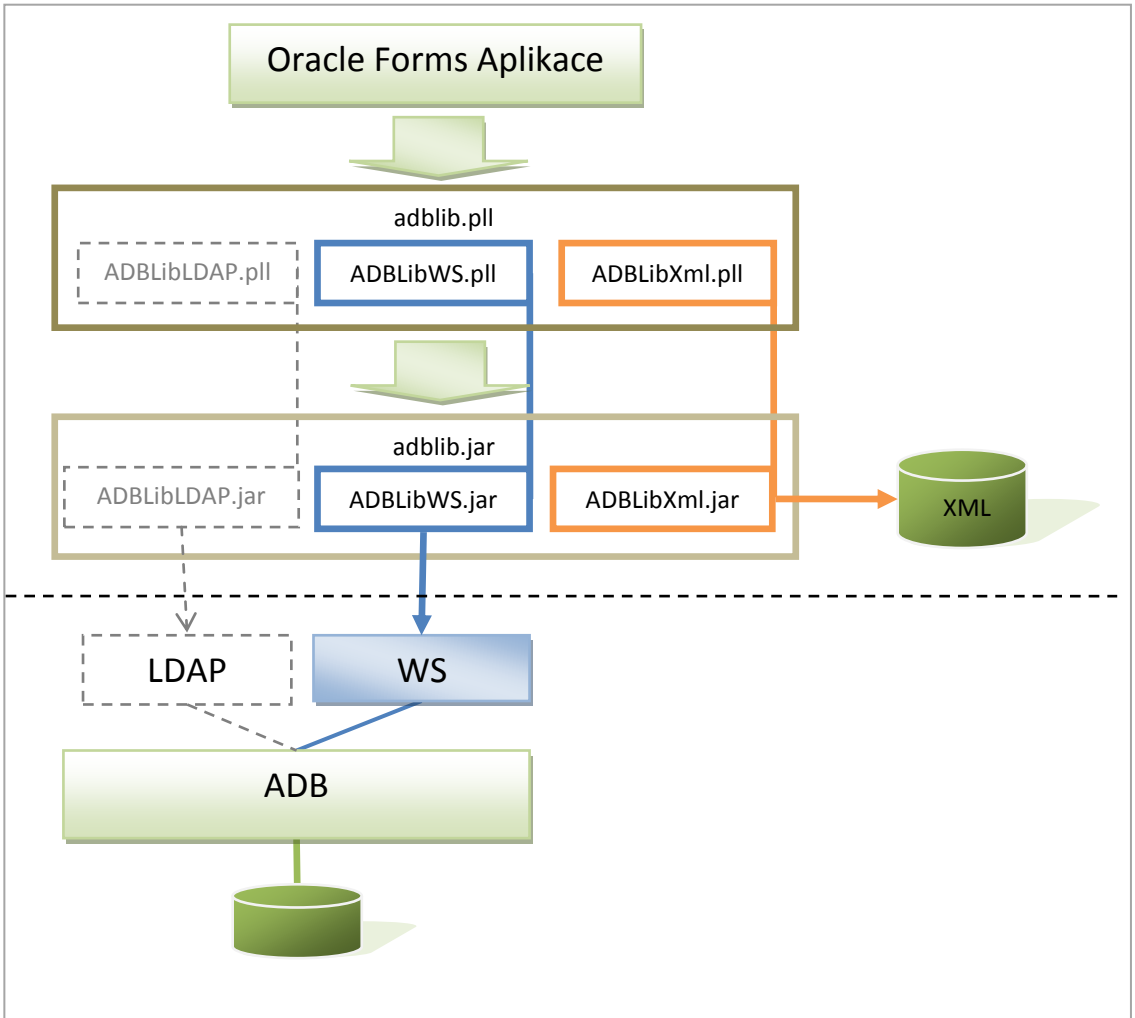

*Obrázek 7 - Ukázka GUI ADB aplikace - seznam uživatelů*

## 2.3.2 Knihovna

Knihovna ADBLib slouží ke komunikaci s autorizační databází ADB. V současné době jsou k dispozici 2 verze této knihovny (třetí verze, určená pro komunikaci prostřednictvím LDAP protokolu, bude dostupná později):

- Verze XML určená hlavně pro usnadnění vývoje, protože pro úpravu stávající či vývoj nové Oracle Forms aplikace není potřeba mít k dispozici celý systém autorizační databáze, ale stačí vytvořit si pouze data pomocí XML souborů.
- Verze WS, která v současné představuje dočasné řešení komunikace s vlastní Autorizační databází, než bude k dispozici rozhraní LDAP

Jednotné rozhraní knihovny ADBLib umožňuje vývoj Oracle Forms aplikace například na XML verzi, její odladění a poté prostou výměnou dvou souborů na aplikačním serveru Oracle Forms lze docílit výměnu verze ADBLib knihovny.




*Obrázek 8 - Schéma využití knihovny ADBLib*

### 2.3.3 Role

ADB nabízí možnost vytvoření typových rolí, které obsahují více aplikačních rolí. Více informací o rolích je k dispozici v následující kapitole.

### 2.3.4 Lokality

Typové role jsou vázané na pracoviště – lokality. Daná typová role uživatele může být na různých lokalitách a zároveň může mít uživatel v jedné lokalitě mít více typových rolí.

## 2.4 Role

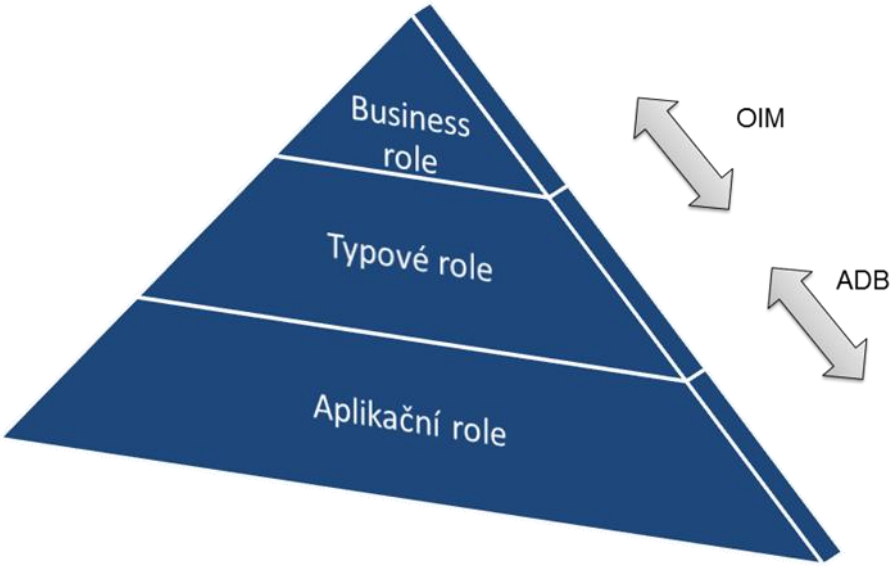
Role představují realizaci řízení oprávnění v aplikacích. Přiřazení role uživateli může být založeno na základě různých atributů uživatele: pracovního zařazení, pracoviště, dočasné potřeby, atd… Cílem je umožnit uživateli přístup pouze k informacím, ke kterým přístup má mít a umožnit mu s informacemi pracovat je tak, jak mu přísluší. K realizaci řízení bezpečnosti slouží 3 úrovně rolí.

Význam jednotlivých úrovní řízení bezpečnosti:

- AR - Aplikační role představuje zabezpečení na úrovni aplikace. Povoluje či zabraňuje tak vykonání konkrétní funkce aplikace. V případě vlastního úložiště dat se o správu aplikačních rolí stará sama

aplikaci. V případě použití externího úložiště ADB se o aplikační role stará ADB a na požádání aplikační role předává aplikaci.

- TR - Typové role představují seskupení oprávnění do logických (nedělitelných) celků. Umožňují usnadnění správy oprávnění v rámci jedné aplikace. K mapování aplikačních rolí na typové role dochází buď v ADB, tedy v případě využití externího úložiště dat anebo přímo v aplikaci, pokud to aplikace podporuje. V případě, že aplikace je aplikace integrována přímo, typové role nepodporuje a aplikačních rolí je málo, je možné prohlásit aplikační role za typové a provést tedy přímé mapování business rolí na role typové.
- BR - Business role seskupují typové role (tedy jednu a více aplikačních rolí) napříč více aplikacemi a odpovídají tak přiděleným zodpovědnostem (rolím) v rámci podnikových procesů. Například BR1=TR1+TR4+TR6… K mapování BR na TR dochází v OIM.

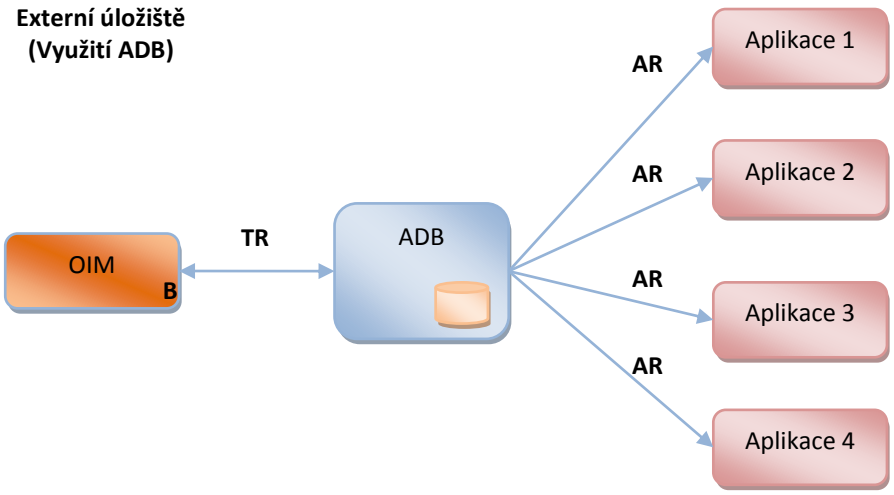



*Obrázek 9 - Pyramida rolí*

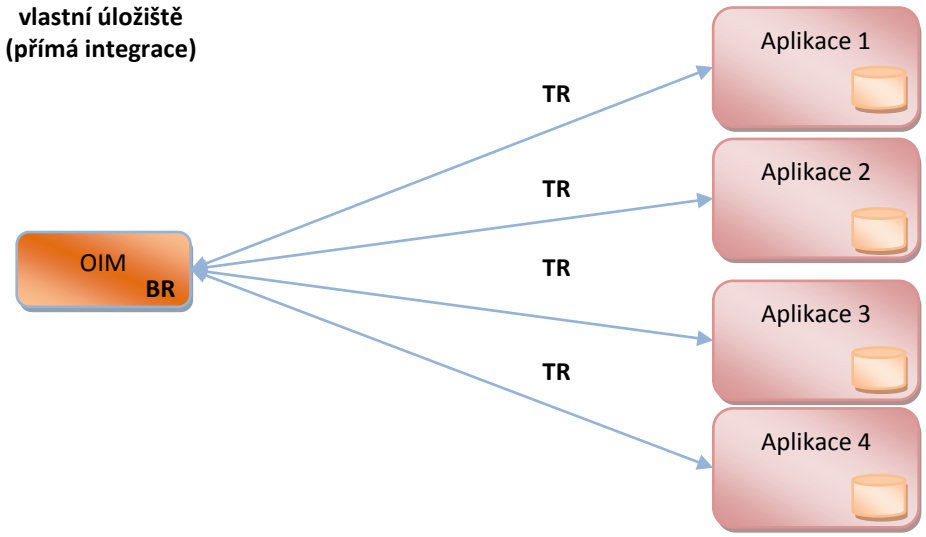
Důvodem použití více úrovní rolí je zajištění jak snadné správy přiřazení rolí uživateli, tj. práce s malým množstvím rolí, tak i v možnosti definovat velké množství oprávnění (aplikačních rolí) na úrovni aplikace.

Jednotlivé úrovně jsou umístěny v různých systémech a to na základě typu použité integrace:

- Mapování Business rolí na Typové role jsou vždy umístěny přímo v OIM
- Mapování Typových rolí na role aplikační se liší dle použité integrace
    - **Nepřímá integrace** – typové role jsou na aplikační mapovány v externím úložišti dat, v ADB (viz Obrázek 10 – Role v nepřímé integraci)
    - **Přímá integrace** – typové role jsou na aplikační mapovány ve vlastním úložišti aplikace (viz Obrázek 11 - Role v přímé integraci)




*Obrázek 10 – Role v nepřímé integraci*



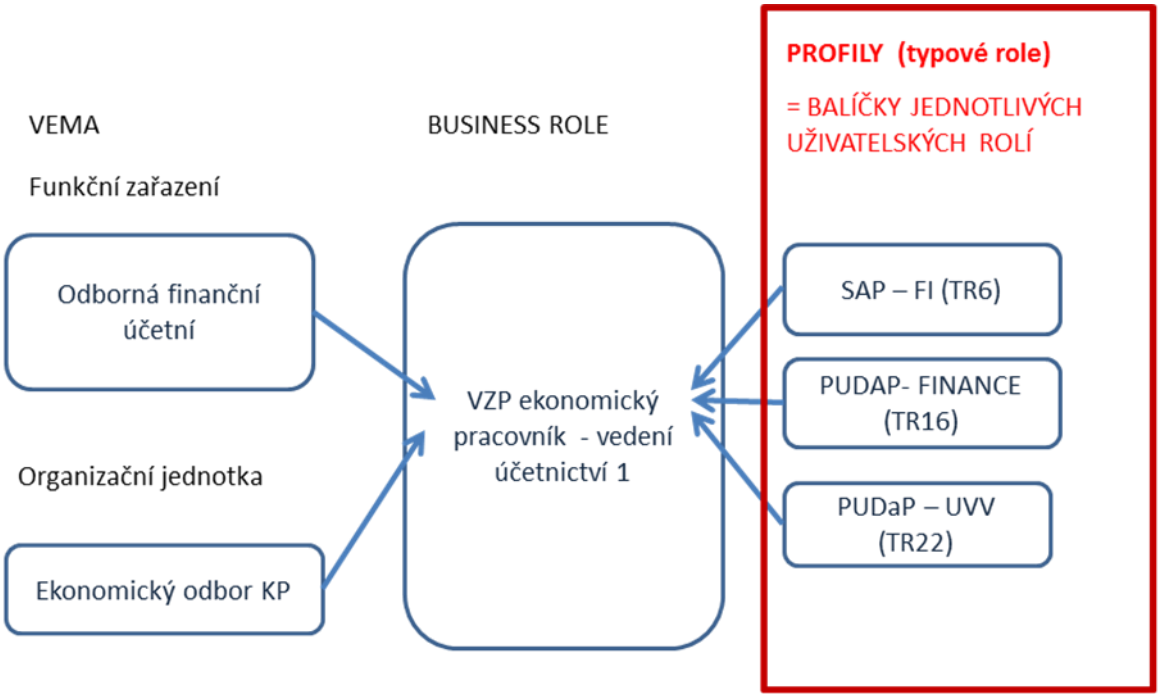

*Obrázek 11 - Role v přímé integraci*

## 2.4.1 Metodika definování rolí

Jednotlivé úrovně rolí mají rozdílný význam v interpretaci dané role.

- Aplikační role – představují identifikace rolí, které jsou jednoznačně interpretovatelné aplikační logikou aplikace, tj. řídí možnosti oprávnění v aplikaci

- Typové role – představují procesní kroky v agendě, která je aplikací podporovaná. Příkladem může být – zanesení objednávky, schválení faktury, rozhodnutí o žádosti, agenda EU dokladů atd. TR se skládá z AR, tj. TR náleží jedné aplikaci.
- Business role – představuje roli v podnikových procesech, tj. jedná se o tzv. kategorii zaměstnance – například účetní, krajský účetní kontrolor, ekonomický ředitel, přepážková pracovnice atd.

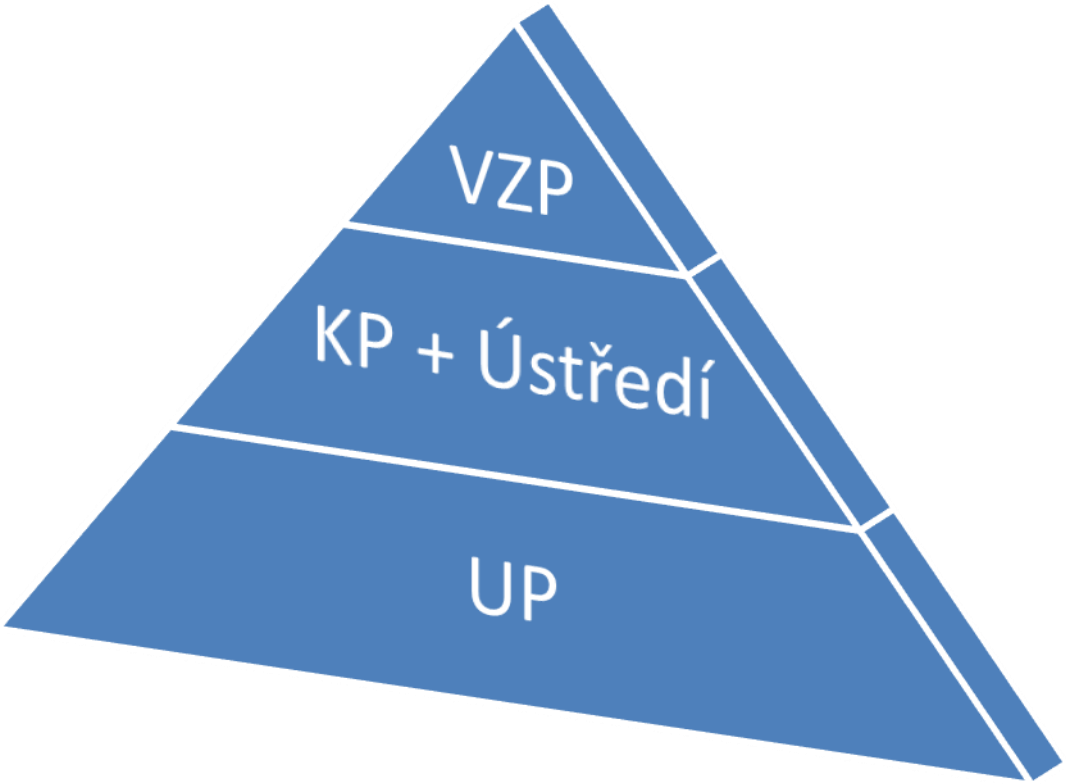



*Obrázek 12Příklad Business role a vazby na typové role*

## 2.4.2 Kombinace „Role“ a „Pracovní úsek“

V předchozím textu byl výraz „role“ použit pro funkční vymezení v rámci možností VZP. Toto vymezení ale není úplné, konkrétní role, která se přiděluje uživateli, musí ještě obsahovat vymezení se k pracovnímu úseku VZP, tj. vymezuje se datově. Kombinaci „role“ a „pracovního úseku“ budeme označovat jako instanci role. Tato konvence platí pro všechny úrovně rolí – pro business role, typové role i aplikační role.

Následující schéma zobrazuje hierarchické uspořádání pracovních úseků VZP:




Hierarchie se má úrovně:

- VZP – veškerá data VZP
- KP (včetně ústředí) – krajské celky VZP a ústředí, tj. 14 krajů a ústředí
- UP – územní pracoviště, cca 80 okrasních měst ČR, každé územní pracoviště přísluší právě jednomu kraji

Kód pro VZP je 0, kraje mají kódy 1 až 14, ústředí má kód 9800, územní pracoviště mají 4 ciferný kód, kde 3 a 4 pozice je 0, např. 2100.

Příklady instancí rolí jsou:

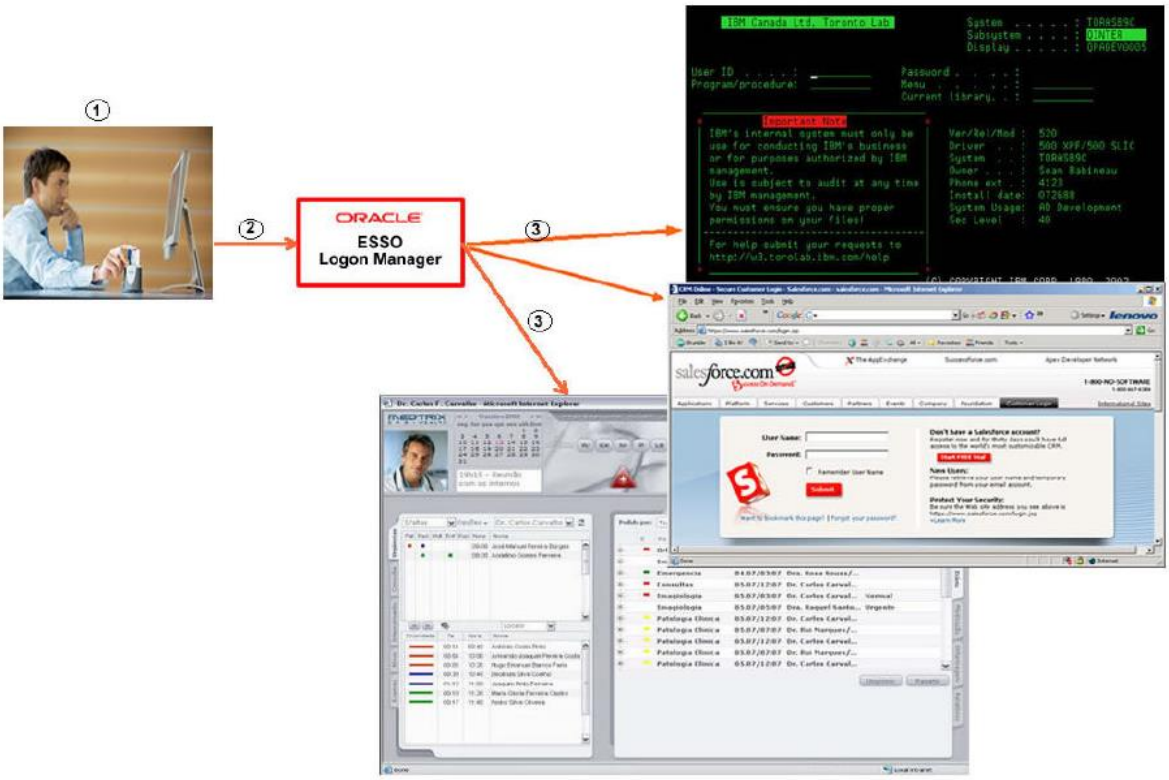
- FIN_TR34_7200
- BR15_0
- RSZP_PK_U66_15

## 2.5 ESSO LM

Oracle Single Sign-On Logon Manager (eSSO LM) zajišťuje zabezpečené uložení přihlašovacích informací a umožňuje automatické přihlášení do různých druhů aplikací, například:

- Windows aplikace
- Internetové aplikace

- Java aplikace
- Oracle Forms aplikace




*Obrázek 13Princip Oracle eSSO LM*

Ke spárování uživatele a profilu v eSSO LM slouží uživatelův doménový účet.

Aby bylo možné přihlášení k aplikaci pomocí jejího přihlašovacího dialogu, je potřeba zajistit identifikovatelnou tohoto dialogu, například jednoznačně identifikovatelným textem v názvu přihlašovacího dialogu.

Pro úspěšnou integraci aplikace do IDM řešení je nutné vytvořit přihlašovací profil aplikace v systému eSSO LM. Přihlašovací profil zajišťuje rozeznatelnost přihlašovací dialog aplikace pro automatické zadání jména a hesla systémem Logon Manager, který je nainstalován na pracovní stanici uživatele. V průběhu procesu integrace může být identifikována potřeba provést úpravu přihlašovacího dialogu tak, aby ho mohl Logon Manager jednoznačně identifikovat přihlašovací dialog.

Systém Oracle eSSO není jediným způsobem zajištění SSO ve VZP. Mezi další způsoby patří například metody / technologie:

- Kerberos,
- NTLM,

které se ve VZP využívají, především v prostředí technologií společnosti Microsoft.

## 2.5.1 Spolupráce systémů OIM a eSSO

Systém OIM je řídícím prvkem mezi IDM systémy, řídí tedy i životní cyklus účtů v integrovaných aplikacích, tj. včetně událostí typu založení účtu, změna hesla k účtu atd. Systémem OIM při těchto operacích

paralelně komunikuje se systémem eSSO a předává mu přihlašovací údaje, které jsou právě modifikovány v integrované aplikaci. Uživatel nezná přihlašovací údaje a systém eSSO vyplňuje přihlašovací údaje za uživatele v okamžiku zobrazení přihlašovacího dialogu integrované aplikace.

## 2.6 RAP

Rozcestník aplikací (RAP) je z pohledu uživatele aplikace, která zobrazuje seznam dostupných aplikací a umožňuje jejich spuštění. Za aplikací je skryt celý systém pro evidenci dostupných aplikací k jednotlivým uživatelům.

*Obrázek 14 - Schéma zobrazení aplikace RAP*

Každý uživatel systému RAP musí mít vytvořený uživatelský účet a mít nastaveny pracovní plochy a aplikace. Spuštěním klientské aplikace RAP dojde k přihlášení uživatele (resp. klienta – tj. klientské aplikace) do systému RAP. Uživatel je ověřován na základě uživatelského jména, pod kterým je přihlášen do domény. Při úspěšném přihlášení je uživateli vygenerováno komunikační číslo, které nadále slouží pro vlastní komunikaci se systémem. Dále je uživateli nastavena klientská aplikace RAP. Jsou zjištěny pracovní plochy uživatele, záložky (karty) a aplikace na nich. Klient také získá hodnotu intervalu pro pravidelné oznamování stavu systému RAP.

V tuto chvíli je klient přihlášen a může spouštět přidělené aplikace. Spouštěné aplikace je opět realizováno webovou službou. Dle typu spuštěné aplikace klient rozhodne o způsobu využití vráceného příkazu z odpovědi služby.

- V případě aplikace typu **EXE** dojde k přímému spuštění aplikace na počítači uživatele.
- Pokud se jedná o aplikaci typu **URL**, dojde ke spuštění Internet Exploreru s přednastaveným url.
- U aplikace typu **HOST**, která je vzdálenou aplikací (tzv. server-side) se nejprve na základě tzv. load-balancingu vybere aplikační server a dojde ke spuštění internetového prohlížeče s otevřením aplikace z

vybraného aplikačního serveru. Tento případ může nastat zejména pro aplikace běžící na technologii Oracle Forms.

### 2.6.1 Integrace aplikace s RAP

Pro integraci aplikace se systémem RAP je třeba:

- Určit typ aplikace
- Připravit název a popis aplikace tak, jak bude vystupovat na kartě pracovní plochy uživatele
- Připravit způsob spouštění aplikace (příkazový řádek, URL, parametry, server …)
- Případně i připravit ikonu představující aplikaci

## 2.7 GMUSERS – Katalog uživatelů

Dalším tématem spolupráce IDM a podnikových aplikací je distribuce katalogu uživatelů. Katalog uživatelů je spravován personálním systémem VEMA, obsahuje veškeré personální informace.

Katalog je realizován ve formě tabulky GMUSERS a primárním úložištěm je sdílený číselník.

Tabulka GMUSERS obsahuje veškeré zaměstnance VZP a je možné jí mít k dispozici pomocí SDI (silné datové integrace).

| Sloupec | Typ | Nepovinný (Nullable) |
|---|---|---|
| **AD_USERNAME** | VARCHAR2(30) | No |
| **JMENO** | VARCHAR2(30) | No |
| **PRIJMENI** | VARCHAR2(30) | No |
| **TITUL** | VARCHAR2(20) | Yes |
| **TEL** | VARCHAR2(1000) | Yes |
| **FAX** | VARCHAR2(100) | Yes |
| **EMAIL** | VARCHAR2(100) | Yes |
| **PRAC_USEK** | VARCHAR2(4) | No |
| **FUNKCE** | VARCHAR2(300) | No |
| **PLATNOST** | CHAR(1) | No |

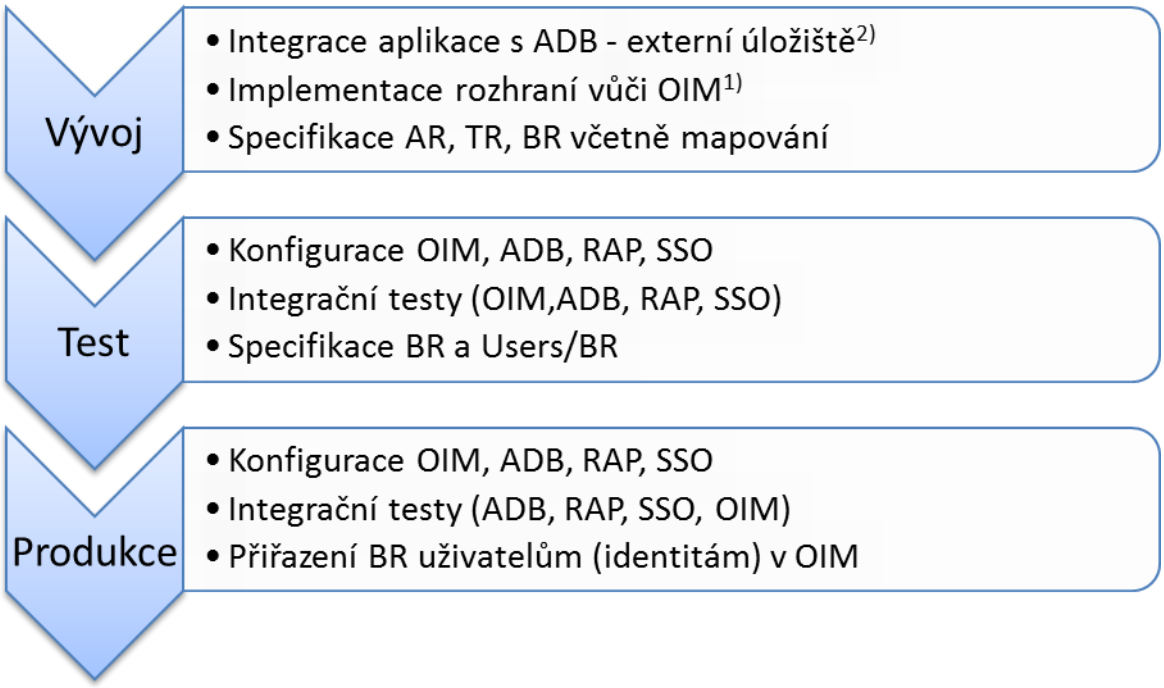
# 3. Fáze integrace aplikace

Integrace aplikace do IDM není otázkou jednoho kroku, ale představuje komplexní proces, který trvá typicky několik týdnů a obsahuje řadu nutných součinností.

Z pohledu dodavatele aplikací proces integrace do IDM dělíme do 3 fází:

- **Vývoj** – vlastní úprava aplikace pro integraci do IDM
- **Test** – mapování business a typových rolí, provádění integračních testů

- **Produkce** – konfigurace a nasazení do produkčního prostředí včetně přidělení business rolí koncovým uživatelům




*Poznámky:*

1) *Jedná se o variantu integrace „vlastní“ úložiště / přímá integrace s OIM*
2) *Jedná se o variantu integrace „externí“ úložiště / integrace skrze ADB*

Samotná proces integrace aplikace se dá dělit do dvou oblastí:

- Technologická oblast – integrační vrstva, tj. jedná se o samotné zajištění komunikace IDM komponent a integrované aplikace.
- Aplikační oblast - business úroveň, tj. jedná se o problematiku řízení identit a rolí v integrovaných aplikacích – definování business rolí, schvalovacích procesů, typových rolí atd.

Ve fázi vývoje se typicky řeší úlohy z technologické (integrační) vrstvy. Ve fázích testů a produkčního provozu se naopak řeší především oblast aplikační.

## 3.1 Kroky a zodpovědnosti během integrace aplikace do IDM řešení

| Fáze | Procesní krok | VZP - IDM | VZP - garant aplikace | Dodavatel aplikace | HP/GEM | Komentář |
|---|---|---|---|---|---|---|
| | Předání materiálů pro integraci s IDM | | | | | Dokumentace, knihovny, přístupová oprávnění |
| VÝVOJ | Implementace API (rozhraní) pro OIM komunikaci[1)] | | | X | | |
| | Vhodnost LOGIN dialogu aplikace pro SSO | | | X | | |
| | Integrace s ADB (ADB knihovna)[2)] | | | X | | Případná změna modelu řízení oprávnění |
| | Podpora dodavatele při integraci s IDM | | | | X | |
| | Seznam TR, AR (včetně mapování) pro nastavení ADB[2)] | | | X | | |
| | Seznam TR pro nastavení OIM[1)] | | | X | | |
| | Specifikace BR a schvalovacích procesů | | X | | X | |
| | Rozšíření konfigurace OIM (BR, konektor k aplikaci) | | | | X | |
| TEST | Konfigurace ADB dle podkladů TR/AR[2)] | X | | | | |
| | Konfigurace OIM včetně BR [1)] | X | | | | |
| | Podklady pro RAP, eSSO | | | X | X | URL, test uživatel/heslo |
| | Konfigurace RAP, eSSO | X | | | | |
| | Specifikace BR a schvalovacích procesů | | X | | X | |
| | Specifikace mapování „uživatelů VZP a BR“ | | X | | | |
| | Integrační testy (RAP, eSSO, OIM, ADB) | X | | X | X | |
| PRODUKCE | Konfigurace ADB dle podkladů TR/AR[2)] | X | | | | |
| | Konfigurace OIM včetně BR [1)] | X | | | | |
| | Přiřazení BR v OIM dle mapování „uživatelů a BR“ | X | | | | |
| | Integrační testy (RAP, eSSO, OIM, ADB) | | | | | |
| | Podklady pro RAP, eSSO | | X | X | | |
| | Konfigurace RAP, eSSO | X | X | | | Zpřístupnění aplikace pro koncové uživatele |

*Poznámky:*

1) *Jedná se o variantu integrace „vlastní“ úložiště / přímá integrace s OIM*
2) *Jedná se o variantu integrace „externí“ úložiště / integrace skrze ADB*

# 4. PL/SQL API – komunikační rozhraní

## 4.1 Procedura Create User

Tato procedura je určena k vytvoření uživatelského účtu.

```
PROCEDURE CreateUser
(
UserID in varchar2,
FirstName in varchar2,
LastName in varchar2,
Organization in varchar2,
EmployeeType in varchar2,
ManagerID in varchar2,
Email in varchar2,
Telephone in varchar2,
UserLocked in varchar2,
StartDate in DATE,
EndDate in DATE,
UserPassword in varchar2,
Result out varchar2
)
```

*Parametry:*

- *UserID – jedinečný identifikátor uživatele*
- *FirstName – jméno uživatele*
- *LastName – příjmení uživatele*
- *Organization - organizace*
- *EmployeeType – typ uživatele*
- *ManagerID – jedinečný identifikátor nadřízeného daného uživatele*
- *Email – email uživatele*
- *Telephone – telefon uživatele*
- *UserLocked – určuje, zda je uživatelský účet aktivní (uživatel může přistupovat do Forms aplikace)*
- *StartDate – začátek platnosti účtu*
- *EndDate – konec platnosti účtu*
- *UserPassword – heslo pro uživatelský účet*
- *Result – výsledek procedury*

## 4.2 Procedura UpdateUser

Tato procedura je určena k změně parametrů uživatelského účtu.

```
PROCEDURE UpdateUser
(
UserID in varchar2,
FirstName in varchar2,
LastName in varchar2,
Organization in varchar2,
EmployeeType in varchar2,
ManagerID in varchar2,
Email in varchar2,
Telephone in varchar2,
StartDate in DATE,
EndDate in DATE,
Result out varchar2
)
```

*Parametry:*

- *UserID – jedinečný identifikátor uživatele*
- *FirstName – jméno uživatele*
- *LastName – příjmení uživatele*
- *Organization – organizace*
- *EmployeeType – typ uživatele*
- *ManagerID – jedinečný identifikátor nadřízeného daného uživatele*
- *Email – email uživatele*
- *Telephone – telefon uživatele*
- *StartDate – začátek platnosti účtu*
- *EndDate – konec platnosti účtu*
- *Result – výsledek procedury*

## 4.3 Procedura ChangePassword

Tato procedura je určena k změně hesla k uživatelskému účtu.

```
PROCEDURE ChangePassword
(
UserID in varchar2,
UserPassword in varchar,
```

```
Result out varchar2
)
```

*Parametry:*

*UserID – jedinečný identifikátor uživatele*

*UserPassword – nové heslo pro uživatelský účet*

*Result – výsledek procedury*

## 4.4 Procedura LockUser

Tato procedura je určena k uzamčení uživatelského účtu. Uživatelský účet se stává neaktivním.

```
PROCEDURE LockUser
(
UserID in varchar2,
Result out varchar2
)
```

*Parametry:*

- *UserID – jedinečný identifikátor uživatele*
- *Result – výsledek procedury*

## 4.5 Procedura UnlockUser

Tato procedura je určena k odemčení uživatelského účtu. Uživatelský účet se stává aktivním.

```
PROCEDURE UnlockUser
(
UserID in varchar2,
Result out varchar2
)
```

*Parametry:*

- *UserID – jedinečný identifikátor uživatele*
- *Result – výsledek procedury*

## 4.6 Procedura DeleteUser

Tato procedura je určena k vymazání uživatelského účtu ze správy uživatelů.

```
PROCEDURE DeleteUser
(
UserID in varchar2,
Result out varchar2
)
```

*Parametry:*

- *UserID – jedinečný identifikátor uživatele*

- *Result – výsledek procedury*

## 4.7 Procedura AddRole

Tato procedura je určena k přidání role pro daného uživatele.

```
PROCEDURE AddRole
(
UserID in varchar2,
Workplace in varchar2,
Role in varchar2,
Result out varchar2
)
```

*Parametry:*

- *UserID – jedinečný identifikátor uživatele*
- *Workplace – pracoviště uživatele*
- *Role – role uživatele*
- *Result – výsledek procedury*

## 4.8 Procedura RemoveRole

Tato procedura je určena k odebrání role pro daného uživatele

```
PROCEDURE RemoveRole
(
UserID in varchar2,
Workplace in varchar2,
Role in varchar2,
Result out varchar2
)
```

*Parametry:*

- *UserID – jedinečný identifikátor uživatele*
- *Workplace – pracoviště uživatele*
- *Role – role uživatele*
- *Result – výsledek procedury*

## 4.9 Návratové kódy

*USER_NOT_EXIST - Uživatelský účet neexistuje (UpdateUser, ChangePassword, LockUser, UnlockUser, DeleteUser)*

*USER_EXIST - Uživatelský účet již existuje (procedura CreateUser)*

*USER_IS_LOCKED - Uživatelský účet je již zamčen (procedura LockUser)*

*USER_IS_UNLOCKED - Uživatelský účet je již odemčen (procedura UnlockUser)*

*USER_PHONE_NULL - Není vyplněn telefonní kontakt (procedury CreateUser)*

*USER_PASSW_BAD - Neplatné uživatelské heslo, nelze nastavit nové heslo (procedury CreateUser, ChangePassword )*

*USER_LAST_NAME_NULL - Chybí příjmení uživatele (procedury CreateUser)*

*USER_FIRST_NAME_NULL - Chybí jméno uživatele (procedury CreateUser)*

*/* návratové kódy související s přiřazením rolí */*

*ROLE_NOT_EXIST - Dané přiřazení role neexistuje (procedura RemoveRole)*

*ROLE_EXIST - Dané přiřazení role již existuje (procedura AddRole)*

*ROLE_USER_NOT_EXIST - Uživatelský účet pro přiřazení role neexistuje (procedura AddRole)*

*ROLE_WORKPLACE_NOT_EXIST - Pracoviště pro přiřazení role neexistuje (procedura AddRole)*

*ROLE_RIGHTS_NOT_EXIST - Skupina práv (role) pro přiřezení neexistuje (procedura AddRole)*

*/* návratový kód pro ostatní případy */*

*OIM_UNKNOWN_ERROR - Ostatní chyby (všechny procedury při neznámé chybě)*

# 5. Reference

Následující tabulka obsahuje seznam dokumentů, které má VZP k dispozici, včetně krátkého popisu obsahu dokumentu.

| Název dokumentu | Popis |
|---|---|
| ADB_API.doc | Popis knihovny ADB |
| ADB_uzivatelska_prirucka.doc | Uživatelská příručka aplikace ADB |
| GMRAP_UzivatelskaPriruckaAdmin.doc | Uživatelská příručka administrátora RAP |
| GMRAP_UzivatelskaPrirucka.doc | Uživatelská příručka uživatele RAP |
| OIM_PL_SQL_API.docx | Popis rozhraní aplikace pro komunikaci s OIM 1) |

*Poznámky:*

1) *Popis rozhraní aplikace pro komunikaci s OIM je uveden v kapitole 4. tohoto dokumentu*

# Integrace aplikace s CSČ

## Příloha standardů a podmínek dodávek informačního systému VZP ČR

Verze: 1.06
Datum: 17.10.2017

## UPOZORNĚNÍ:

Tento dokument je zpracován Všeobecnou zdravotní pojišťovnou České republiky (dále též jen „VZP ČR“ nebo „VZP“). Všeobecná zdravotní pojišťovna České republiky jej uveřejňuje v rámci zadávací dokumentace jí zadávaných veřejných zakázek. Tento dokument umožňuje utvořit si představu o standardech informační architektury ICT VZP ČR. Účelem jeho uveřejnění je poskytnout informace nezbytné pro integraci dodávané komponenty se stávajícím informačním systémem v souladu se Standardy ICT- VZP- NIS.

Uveřejněním tohoto dokumentu není dotčena právní odpovědnost spojená s jeho zneužitím.

V tomto dokumentu bylo použito názvů subjektů a názvů produktů, které mohou být chráněny příslušnými právními předpisy.

**Otevřením tohoto dokumentu berete výše uvedené skutečnosti na vědomí.**

# Obsah

1. Úvod ..... 7
2. Struktura zprávy ..... 7
3. Popis jednotlivých služeb ..... 7
3.1 Služba „Poskytnutí seznamu verzí číselníku“ ..... 7
3.1.1 Parametry služby ..... 8
3.2 Služba „Poskytnutí verzí číselníku“ ..... 9
3.2.1 Parametry služby ..... 9
3.3 Služba „Nová verze číselníku“ ..... 11
3.3.1 Parametry služby ..... 11
3.4 Služba „Převzetí protokolu o zpracování číselníku“ ..... 13
3.4.1 Parametry služby ..... 13
3.5 Služba „Změna stavu paketu“ ..... 14
3.5.1 Parametry služby ..... 14
3.6 WSDL popis služeb ..... 15
4. Postup zařazení nových číselníků do CSC ..... 15

# Historie dokumentu

| Verze | Datum | Autor | Popis |
|---|---|---|---|
| 1.06 | 17.10.2017 | ÚICT VZP ČR | |

# 1. Úvod

Dokument obsahuje sadu standardů pro vybudování integračních vazeb nově dodávaných komponent informačního systému se stávajícími komponentami prostřednictvím integrační platformy v souladu se Standardy ICT VZP ČR. Vytvořené standardy jsou základem pro další rozšiřování systému zaváděním nových komponent a to jak „standardních“, tak i vytvářených dle specifických požadavků VZP ČR. Tento dokument je součástí výše uvedených Standardů ICT.

V případě specifikace rozšíření informačního systému zaváděním nových komponent ve smlouvě s dodavatelem, má specifikace uváděná v této smlouvě přednost před Standardy.

Obecně lze říci o službách CSČ, že používají pro svoji asynchronní komunikaci technologii Oracle Advanced Queuing. V této technologii probíhá komunikace prostřednictví front zpráv. V CSČ jsou založeny 2 základní fronty SC_IN_Q pro sběr vstupních požadavků a SC_EXTERNI_Q do níž se ukládají výsledky a dále jsou propagovány do IPF.

# 2. Struktura zprávy

Pro rozesílání i přijímání dat bude použit standardní formát zprávy **vzpipfzprava**. definovaný IPF viz příloha Integrační vazby IPF. CSČ generuje zprávu dle následujícího pravidla:

CORRID => request.CORRID nebo request.MSGID v závislosti na vyplnění request.CORRID ,

PUVODCE => request.PUVODCE,

ODESILATEL => 'CSC',

ODESILATELDOPLNEK => '9900',

PRIJEMCE => request.ODESILATEL,

PRIJEMCEDOPLNEK => request.ODESILATELDOPLNEK,

NAZEVSLUZBY => request.NAZEVSLUZBY,

NAZEVZPRAVY => v závislosti na službě,

VERZEZPRAVY => '1.0',

REFERENCE => request.REFERENCE,

PARAMETRD1 => systimestamp,

DATAC => xml data – závisí na službě, struktura xml odpovídá jednotlivým schématům.

# 3. Popis jednotlivých služeb

## 3.1 Služba „Poskytnutí seznamu verzí číselníku“

Cílem této služby je poskytnout externím aplikacím seznam všech verzí zvoleného číselníku. Tato služba bude probíhat ve dvou fázích

- IPF nebo externí aplikace uloží požadavek na seznam číselníku do vstupní zprávy CSČ SC_IN_Q. Tento požadavek bude obsahovat označení číselníku a období
- CSČ vygeneruje zprávu, která obsahuje seznam verzí číselníku, informace o stavu zpracování požadavku a propaguje se do IPF fronty GMCSC_Q. Jednotlivé verze budou obsahovat metadata a anotace.
- V případě, že daný číselník neexistuje, je vrácen chybový kód ve stavVyrizeniPozadavku.

### 3.1.1 Parametry služby

Název služby: Poskytnutí seznamu verzí číselníku

Označení služby: poskytniSeznamCiselniku

Typ služby: Asynchronní

Požadavek:

| | | |
|---|---|---|
| oznaceniCiselniku | string | 1 |
| - označení číselníku musí existovat v CSČ. Např. CISELPOB | | |
| obdobiOd | date | 1 |
| - datum ve formátu RRRR-MM-DD např. 2000-12-01 | | |
| obdobiDo | date | 1 |

Odpověď

| | | |
|---|---|---|
| Ciselnik | complex | 0-n |
| oznaceniCiselniku | string | 1 |
| - označení číselníku musí existovat v CSČ. Např. CISELPOB | | |
| verzeStruktury | string | 1 |
| verzeObsahu | string | 1 |
| platnostOd | date | 1 |
| expirace | date | 1 |
| popisStruktury | string | 1 |
| popisObsahu | string | 1 |
| interní | enum | 1 |
| „A - ano“ | | |
| „N - ne“ | | |
| externi | enum | 1 |
| A - ano“ | | |
| „N - ne“ | | |
| anotaceStruktury | base64 | 1 |
| - v této položce je uložen binární soubor | | |
| anotaceObsahu | base64 | 1 |
| - v této položce je uložen binární soubor | | |
| formatCiselniku | enum | 1 |
| default „CSV“ | | |

| | | |
|---|---|---|
| kodovaStranka | enum | 1 |
| default „EE8PC852“ | | |
| srovnavaciProtokol | base64 | 1 |
| - protokol je zazipovaný a zakódovaný base64 | | |
| sloupec | complex | 1-n |
| poradi | number | 1 |
| nazevSloupce | string | 1 |
| datovyTyp | string | 1 |
| Externi | enum | 1 |
| „A – sloupec bude součástí externí a interní formy číselníku“ | | |
| „N – sloupec bude součástí pouze interní formy číselníku“ | | |
| „E - sloupec bude součástí pouze externí formy číselníku“ | | |
| popisSloupce | string | 1 |
| stavVyrizeniPozadavku viz. výše 1 | | |

## 3.2 Služba „Poskytnutí verzí číselníku“

Cílem této služby je poskytnout externím aplikacím vybrané číselníky včetně metadat, anotací a dat. Tato služba bude probíhat ve dvou fázích

- IPF nebo externí aplikace uloží požadavek na číselníky do vstupní zprávy CSČ SC_IN_Q. Tento požadavek bude obsahovat označení číselníku, seznam verzí číselníku a formu číselníku (interní nebo externí)
- CSČ vygeneruje zprávu, která obsahuje verze číselníků, informace o stavu zpracování požadavku a propaguje se do IPF fronty GMCSC_Q. Jednotlivé verze budou obsahovat metadata a anotace a data.
- V případě, že daný číselník neexistuje, je vrácen chybový kód ve StavVyrizeniPozadavku.

### 3.2.1 Parametry služby

Název služby: Poskytnutí verzí číselníku

Označení služby: poskytniVerzeCiselniku

Typ služby: Asynchronní

Požadavek:

| | | |
|---|---|---|
| oznaceníCiselniku | string | 1 |
| interni | enum | 1 |
| „A“ – požaduje interní formát číselníku | | |
| „N“ – požaduje externí formát | | |
| verzeObsahu | string | 1-n |

Odpověď

ciselnik complex 0-n

| | | |
|---|---|---|
| oznaceniCiselniku | string | 1 |
| verzeStruktury | string | 1 |
| verzeObsahu | string | 1 |
| platnostOd | date | 1 |
| expirace | date | 1 |
| popisStruktury | string | 1 |
| popisObsahu | string | 1 |
| interní | enum | 1 |
| „A“ - ano | | |
| „N“ - ne | | |
| externi | enum | 1 |
| „A“ - ano | | |
| „N“ - ne | | |
| anotaceStruktury | base64 | 1 |
| anotaceObsahu | base64 | 1 |
| formatCiselniku | enum | 1 |
| „CSV“ | | |
| „XML“ | | |
| default „csv“ | | |
| kodovaStranka | enum | 1 |
| „EE8PC852“ – dos PC852 | | |
| „EE8ISO8859P2“ - iso | | |
| „EE8MSWIN1250“ – ansi 1250 | | |
| default „EE8PC852“ | | |
| data | base64 | 1 |
| - Obsah číselníku je zazipovaný a zakódovaný base64 | | |
| srovnavaciProtokol | base64 | 1 |
| sloupec complex 1-n | | |
| poradi | number | 1 |
| nazevSloupce | string | 1 |
| datovyTyp | string | 1 |

| | | |
|---|---|---|
| externi | enum | 1 |
| „A – sloupec bude součástí externí a interní formy číselníku“ | | |
| „N – sloupec bude součástí pouze interní formy číselníku“ | | |
| „E - sloupec bude součástí pouze externí formy číselníku“ | | |
| popisSloupce | string | 1 |
| stavVyrizeniPozadavku | enum | 1 |

## 3.3 Služba „Nová verze číselníku“

Cílem této služby CSČ je převzít novou verzi obsahu číselníku, která vznikla v jiném aplikačním modulu VZP. Importovaný číselník se nastaví do stavu „Typováno“.

V případě, že je administrátorem číselníků v CSČ nastaveno automatické schvalování a distribuce, nastaví se číselník do stavu schváleno a provede se vygenerování všech paketů, ve kterých je tento číselník uveden samostatně. U číselníků s tímto režimem nebude povoleno v CSČ editovat jednotlivé záznamy.

Převzetí číselníku bude probíhat následovně:

- IPF uloží požadavek na převzetí číselníku do vstupní fronty CSČ SC_IN_Q. Tento požadavek bude obsahovat metadata číselníku a obsah číselníku.
- CSČ překontroluje metadata číselníku(musí souhlasit struktura) a data číselníku dekóduje a uloží do CSČ. Do poznámky verze obsahu zapíše informaci, že byl číselník pořízen z AQ.
- V případě, že je povoleno automatické schvalování číselníku a distribuce, nastaví stav na „schváleno“ a provede distribuci paketu
- CSČ vygeneruje odpověď, která obsahuje informace o stavu zpracování požadavku a propaguje se do IPF fronty GMCSC_Q. O případných chybách, které vzniknou při následné kontrole či distribuci číselníku, bude notifikován garant číselníku.

### 3.3.1 Parametry služby

Název služby: Nová verze číselníku

Označení služby: **NovaVerzeCiselniku**

Označení zprávy: **prevezmiVerziCiselniku**

Typ služby: Asynchronní

Požadavek:

ciselnik complex 1-n

oznaceniCiselniku varchar(40) 1

- Označení číselníku musí existovat v CSČ.

popisObsahu varchar(40) 1

verzeStruktury varchar(20) 1

- Pro oddělení desetinných míst je použita tečka. Verze struktury musí existovat v CSČ.

platnostOd date 1

platnostDo date 1

formatCiselniku enum 1

„csv“

„xml“

default „csv“

- V současné době je podporován pouze **csv** formát.

kodovaStranka enum 1

„EE8PC852“

„EE8ISO8859P2“

„EE8MSWIN1250“

default „EE8PC852“

- V současné době je podporována pouze **EE8PC852**

data blob 1

- Data (csv) jsou zazipována a zakódována base64. CSV data jsou v kódové stránce EE8PC852, jako oddělovač je použita čárka, jednotlivé řádky jsou odděleny CRLF, pořadí sloupců csv musí odpovídat pořadí sloupců ve struktuře CSČ, textové sloupce jsou v uvozovkách, datum je ve formátu DDMMRRRR;

anotaceObsahu blob 0-1

- Zip soubor, který je zakódovaný base64

anotaceSoubor varchar(50) 0-1

- Označení souboru, který je v položce anotaceObsahu. Např. anotace.zip

Odpověď

| | | |
|---|---|---|
| ciselnik | complex | 1-n |
| oznaceniCiselniku | varchar(40) | 1 |
| verzeObsahu | varchar(20) | 1 |
| stavVyrizeniPozadavku | complex | 1 |
| kod | enum | 1 |

„0“

„1“

„-1“

„-2“

| | | |
|---|---|---|
| popis | varchar(32000) | 1 |

## 3.4 Služba „Převzetí protokolu o zpracování číselníku“

Cílem této služby je uložit protokol o zpracování číselníků na „místě aktualizace“ do databáze CSČ. Místem aktualizace se rozumí jakákoliv aplikace na pobočce nebo v centru VZP. V CSČ existuje číselník těchto míst. Tato služba probíhá následovně:

- IPF uloží požadavek do vstupní zprávy CSČ SC_IN_Q. Tento požadavek bude obsahovat protokol, místo aktualizace, datum aktualizace, identifikaci paketu, se kterým číselník dorazil na místo aktualizace
- CSČ uloží protokol a vygeneruje odpověď, která se propaguje se do IPF fronty GMCSC_Q.
- V případě, že dojde při zpracování požadavku k chybě, je vrácen chybový kód ve StavVyrizeniPozadavku a Popis chyby.

### 3.4.1 Parametry služby

Název služby: Převzetí zprávy o zpracování číselníku

Označení služby: **ProtokolZpracCiselniku**

Označení zprávy: **prevezmiProtokol**

Typ služby: Asynchronní

Požadavek:

| | | |
|---|---|---|
| nazevProtokolu | varchar(255) | 1 |
| typProtokolu | enum | 1 |

„S“ - protokol o stavu číselníků po aktualizaci

„O“ – Jakýkoliv jiný protokol

| | | |
|---|---|---|
| protokol | base64 | 1 |

- V případě typu protokolu = „S“ se jedná o zazipovaný a zakódovaný (base64) xml protokol o zpracování. Schéma tohoto protokolu je uvedeno v přílohách (**ciselnik.xsd – stavAktualizace**).
- V případě typu protokolu = „O“ se jedná o zazipovaný a zakódovaný plane text.

| | | |
|---|---|---|
| datumVzniku | date | 1 |
| mistoVzniku | varchar(20) | 1 |

- hodnota musí být z číselníku míst aktualizací. Např. číslo pobočky.

| | | |
|---|---|---|
| identifikace | varchar(50) | 1 |

- V případě typu protokolu = „S“ se zde uvádí identifikace paketu, kterým se číselníky aktualizovaly jinak není povinný.

Odpověď

| | | |
|---|---|---|
| StavVyrizeniPozadavku | complex | 1 |

Kod enum 1

„0“

„1“

„-1“

„-2“

Popis varchar(32000) 1

## 3.5 Služba „Změna stavu paketu“

Cílem této služby je změnit stav paketu. Tato služba bude probíhat následovně:

- IPF uloží požadavek do vstupní zprávy CSČ SC_IN_Q. Tento požadavek bude obsahovat označení paketu a nový stav
- CSČ provede změnu stavu paketu a případě vzniku produkčního paketu provede distribuci

V případě, že dojde při zpracování požadavku k chybě, je vrácen chybový kód ve StavVyrizeniPozadavku a Popis chyby.

### 3.5.1 Parametry služby

Název služby: Změna stavu paketu

Označení služby: **ZmenaStavuPaketu**

Označení zprávy: **zmenStavPaketu**

Typ služby: Asynchronní

Požadavek:

oznaceniPaketu varchar(20) 1

- Označení paketu musí být ze seznamu typu paketu v CSČ

novyStav enum 1

„T“ – testovací paket. Tento stav vznikne automaticky při vygenerování testovacího paketu.

„TZ“ – zamčený testovací paket.

„P“ – produkční paket.

Odpověď

stavVyrizeniPozadavku complex 1

kod enum 1

„0“

„1“

„-1“

„-2“

popis varchar(32000) 1

Pro změnu stavu paketu platí jistá omezující pravidla. Například nemůžete zamykat paket, který je již uzamčený. V následující tabulce je přehled všech povolených kombinací

| Nový stav | Původní stav |
|---|---|
| Testovací – odemknutý | Testovací - zamknutý |
| Testovací – zamknutý | Testovací - odemknutý |
| Produkční | Testovací (nezávisí na zamknutí) |

## 3.6 WSDL popis služeb

Odpovídající WSDL popisy výše popsaných služeb jsou uvedeny v aplikaci Evidence služeb, do které má dodavatel přístup od podpisu smlouvy na dodávku komponent IS VZP ČR.

# 4. Postup zařazení nových číselníků do CSC

Nový číselník je zařazen na základě žádosti uživatele v aplikaci Centrální správa číselníků. Žádost poté probíhá workflow ve VZP ČR s následujícími kroky:

1) Typování žádosti
2) Schvalování žádosti
3) Vyřízení žádosti
4) Prohlížení žádosti

Postup pro vytvoření číselníku je v souladu s Uživatelskou příručkou Centrální správy číselníků následující :

1) Administrátor musí založit číselník
    a. Nastavit
        i. garanta struktury
        ii. operátora/y struktury
        iii. garanta obsahu
        iv. operátora/y obsahu
        v. notifikace
    b. přiřadí číselník do distribučních paketů, nebo vytvoří zcela nový paket pro distribuci
        i. nastaví způsob distribuce paketu
            1. AQ
            2. Pomocí souborů (File systém)
2) operátor struktury
    a. založí novou strukturu číselníku a dá ke schválení garantovi struktury
3) garant struktury
    a. musí strukturu schválit, odmítnout
4) operátor obsahu
    a. naplní obsah číselníku a předá ke schválení na garanta obsahu
5) garant obsahu
    a. schválí/odmítne obsah k distribuci
6) administrátor
    a. provede distribuci – odeslání paketu s novým obsahem číselníku

# Popis integračních vazeb prostřednictvím IPF a metodika realizace integračních vazeb

## Příloha standardů a podmínek dodávek informačního systému VZP ČR

Verze: 1.06
Datum: 17.10.2017

## UPOZORNĚNÍ:

Tento dokument je zpracován Všeobecnou zdravotní pojišťovnou České republiky (dále též jen „VZP ČR“ nebo „VZP“). Všeobecná zdravotní pojišťovna České republiky jej uveřejňuje v rámci zadávací dokumentace jí zadávaných veřejných zakázek. Tento dokument umožňuje utvořit si představu o standardech informační architektury ICT VZP ČR. Účelem jeho uveřejnění je poskytnout informace nezbytné pro integraci dodávané komponenty se stávajícím informačním systémem v souladu se Standardy ICT- VZP- NIS.

Uveřejněním tohoto dokumentu není dotčena právní odpovědnost spojená s jeho zneužitím.

V tomto dokumentu bylo použito názvů subjektů a názvů produktů, které mohou být chráněny příslušnými právními předpisy.

**Otevřením tohoto dokumentu berete výše uvedené skutečnosti na vědomí.**

.

# Obsah

1. Úvod ... 9
2. Popis integračních vazeb prostřednictvím IPF ... 9
2.1 Webové služby, IPF procesy ... 9
2.1.1 Pojmenování ... 9
2.1.2 Styly ... 9
2.1.3 Standardy ... 10
2.1.4 SOAP protokol a webové služby ... 10
2.1.5 WSDL ... 10
2.1.6 Význam elementů WSDL ... 10
2.1.7 Podporované WS standardy ... 12
2.2 Definice XSD schémat ... 13
2.3 Standardní datové XML elementy ... 13
2.4 Synchronní požadavky ... 14
2.5 Práce s frontou požadavků ... 14
2.5.1 PojmenováníJmenné konvence názvů front ... 14
2.5.1.1 Názvy front aplikací (v aplikacích) ... 15
2.5.1.2 Názvy front na IPF ... 15
2.5.2 Odlišení prostředí ... 16
2.5.3 Jednotná zpráva pro AQ ... 16
2.6 Pravidla pro stavbu zprávy VZPIPFZPRAVA ... 18
2.7 Posílání zpráv ... 18
2.7.1 Směrovací aparát ... 18
2.8 Dokumentace webových služeb ... 20
2.9 Další vlastnosti dodržované v souvislosti s IPF procesy ... 20
2.9.1 Předepsané vlastnosti procesů ... 20
2.9.2 Vlastnosti aplikací komunikujících s IPF ... 20
2.9.3 Instalace procesů do testovacího prostředí IPF ... 20
2.9.4 Instalace do produkčního prostředí IPF ... 21
2.10 IPF partitions ... 21
2.10.1 Jmenné konvence pro BPEL partitions ... 21
2.10.2 Konvence pro umístění služeb do partitions ... 21
2.10.3 ESB jmenné konvence ... 22
3. Metodika realizace integračních vazeb ... 22
3.1 Účel metodiky ... 22

3.2 Návrh architektury integrace aplikační komponenty ..... 22
3.3 Popis integračních vazeb v analytickém projektu ..... 22
3.4 Testovací scénáře integračních vazeb ..... 23
3.5 Zavedení integračních služeb do aplikace Evidence služeb ..... 23
3.6 Popis integračních vazeb v administrátorské dokumentaci ..... 23
3.7 Workshop k objasnění realizovaných integračních vazeb ..... 23
3.8 Realizace změn integračních vazeb ..... 23

# Seznam obrázků

Obrázek 1- jmenné konvence front vzhledem ke směrovacímu aparátu ..... 16

# Historie dokumentu

| Verze | Datum | Autor | Popis |
|---|---|---|---|
| 1.06 | 17.10.2017 | ÚICT VZP ČR | |

# 1. Úvod

Dokument obsahuje sadu standardů pro vybudování integračních vazeb nově dodávaných komponent informačního systému se stávajícími komponentami prostřednictvím integrační platformy v souladu se Standardy ICT VZP ČR. Vytvořené standardy jsou základem pro další rozšiřování systému zaváděním nových komponent a to jak „standardních“, tak i vytvářených dle specifických požadavků VZP ČR. Tento dokument je součástí výše uvedených Standardů ICT.

V případě specifikace rozšíření informačního systému zaváděním nových komponent ve smlouvě s dodavatelem, má specifikace uváděná v této smlouvě přednost před Standardy.

Cílem tohoto dokumentu je popis služeb a procesů vytvářených při realizaci integračních vazeb mezi komponentami informačního systému VZP ČR prostřednictvím integrační platformy a definování metodiky realizace integračních vazeb.

# 2. Popis integračních vazeb prostřednictvím IPF

## 2.1 Webové služby, IPF procesy

### 2.1.1 Pojmenování

Webové služby i služby obecně by měly zapadat do této jmenné konvence:

**Název služby:** ssssAaaaaaBbbbbbCccccc

ssss - sloveso, rozkazovací způsob, malá písmena (včetně počátečního písmene!), bez diakritiky, vyjadřuje podstatu služby, přičemž za obdobné aktivity se používá stejné označení podle následující tabulky:

AaaaaaBbbbbbCccccc - další slova, první písmeno velké, bez diakritiky, převážně podstatná jména v jednotném čísle v prvním pádě, přídavná jména,...

**Datové položky:** AaaaaaBbbbbbCccccc

AaaaaaBbbbbbCccccc - několik slov, první písmeno velké, bez diakritiky, převážně podstatná jména v jednotném čísle v prvním pádě, přídavná jména,…

Pokud položka názvu nebo datová položka obsahuje zkratky, pak jsou všechny znaky velké.

např. dejNazevZZP

### 2.1.2 Styly

**RPC style**

Pro svoji jednoduchost je RPC styl blízký všem, kdo začínají pracovat s webovými službami. RPC styl byl od prvních verzí SOAPu podporován v Java nástrojích. V systémech VZP ČR bude RPC styl podporován jen ve velmi odůvodnitelných případech. V ostatních bude použit Document style.

**Document style**

Dokument styl je druhý ze stylů podporovaných v protokolu SOAP ve webových službách. Oproti RPC stylu, je v SOAP zprávě zaslán celý XML dokument nikoliv „pouze“ parametry volané funkce nebo procedury a samozřejmě toto volání není vázáno na konkrétní funkci nebo proceduru. XML fragment může být samozřejmě popsán ve WSDL. Návratovou hodnotou z volané služby je také XML fragment.

**Dokument styl je preferovanou variantou webových služeb. RPC styl používáme jen tam, kde se ukáže obhajitelně opodstatněný.**

### 2.1.3 Standardy

### 2.1.4 SOAP protokol a webové služby

SOAP protokol pro komunikaci webových služeb (WS) je nadstavbou HTTP protokolu. Fyzicky je to standardem definovaná část XML dokumentu – obálka, do které se vloží vlastní data, a vše se pak posílá protokolem HTTP. Standard pro SOAP definuje také další hlavičky HTTP.

Komunikace pomocí SOAP webovými službami je definovaná pomocí WSDL (Web Service Definition Language) a struktura vlastních dat požadavku a odpovědi pomocí XSD (XML schema definition).

### 2.1.5 WSDL

WSDL definuje způsob komunikace mezi službami, tj. názvy a definice posílaných zpráv, pojmenování operací, styly, název služby, u nasazené služby pak také její endpoint. Dále obsahuje definice dalších rozšíření, jako WS-Addressing, WS-Security, WS-Reliability apod.

Pro další popis je nutné vysvětlit, co znamená „namespace“ (volně také jmenný prostor). Je to definice prostředí, která označuje logickou skupinu unikátních identifikátorů (např. deklarací elementů, atributů apod. v XML). Identifikátor definovaný v namespace je s ním pak pevně asociován. Lze tak nezávisle definovat stejný identifikátor v rámci několika rozdílných namespace. Namespace může mít teoreticky jakékoliv unikátní označení, v XML se obvykle používá notace urn:JmenoNamespace nebo ještě častěji název obdobný URL - http://LibovolnaDomenaAutora/rozlisujiciOznaceni/verze. Volba namespace musí být unikátní, proto se používá uvedená notace, kde doménou je doména autora/dodavatele služby. V naprosté většině je to xmlns následované tečkou a doménou druhého řádu dodavatele. Za lomítkem následuje další dělení, které je již v kompetenci dodavatele a jeho interních standardů. Definice namespace se v rámci XSD definicí udává atributem **targetNamespace**.

Namespace lze definovat také explicitním uvedením xmlns atributu u každého elementu. Tento způsob definice namespace však není preferovanou variantou.

### 2.1.6 Význam elementů WSDL

**<definitions>** - tento element je kořenový element dokumentu WSDL. Obsahuje deklaraci WSDL namespace jakožto základního namespace pro dokument, takže všechny elementy patří do tohoto namespace neobsahují-li jinou deklaraci namespace. Základní namespace je definován atributem targetNamespace elementu. Atribut name je společný názvu webové služby.

**<types>** - vnitřní element <definitions>. Obsahuje definici dále používaných typů (dat obvykle obsažených v požadavku nebo odpovědi). Lze definovat několik schémat.

**<schema>** - vnitřní element <types>. Obsahuje konkrétní definici typů nebo odkaz na ně. Element obsahuje platné XSD schéma nebo odkaz na něj do souboru pomocí dalšího elementu <import>.

**<message>** - vnitřní element <definitions>. Pro popis struktury zpráv se používá element <message>, který obsahuje nula nebo více elementů <part>. Element <part> odpovídá parametru nebo návratové hodnotě vzdálené procedury.

**<operation>** - vnitřní element <portType>. Operace slouží pro přiřazení páru požadavek-odpověď k volání metody. Operace se definuje elementem <operation>, který specifikuje, která zpráva je vstupem a která výstupem pomocí podřízených elementů <input> a <output>.

**<portType>** - vnitřní element <definitions>. Kolekce všech operací (t.j. i metod) se nazývá portType. Element <operation> je tedy prvkem elementu <portType>

Parametry typicky definované aplikačním serverem

**<binding>** - vnitřní element <definitions>. Element se používá pro převod z abstraktních datových typů, zpráv a operací do konkrétní fyzické reprezentace zpráv. Definuje konkrétní aspekty operací.

Názvem binding může být cokoliv. Ovšem tento název musí být obsažen v atributu binding elementu <port> (viz definice služby výše).

**<soap:binding>** - vnitřní element <binding>. Uvnitř elementu <binding> může být SOAP extension element <soap:binding>, který specifikuje použitý přenosový protokol (SOAP může používat HTTP, SMTP nebo jiný protokol) a styl požadavku (např. rpc nebo dokument). Ve VZP se v naprosté většině používá **styl dokument** resp. document.

Další podřízené elementy:

Pro každou operaci, kterou služba exponuje, je třeba specifikovat hodnotu SOAPAction HTTP hlavičky. SOAPAction je HTTP hlavička, kterou klient posílá, když vyvolává službu. Server SOAP může tuto hlavičku použít pro stanovení služby nebo jí využít jiným způsobem. SOAPAction se specifikuje následujícím způsobem:

```
    <binding name='WeatherSoapBinding' type='wsdlns:WeatherSoapPort'>
  <soap:binding style='document' transport='http://schemas.xmlsoap.org/soap/http'/>
    <operation name='GetTemperature'>
      <soap:operation soap:Action='http://tempuri.org/action/Weather.GetTemperature'/>
  ...
    </operation>
</binding>
```

V zásadě se přidává element <operation> se stejným jménem, jako operace definovaná dříve. Dovnitř elementu <operation> se vkládá element <soap:operation> s atributem soapAction. Nakonec musí být specifikováno, jako jsou kódovány vstupní a výstupní zprávy této operace.

Uvnitř elementu <operation> jsou elementy <input> a <output>, které obsahují element <soap:body>. Ten specifikuje způsob kódování dat. URI http://schemas.xmlsoap.org/soap/encoding/ určuje styl kódování, který je popsaný ve specifikaci SOAP 1.1.

**<service>** - vnitřní element <definitions>. Každá služba je popsána prostřednictvím elementu <service>. Uvnitř elementu <service> jsou specifikovány porty, na kterých je tato služba přístupná. Port specifikuje adresu služby např.: " http://localhost/demos/wsdl/devxpert/weatherservice". Definice portu může vypadat například takto:

```
    <port name ='WeatherSoapPort' binding='wsdlns:WeatherSoapBinding'>
  <soap:address location='http://localhost/demos/wsdl/devxpert/weatherservice.asp' />
</port>
```

Každý port má unikátní jméno a atribut binding. O atributu binding viz výše. V případě používání SOAP obsahuje element port element <soap:address/> s aktuální adresou služby - URL.

**<plnk:partnerLinkType>** - vnitřní element <definitions>. Element partnerLinkType je specifický pro integrační platformu a definuje „partner link“ v rámci BPEL procesů – viz BPEL standard.

Příklad:

```
<definitions name="NotifikujPrijem"
targetNamespace="http://wsdl.gemsystem.cz/NotifikujPrijem"
        xmlns="http://schemas.xmlsoap.org/wsdl/"
        xmlns:ns4="http://xmlns.oracle.com/pcbpel/adapter/aq/outbound/"
        xmlns:ns0="http://xmlns.gemsystem.cz/NotifikujPrijem"
        xmlns:plnk="http://schemas.xmlsoap.org/ws/2003/05/partner-link/"
        xmlns:ns3="http://wsdl.gemsystem.cz/PoskytniSoubor"
        xmlns:ns2="http://xmlns.gemsystem.cz/RZPTypes"
        xmlns:client="http://wsdl.gemsystem.cz/NotifikujPrijem">
       <types>
           <schema xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:ns0="http://xmlns.gemsystem.cz/NotifikujPrijem"
                xmlns:plnk="http://schemas.xmlsoap.org/ws/2003/05/partner-link/"
                xmlns:client="http://wsdl.gemsystem.cz/NotifikujPrijem"
xmlns:ns2="http://xmlns.gemsystem.cz/RZPType"
                xmlns:ns3="http://wsdl.gemsystem.cz/PoskytniSoubor">
               <import namespace="http://xmlns.gemsystem.cz/RZPTypes"
schemaLocation="RZPTypes.xsd"/>
               <import namespace="http://xmlns.gemsystem.cz/NotifikujPrijem"
schemaLocation="NotifikujPrijem.xsd"/>
       <import namespace="http://wsdl.gemsystem.cz/PoskytniSoubor"
location="PoskytniSouborSOAP.wsdl"/>
           </schema>
       </types>
       <message name="NotifikujPrijemResponseMessage">
           <part name="payload" element="ns0:NotifikujPrijemResponse"/>
       </message>
       <message name="NotifikujPrijemRequestMessage">
           <part name="payload" element="ns0:NotifikujPrijem"/>
       </message>
       <portType name="NotifikujPrijem">
           <operation name="process">
               <input message="client:NotifikujPrijemRequestMessage"/>
               <output message="client:NotifikujPrijemResponseMessage"/>
           </operation>
       </portType>
       <plnk:partnerLinkType name="NotifikujPrijem">
           <plnk:role name="NotifikujPrijemProvider">
               <plnk:portType name="client:NotifikujPrijem"/>
           </plnk:role>
       </plnk:partnerLinkType>
   </definitions>
```

### 2.1.7 Podporované WS standardy

Podporovány jsou tyto standardy:

- WS-Security
- WS-Adressing
- WS-Corelation
- WS-Eventing
- WS-Policy
- WS-Reliability

## 2.2 Definice XSD schémat

XSD definice jsou nedílnou součástí definice celé služby uvedené ve WSDL. Tak, jako WSDL definuje samotnou službu a způsob její komunikace, tak XSD definuje data přenášená touto službou. VZP standard nedefinuje, zda musí být definice dat uvedená v rámci WSDL souboru nebo jako samostatný soubor, který se do WSDL pomocí příslušných definujících elementů importuje.

XSD a **všechny** datové položky jím definované však **musí být zahrnuty** do příslušného namespace udaném v atributu „**targetNamespace**“ (viz 2.1.3 Standardy

SOAP protokol a webové služby).

Používá-li se atribut targetNamespace, kterým se definuje výchozí namespace, je dále povinné použít atribut elementFormDefault=“qualified“. Tím se definuje, že všechny elementy (i ty definované v potomcích rodičovských elementů (komplexní typy) budou kvalifikované, tj. budou přiřazeny do výchozího definovaného namespace. Bez atributu elementFormDefault nastaveným na qualified vzniknou v definic XML elementy, které mají anonymní namespace, což je ve VZP nepřípustné.

Je doporučeno při vystavování webových služeb aplikací prostřednictvím IPF nepublikovat datové elementy služby aplikace ve službě IPF, ale vytvořit si vlastní rozhraní (i když se bude třeba lišit jenom hodnotou namespace) a data do nového rozhraní transformovat. Předejde se tak problémům s případnými úpravami rozhraní IPF v budoucnu.

XSD definice je vhodné definovat alespoň v rámci jedné služby na jednom místě.

## 2.3 Standardní datové XML elementy

Elementy zpráv jsou definovány s malým počátečním písmenem. Následující slova v názvu elementu jsou psána s velkým písmenem (velbloudí nebo také camel písmo).

V komunikaci webových služeb byly ve VZP prozatím stanoveny tyto standardní elementy zpráv:

Elementy v **požadavku i odpovědi** zprávy:

**<konzument>**, typ string - element obsahuje název komponenty IS VZP ČR, která reprezentuje vstupní bod pro vyřizování obchodních případů daného typu. Název je jediný pro danou komponentu bez ohledu na počet typů obchodních případů iniciovaných z dané komponenty. Název komponenty by měl být výstižný, stručný a bez použití diakritiky. Např. Portál VZP ČR používá hodnotu “Portal”.

**<referenceKonzumenta>**, typ string - element obsahuje unikátní identifikaci volání služby na straně konzumenta Jednoznačně identifikuje případ založený danou komponentou. V případě Portálu VZP ČR je používáno ID volání.

V případě komunikace přes AQ jsou **navíc** tyto údaje obsaženy v metadatových atributech objektu VZPIPFZPRAVA:

- atribut PUVODCE obsahuje hodnotu elementu konzument
- atribut REFERENCE obsahuje hodnotu elementu referenceKonzument

Elementy v odpovědi zprávy:

**<stavVyrizeniPozadavku>** , typ Complex

**<kod>**, typ integer

**<popis>**, typ string

Element obsahuje každá odpověď webové služby. V podřízených parametrech služby bez ohledu na typ, technologii použitou pro komunikaci s konzumentem, či technologii použitou pro implementaci poskytující komponenty. se uvádí stav vyřízení požadavku služby, kde „kod“ je číselný údaj číselníku:

-2 – chybná vstupní data

-1 – služba není funkční

0 – služba nevrátila žádný záznam nebo na základě požadavku nebyla provedená žádná akce

1 – výstup služby je v pořádku nebo služba vrátila právě jeden záznam.

9 – služba vrátila oproti očekávání více záznamů

Element popis může uvádět slovní interpretaci vyřízení požadavku nebo popis chybového stavu. Není však nutně povinný jej vyplňovat vždy , nemusí být uveden, pokud kod=1.

Dalším elementem, který je nutné respektovat jako standard **v rámci jakéhokoliv datového XML přenosu** je:

**<dokument>**, typ Complex

**<nazev>**, typ string

**<mime>**, typ string

**<obsah>**, typ base64String

Element dokument má pevně definovanou strukturu, kde „nazev“ je název dokumentu, „mime“ je mime typ dokumentu (viz HTTP MIME typy) a element „obsah“ obsahuje vlastní dokument v kódování Base64.

## 2.4 Synchronní požadavky

Komunikace synchronním způsobem webovými službami není preferovaným standardem. V některých případech je použití synchronní komunikace nevyhnutelné nebo velmi výhodné (k použití synchronní komunikace **musí být vždy oprávněný důvod**). Při rozhodování, zda a kterou komunikaci použít, je nutné respektovat základní pravidla. Při výběru se rozhodujeme podle níže uvedených parametrů komunikace:

- synchronní komunikace – odpověď vrácena v rámci aktuálně navázané relace na úrovni TCPP/IP. Komunikace proběhne do cca 60 vteřin, malé zprávy.
- asynchronní komunikace – odpověď vrací volaný systém aktivním navázáním komunikace (nová relace TCP/IP) se systémem volajícím (callback). Komunikace probíhá cca déle jak 60 vteřin a/nebo jde o přenos velkých zpráv (~ jednotky MB a více).

## 2.5 Práce s frontou požadavků

Většina asynchronních požadavků a odpovědí bude realizována prostřednictvím JMS nebo AQ. Pokud se nejedná o existující systém bez možnosti konfigurace je vhodné, aby byly použity standardizované jmenné konvence a obsah zpráv.

Aplikace může mít libovolný počet front. Doporučujeme však minimalizovat jejich počet a typ služby odlišovat v těle zprávy.

### 2.5.1 PojmenováníJmenné konvence názvů front

Název fronty: [PREFIX]JMENO_Q

Například PBVYDAJ_Q

Název Queue Table: JmenoFronty_T

Například PBVYDAJ_T

#### 2.5.1.1 Názvy front aplikací (v aplikacích)

Názvy front AQ podléhají jmenným konvencím aplikace. Název fronty, kterou aplikace přijímá zprávy od IPF (to jest Fronty v aplikaci) má maximální **povolenou délku 10 znaků** (delší řetězec zapříčiní nefunkčnost směrovacího aparátu).

#### 2.5.1.2 Názvy front na IPF

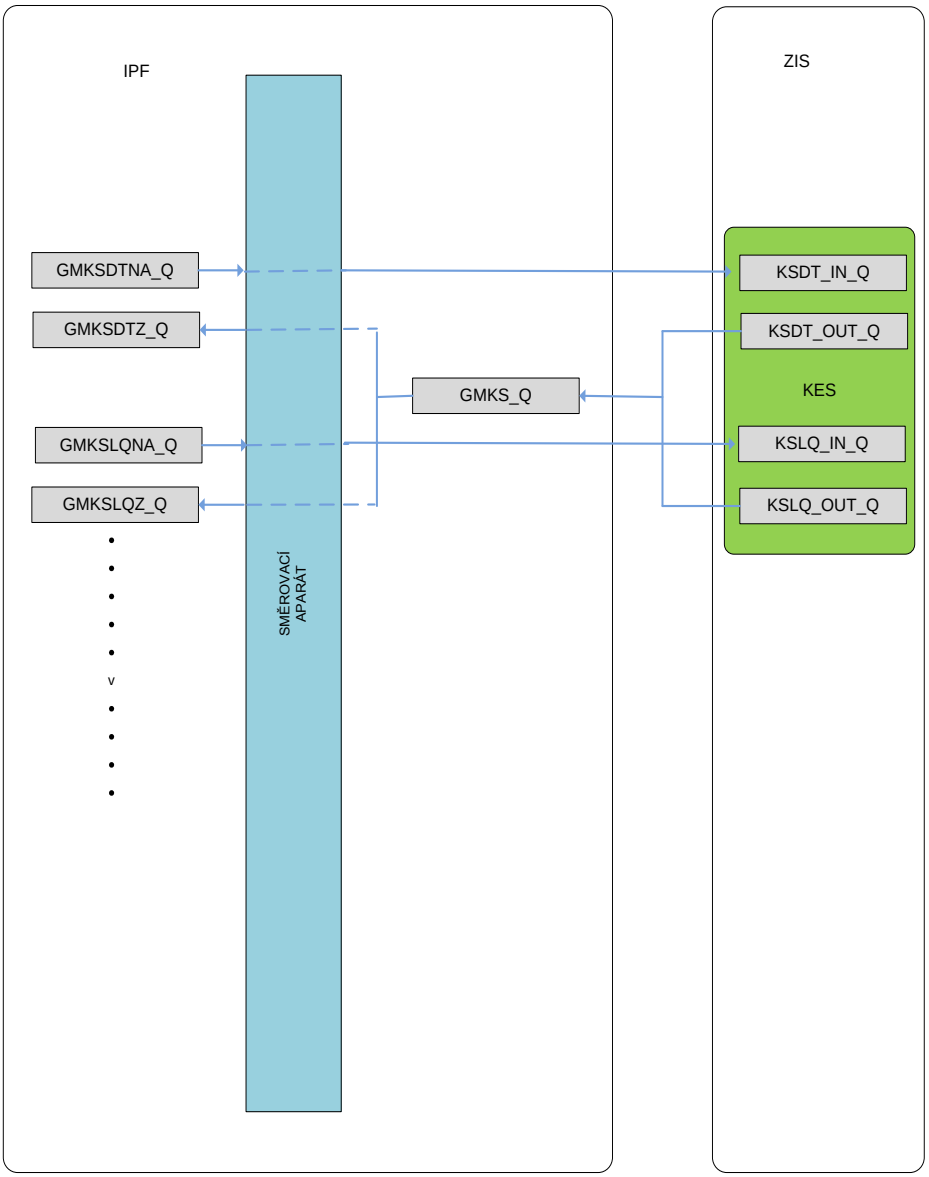
Názvy front, nad kterými je postaven kombinovaný AQ adapter, má tvar WWXXXYYYYYZZ_Q. **Maximální délka 30 znaků**.

- Část WW je tvořena prefixem dodavatele (např. GM pro GEM System International s.r.o., PB pro PIKE ELECTRONICS s.r.o., Brno).
- Část XXX je název aplikace, ze které přicházejí zprávy. Délka 3 znaky (např. KES pro aplikaci KES v ZIS).
- Část YYYYY slouží pro rozlišení front komunikující se stejnou aplikací. Je možné vynechat, pokud s danou aplikací nekomunikuje více služeb. Tato možnost není doporučena z důvodu budoucího rozšíření komunikace aplikace s dalšími službami. Délka 0 – 5 znaků.
- Část ZZ tvoří buď výraz NA, pokud se jedná o AQ frontu určenou pro zprávy posílané ven z IPF nebo výraz Z pro AQ frontu určenou pro zprávy posílané do IPF.

Název fronty, do které jsou propagovány všechny zprávy z dané aplikace umístěné v ZISu, má tvar WWXXX_Q.

- Část WW je tvořena prefixem dodavatele.
- Část XXX je název aplikace, ze které přicházejí zprávy. Délka 3 znaky (např. KES pro aplikaci KES v ZIS).

Všechny zde uvedené počty znaků jsou doporučené hodnoty.




*Obrázek 1- jmenné konvence front vzhledem ke směrovacímu aparátu*

### 2.5.2 Odlišení prostředí

Tělo zprávy obsahuje atribut, který umožňuje odlišit prostředí, z kterého zpráva vznikla a pro které je určena. Tento atribut se ve standardní zprávě nazývá „Prostředí“. Může nabývat hodnot „PROD“, „DEV“ nebo „TEST“. Každá instance komponenty musí být konfigurovatelná podle toho o jaké prostředí se jedná. Zprávy, které by do tohoto prostředí neměly přicházet, musí být logovány a jejich zpracování ignorováno.

### 2.5.3 Jednotná zpráva pro AQ

```
CREATE TYPE VZPIPFZPRAVA IS OBJECT (
 -- $Id: VZPIPFZPRAVA.sql,v 1.2 2006/09/29 07:37:17 sherry Exp $
        -- ID zpravy pridane nekterym z odesilatelu (neni to ID zpravy ve fronte AQ)
 MsgID RAW(16),
 -- Korelacni ID:
```

```
        -- pokud odpovidam na zpravu, ktera mela vyplneny atribut CorrID, uvedu do nej ve sve odpovedi totez
        -- pokud prijde z prava s prazdymm CorrID, vyplnim do CorrID sve odpovedi hodnotu MsgID zpravy prichozi
CorrID RAW(16),
-- To kde vznikl cely tok zprav, napriklad "PORTAL"
Puvodce VARCHAR2(30),
-- Odesilatel teto zpravy napriklad "IPF" nebo "VZPP2-Outcome"
Odesilatel VARCHAR2(30),
-- Upresneni odesilatele, napr. "7200" (rozliseni pro pripad, ze je vice instanci
-- aplikace)
OdesilatelDoplnek VARCHAR2(30),
-- Adresat teto zpravy, napr. "VZPP2/Outcome"
Prijemce VARCHAR2(30),
-- Upresneni adresata zpravy, napr. "7200" (z IPF bude obsahovat
-- cislo okresu) je to doplnek kdy mame vice instanci aplikaci
PrijemceDoplnek VARCHAR2(30),
-- Prostredi: "PROD" pro produkci, "TEST" testovaciho prostredi,
-- "DEV" vyvojove prostredi
Prostredi VARCHAR2(30),
-- Nazev sluzby na okrese, napr. "PrijemDavek"
NazevSluzby VARCHAR2(30),
-- Nazev zpravy, napriklad "KDavka"
NazevZpravy VARCHAR2(30),
-- Verze zpravy napriklad "3"  (v budoucnu se muze menit, aplikace musi
-- znat verzi komunikace)
VerzeZpravy VARCHAR2(30),
-- napr id podani z PORTALU (obecne nejaka reference puvodniho systemu)
Reference VARCHAR2(128),
-- k volnemu pouziti (obsahuje pouze provozni/komunikacni informace ne obchodni data)
ParametrV1 VARCHAR2(128),
-- k volnemu pouziti (obsahuje pouze provozni/komunikacni informace ne obchodni data)
ParametrV2 VARCHAR2(128),
-- k volnemu pouziti (obsahuje pouze provozni/komunikacni informace ne obchodni data)
ParametrD1 DATE,
-- k volnemu pouziti (obsahuje pouze provozni/komunikacni informace ne obchodni data)
ParametrD2 DATE,
-- k volnemu pouziti (obsahuje pouze provozni/komunikacni informace ne obchodni data)
ParametrN1 NUMBER,
-- k volnemu pouziti (obsahuje pouze provozni/komunikacni informace ne obchodni data)
ParametrN2 NUMBER,
-- znakova obchodni data (napr. XML)
DataC CLOB,
```

```
  -- binarni obchodni data (napr. Datove rozhrani)
  DataB BLOB
);
/
```

## 2.6 Pravidla pro stavbu zprávy VZPIPFZPRAVA

Existují doporučená pravidla, která svazují některé parametry typu VZPIPFZPRAVA:

- Parametr NazevZpravy by se měl shodovat s kořenovým elementem XML zprávy obsaženým v DataC
- Binární data primárně vkládat do položky DataB
- Atribut PUVODCE obsahuje hodnotu prvku konzument
- Atribut REFERENCE obsahuje hodnotu prvku referenceKonzumenta
- Při poskytování služby přes AQ musí být do všech odpovědních zpráv přenášeny hodnoty atributů „konzument“ a referenceKonzumenta“ z původního požadavku, který je vyřizován

## 2.7 Posílání zpráv

K posílání zpráv mezi systémy se primárně užívá Směrovacího aparátu (viz také příručka administrátora IFP - ProgramAdmin). Definice AQ front resp. queue table na IPF je proto vždy vytvářena s parametrem MULTICONSUMER = FALSE (výchozí nastavení).

### 2.7.1 Směrovací aparát

Směrovací aparát přenáší zprávy z front, do nichž zapisují procesy, do front, z nichž jsou dále propagovány systémem AQ do vzdálených databází. Tento směr je označen jako *outbound.* Směrovací záznamy jsou ukládány do tabulky PBIPFOUTBOUND.

**Sloupce tabulky PBIPFOUTBOUND**

| Název sloupce | Hodnota | Příklady |
|---|---|---|
| SRC_QUEUE | Název fronty, do níž zapisuje proces | PBVYUPOJNAUP_Q, PBVALPOJNA_Q |
| PRIJEMCE | Název aplikace, pro kterou jsou zprávy určeny | VZPP2-Outcome, VZPP2-Income, PSi |
| PRIJEMCEDOPLNEK | Odlišení instancí aplikací – číslo ÚP | 1900, 7200,…; u ústředních aplikací 9900 |
| PROSTREDI | Prostředí IPF | DEV, TEST nebo PROD |
| NAZEVSLUZBY | Název služby | VytvorSestavu, VyuctovaniPojistence |
| NAZEVZPRAVY | Název zprávy | VytvorSestavu, VyuctovaniPojistence |
| VERZEZPRAVY | Verze zprávy | Výchozí verze všech zpráv je 1.0. Dále se pokračuje 1.1, 1.2,…, 2.0 (dle míry provedených úprav). |
| DEST_QUEUE | Název fronty ve vzdálené databázi, do níž mají být propagovány zprávy z IPF. | PBPSIDEJ_Q, PEIPFIN_Q |

| Název sloupce | Hodnota | Příklady |
|---|---|---|
| | Maximální délka názvu je 10 znaků. | |
| DEST_QUEUE_OWNER | Vlastník fronty ve vzdálené databázi, do níž mají být propagovány zprávy z IPF | PVZP, CVZP |
| PBIPFDBLINK | Klíč databázového linku, který má být při propagaci do vzdálené databáze použit | VZP_OP19_HP1, VZP_OP72_HP1, VZP_OP99_HP2 |
| KORELOVAT | Ano nebo Ne | Pokud směrovací záznam definuje odeslání požadavku z kombinovaného AQ adaptéru (invoke – receive), pak Ano. V ostatních případech Ne. |

Po vložení záznamů do tabulky PBIPFOUTBOUND je nutné spustit proceduru GMIPFAQDISPATCH_ADM.CREATE_QUEUES, která vytvoří fronty, a propagační joby do vzdálené databáze.

Směrovací aparát přenáší zprávy z front, do nichž propagují zprávy vzdálené aplikace, do front, z nichž jsou vybírány procesy. Tento směr je označen jako *inbound.* Směrovací záznamy jsou ukládány do tabulky PBIPFINBOUND.

**Sloupce tabulky PBIPFINBOUND**

| Název sloupce | Hodnota | Příklady |
|---|---|---|
| SRC_QUEUE | Název fronty, do níž vzdálená aplikace propaguje odchozí zprávy | PBVYD_Q, PBPRI_Q, GMKES_Q |
| PROSTREDI | Prostředí IPF | DEV, TEST nebo PROD |
| NAZEVSLUZBY | Název služby | VytvorSestavu, VyuctovaniPojistence |
| NAZEVZPRAVY | Název zprávy | VytvorSestavu, VyuctovaniPojistenceAck |
| VERZEZPRAVY | Verze zprávy | Výchozí verze všech zpráv je 1.0. Dále se pokračuje 1.1, 1.2,…, 2.0 (dle míry provedených úprav). |
| DEST_QUEUE | Fronta, kterou čte proces. | PBVYUPOJZUP_Q, PBVALPOJZ_Q |
| KORELOVAT | Ano nebo Ne | Pokud směrovací záznam definuje příjem odpovědi do kombinovaného AQ adaptéru (invoke – receive), pak Ano. V ostatních případech Ne. |

Před vložením záznamu do tabulky PBIPFINBOUND je nutno zkontrolovat, zda fronta, jejíž název je uveden ve sloupci SRC_QUEUE, existuje a lze z ní vyzvedávat zprávy.

## 2.8 Dokumentace webových služeb

Každá webová služba bude už od počátku svého vývoje evidována a dokumentována v Evidenci služeb VZP.

## 2.9 Další vlastnosti dodržované v souvislosti s IPF procesy

### 2.9.1 Předepsané vlastnosti procesů

1. Proces, který komunikuje asynchronně přes Advanced Queuing (dále AQ), definuje preferenci *Prostredi.* Preference nabývá hodnot DEV (vývoj na prostředcích dodavatele), TEST (testování v testovacím prostředí VZP ČR) nebo PROD (provoz v produkčním prostředí VZP ČR). Dle hodnoty preference Prostředí lze větvit činnost procesu, hodnota preference je též hodnotou atributu VZPIPFZPRAVA.PROSTREDI všech zpráv, které proces odesílá i přijímá. Uvedené dále v přiměřené míře (vždy kdy je to alespoň trochu smysluplné) platí i u ostatních služeb.
2. Persistentní data proces ukládá do Integrační cache. Názvy tabulek jsou odlišeny prefixy, aby nedošlo ke konfliktu názvů: PB – PIKE ELECTRONIC, GM – GEM SYSTEM. K datům a uloženým procedurám přistupuje proces pomocí lokátoru eis/DB/IntegracniCache.
3. Fronty AQ jsou definovány v Integrační cache. K frontám proces přistupuje pomocí lokátoru eis/AQ/IntegracniCacheOutbound (pro vkládání zpráv do front) a eis/AQ/IntegracniCacheInbound (pro výběr zpráv z front).
4. Preference Debug používaná na SOA 10g pro volitelné ukládání instancí synchronních služeb do dehydration store nelze v případě SOA 11g z principu využít a ani pro něj neexistuje adekvátní náhrada. Z migrovaných služeb je tak parametr odstraněn.
5. Z provozních důvodů nesmí jedna instance daného procesu obsahovat více jak 1 000 aktivit.

### 2.9.2 Vlastnosti aplikací komunikujících s IPF

1. Aplikace komunikující s IPF přes rozlehlou síť (WAN), komunikuje zásadně asynchronně prostřednictvím front AQ – jak v případě, že Integrační platformě poskytuje službu, tak v případě, že konzumuje službu Integrační platformy.
2. Aplikace propaguje všechny zprávy všech odesílacích front do jediné společné fronty v IPF. Vlastník fronty je ICACHE. Aplikace se připojuje prostřednictvím databázového linku pod identifikací vzdáleného uživatele ICACHEPROPAG.
3. Aplikace propaguje zprávy do IPF přes port 1501.

### 2.9.3 Instalace procesů do testovacího prostředí IPF

1. Instalaci nových komponent do testovacího prostředí IPF provádí na základě dohody s administrátory IPF buď dodavatel nebo administrátor IPF.
2. Při instalaci do testovacího prostředí se ověřuje postup instalace, který bude následně použit při instalaci do produkčního prostředí.
3. Ověřují se skripty pro vytváření záznamů do směrovacích tabulek, vytváření nových front a databázových objektů v Integrační cache.
4. Ve „wrapper WSDL“ jsou použity URL endpointů testovacího prostředí.
5. Po deploymentu procesů, u nichž je to třeba, se mění hodnota preference Prostredi na TEST.

### 2.9.4 Instalace do produkčního prostředí IPF

1. Instalaci nových komponent do produkčního prostředí IPF instaluje výhradně administrátor IPF na základě návodu dodavatele. Návod je ověřen při instalaci do testovacího prostředí.
2. Pokud je třeba provést zásah do konfigurace produkčního prostředí (parametry BPEL PM, parametry domény apod.), provádí je výhradně administrátor IPF.
3. Pro instalaci objektů v Integrační cache se zásadně používají skripty ověřené při instalaci do testovacího prostředí IPF.
4. Pro založení záznamů v tabulce PBIPFINBOUND se zásadně používají skripty ověřené při instalaci do testovacího prostředí, v nichž se před instalací do produkčního prostředí změní pouze hodnota pro sloupec PROSTREDI z TEST na PROD.
5. Pro založení záznamů v tabulce PBIPFOUTBOUND se zásadně používají skripty ověřené při instalaci do testovacího prostředí, v nichž se před instalací do produkčního prostředí změní pouze hodnota pro sloupec PROSTREDI z TEST na PROD. V případě, že IPF bude nově zasílat zprávy do aplikace ÚP, se skript obohatí o cyklus přes všechna ÚP (PRIJEMCEDOPLNEK).
6. Pro deployment procesů do produkčního prostředí se zásadně používají instalační balíčky (jar) ověřené v testovacím prostředí.
7. Po deploymentu procesů, u nichž je to třeba, se mění hodnota preference Prostredi na PROD.

## 2.10 IPF partitions

### 2.10.1 Jmenné konvence pro BPEL partitions

- Název partition bude vystihovat oblast řešenou umísťovanými procesy.
- Rozdělení podle synchronnosti bude rozlišeno na konci názvu pomlčkou a přidáním písmene „s“ pro služby synchronní a písmenem „a“ pro služby asynchronní.
- Pro založení nové partition je nutné včas podat návrh na založení nové partition. Návrh obsahuje název, účel a nastavení partition v testovacím a produkčním prostředí.
- Dokud nebude návrh odsouhlasen všemi zúčastněnými stranami, není dovoleno partition založit.
- Zůčastněnými stranami jsou zástupci společností VZP, HP, GEM, PIKE.

Po odsouhlasení návrhu všemi zúčastněnými stranami je třeba vytvořit partition ve všech prostředích (a případně do ní přesunout procesy z particí Vyvoj-s a Vyvoj-a).

Pro umístění technologických služeb slouží partition „techws“. Tato partition obsahuje služby a procesy zřízené pouze z technologických důvodů. Tyto procesy nejsou určeny pro užívání libovolnými konzumenty a nebudou tedy publikovány.

### 2.10.2 Konvence pro umístění služeb do partitions

- Související procesy se budou umisťovat do stejné partition (např. procesy určené pro získávání údajů o pojištěncích, bez ohledu na to, zda jsou údaje získávány z Registru subjektů zdravotního pojištění nebo z Centrálního registru pojištěnců).
- Procesy se budou umisťovat do partitions podle synchronnosti. Snaha o oddělení synchronních a asynchronních služeb do separátních partitions pro potřeby přehlednosti.
- Pokud není žádná z již vytvořených partitions vyhovující pro umístění daného procesu, je třeba dodržet pravidla pro vytváření partitions.
- Do partition techws jsou umísťovány procesy s nulovou business funkčností, určené ke konkrétnímu řešení. Tyto procesy by neměly být nijak veřejně používány.
- Procesy specifické pro B2B jsou ujišťovány do partition B2B.

- Pro vývoj procesů určených do partition, která dosud nebyla odsouhlasena a vytvořena, jsou určeny partitions Vyvoj-s a Vyvoj-a, které lze založit v případě potřeby na vývojovém prostředí kdykoliv.

Při jakékoli sebemenší pochybnosti o správnosti umístění BPEL procesu do konkrétní partition je nutné kontaktovat osobu zodpovědnou za správu příslušné partition.

### 2.10.3 ESB jmenné konvence

Současné řešení ESB obsahuje pro umístění WSDL a jejich směrování Systémy (system) a skupiny (group). Systémy jsou nadřazeny skupinám. ESB systémy odpovídají BPEL partitions. Skupiny jsou použitelné pro další volné třídění. Pro ESB systémy platí výše uvedené konvence (zejména jmenné) jako pro BPEL partitions.

# 3. Metodika realizace integračních vazeb

## 3.1 Účel metodiky

Tato metodika vymezuje základní rámec procesů, které probíhají v rámci realizace integračních vazeb mezi aplikačními komponentami informačního systému VZP ČR. Procesy jsou zastřešovány Kompetenčním centrem integrace (dále KCI) ÚICT, které bylo zřízeno pokynem náměstka ředitele VZP ČR pro informatiku.

Mezi základní činnosti KCI patří dohled nad integračními vazbami mezi aplikačními komponentami informačního systému:

- Posouzení a schválení integračních vazeb mezi aplikačními komponentami
- Posouzení a schválení navrhovaných služeb realizujících integrační vazby
- Správa integračních vazeb v aplikaci Evidence služeb
- Posouzení a schválení testovacích scénářů integračních testů
- Kontrola kvality popisu integračních vazeb v administrátorské dokumentaci

Metodika realizace integračních vazeb stanovuje závazné postupy, které musí být dodržovány ve vztahu ke KCI a jsou popsány v následujících kapitolách.

## 3.2 Návrh architektury integrace aplikační komponenty

V rámci procesu dohledu nad integračními vazbami mezi aplikačními komponentami uspořádá dodavatel příslušné komponenty workshop, na kterém představí KCI předpokládanou architekturu začlenění dodávané aplikační komponenty do IS VZP ČR s důrazem na navrhované integrační vazby.

V rámci workshopu se dodavatel zaměří zejména na popis předpokládaných integračních vazeb v souladu se Standardy IS VZP ČR. Budou popisovány služby požadované od IPF i služby nabízené komponentou. Součástí popisu bude i druh předpokládaných integračních vazeb (synchronní služby, asynchronní služby, silná datová integrace,..).

Navrhovaná architektura integračních vazeb podléhá posouzení a schválení Kompetenčním centrem integrace.

## 3.3 Popis integračních vazeb v analytickém projektu

V rámci etapy zpracování analytického projektu popíše dodavatel v samostatné kapitole předpokládané integrační vazby formou služeb v souladu se Standardy IS. Příslušná kapitola analytického projektu musí být předložena Kompetenčnímu centru integrace k posouzení a schválení.

## 3.4 Testovací scénáře integračních vazeb

V rámci projektu implementace příslušné aplikační komponenty do IS VZP ČR zpracuje dodavatel testovací scénáře integračních testů. Tyto scénáře musí být předloženy Kompetenčnímu centru integrace k posouzení a schválení.

## 3.5 Zavedení integračních služeb do aplikace Evidence služeb

V rámci projektu implementace příslušné aplikační komponenty do IS VZP ČR zavede dodavatel příslušné aplikační komponenty všechny integrační služby do aplikace Evidence služeb. Tento krok učiní dodavatel nejpozději v etapě instalace aplikační komponenty do provozního prostředí IS.

Potvrzení úplnosti služeb v Evidenci služeb KCI bude součástí akceptační procedury v rámci projektu implementace příslušné aplikační komponenty dodavatelem.

## 3.6 Popis integračních vazeb v administrátorské dokumentaci

Realizované integrační vazby v rámci implementace aplikační komponenty popíše dodavatel v administrátorské dokumentaci. V samostatné kapitole se zaměří zejména:

- Kompletní seznam služeb poskytovaných implementovanou aplikační komponentou
- Popis realizovaných AQ front
- Přehled konzumovaných služeb v prostředí IPF

Potvrzení úplnosti popisu integračních služeb v administrátorské dokumentaci KCI bude součástí akceptační procedury v rámci projektu implementace příslušné aplikační komponenty dodavatelem.

## 3.7 Workshop k objasnění realizovaných integračních vazeb

V rámci závěrečného testování implementované aplikační komponenty uspořádá dodavatel aplikační komponenty workshop, na kterém objasní implementované integrační vazby s ostatními aplikačními komponentami zejména pro KCI. Ke každé integrační vazbě uvede, kde v předané dokumentaci je popsána.

## 3.8 Realizace změn integračních vazeb

Tato metodika se týká rovněž všech procesů změn aplikačních komponent s dopadem na integrační vazby, a to i těch, které jsou realizovány mimo rámec projektového řízení (projektové aktivity, změny, opravy, servisní zásahy). Výše uvedené odstavce 3.2 – 3.7 se použijí přiměřeně.

| IDENTIFIKACE APLIKACE | |
|---|---|
| **Název aplikce** | |
| **Zkratka názvu aplikace** | |
| | |
| **Jméno projektového managera** | |
| | |
| **správce aplikace** | |
| **administrátor aplikace** | |
| **administrátor databáze** | |
| **administrátor operačního systému** | |
| **administrátor sítí** | |
| **administrátor monitoringu** | |
| **řešitelská skupina SD** | |

| **Protokol o převzetí aplikace do podpory ICT** | | | ZÁVĚREČNÝ KROK Z PROJEKTOVÉ KANCELÁŘE DO PROVOZU OTP/OKP |
|---|---|---|---|
| **Identifikace aplikace** | **Název - zkratka projektu / aplikace** | | |
| | Datum verze předávacího protokolu | | |
| | | | |
| **Zadavatel** | IT garant | | |
| | Odborný garant | | |
| | **Odborný garant=vlastník** | | |
| | | | |
| **Informace o dodavateli** | **Dodavatel** | | *Kontakt na dodavatele, který zajišťuje support - dle supportní smlouvy.* |
| | Zástupce dodavatele | | |
| | **Smlouva o dílo/Supportní smlouva** | | |
| | Dodatek ke smlouvě | | |
| | | | |
| **Nutná dokumentace pro odbor klientské podpory** | **Uživatelská příručka** | | |
| | Definice podpory z pohledu Service Desku | | *V rámci incident managmenta musí být stanoven způsob podpory se Service Deskem.* |
| | | | |
| **Nutná dokumentace pro odbor technické podpory** | **Administrátorská příručka, provozní dokumentace dle administrátorské osnovy** | | |
| | **Datový model** | | |
| | Instalační návody | | |
| | | | |
| **Školení pro odbor klientské podpory** | **Uživatelská školení** | | |
| | pro Lokální správce | | |
| | | | |
| **Školení pro odbor technické podpory** | **Administrátorské školení = správci aplikace** | | |
| | Jná školení | | |
| | | | |
| **Datum testování** | Betatest | | |
| | Pilotní provoz | | |
| | Zátěžové test | | |
| | **Ostrý provoz** | | |
| | | | |
| **Zrušení projektových přístupů externích pracovníků do produkčního prostředí aplikací** | VPN - Oddělení správy sítí | provedeno AND/NE | |
| | Kerberos - oddělení správy unixových systémů | provedeno AND/NE | |
| | doména Microsoft Windows - Oddělení správy Microsoft systémů | provedeno AND/NE | |
| | Oracle a databázové účty s právy administrace dB - administrátor databáze | NEPŘIDĚLUJÍ SE | |
| | Servisní účty aplikací - aplikační administrátor aplikace | provedeno AND/NE | |
| | | | |
| Žádost o supportní přístupy dodává vlastník supportní smlouvy aplikačního SW = OKP<br>Žádost o supportní přístupy dodává vlastník supportní smlouvy technologických celků = OTP | | | |
| **Zřízení neaktivních supportních přístupů externích pracovníků do produkčního prostředí aplikace** | VPN - Oddělení správy sítí | provedeno AND/NE | |
| | Kerberos - oddělení správy unixových systémů | provedeno AND/NE | |
| | doména Microsoft Windows - Oddělení správy Microsoft systémů | provedeno AND/NE | |
| | Oracle a databázové účty s právy administrace dB - db administrátor | standardně nejsou zakládány. Pouze na vyžádání supportní podpory v rámci řešení IM s prio 1 | |
| | Servisní účty aplikací - aplikační administrátor aplikace | provedeno AND/NE | |
| | | | |
| **Aplikaci předal do provozu, dne:** | | | |
| **Souhlas ředitele odboru architektury, vývoje aplikací a řízení změn, dne:** | | **Mgr. Jaroslav Bogač, MBA** | |
| **Aplikaci převzal do provozu za OKP, dne:** | | **Cibor Legát** | |
| **Aplikaci převzal do provozu za OTP, dne:** | | **Ing. Roman Palkovič** | |

# 1 Společné zásady pro povolení a rušení přístupu

## 1.1.1 Povolování přístupu

1) Účty se zakládají pouze na základě Servisního požadavku.

2) Založení účtu pro oprávněnou osobu může požadovat:

- Projektový vedoucí – pro externí pracovníky po dobu trvání projektu
- Manager L3 správy aplikace – pro aplikace převzaté do provozu
- Garant suportové smlouvy – pro externí pracovníky zajišťující support
- Ředitel OTP nebo náměstek ÚICT VZP ČR – ve všech případech

3) V servisním požadavku musí být uvedeno, k jakému účelu bude účet používán.

4) Jedná-li se o přístup pro externího pracovníka, musí být v servisním požadavku uvedeno pro jakou firmu se účet zřizuje a jméno pracovníka externí firmy, který bude účet používat.

5) V servisním požadavku musí být uvedeno po jakou dobu, má být účet platný.

6) Servisní požadavek musí být odsouhlasen schvalovatelem - pracovníkem zodpovědným za bezpečnost informačních technologií VZP ČR.

7) Následné fyzické přidělení přístupu a zdokumentování tohoto aktu v provozním deníku OTP provádí vždy přidělovatel za příslušnou oblast (VPN, MS doména, Kerberos).

## 1.1.2 Rušení přístupů

1) Po uplynutí doby platnosti, která byla požadována v servisním požadavku, bude účet zablokován.
2) V případě, že pomine důvod používání účtu před uplynutím doby jeho platnosti nebo tato situace nastane u účtu s neomezenou dobou platnosti, je povinností žadatele požádat servisním požadavkem o zrušení účtu/přístupu, aby mohl být udržen konzistentní stav, který vyhovuje auditovaným požadavkům na bezpečnost informačního systému.
3) Při předávání projektu/aplikace do provozu (standardní interní proces VZP ČR mezi ORP a OTP) budou všechny přístupy externích pracovníků do produkčního prostředí této aplikace zablokovány. Budou zároveň změněna všechna hesla „superuživatelských" účtů. Jedná se zejména o unixový účet oracle a databázové účty s právy administrace dB.
4) Tato operace bude provedena a zaznamenána v provozním deníku příslušným přidělovatelem.

**Okruhy informací pro zpracování administrátorské dokumentace**

**A. Popis systému**
1. Přehledový popis architektury aplikace, vč. diagramů a schémat.
2. Popis aplikační logiky, použité objekty (tabulky, fronty) - k čemu slouží, jak jsou procesně navázány, odkud kam co putuje, co se kde loguje - které jsou administrátoři
3. Způsob implementace aplikace do prostředí VZP včetně popisu konkrétního řešení.

**B. Popis technologie a infrastruktury**
1. Rozbor všech objektů na úrovni technologie a infrastruktury.
2. Specifikace a seznam strojů, na nějž byla/má být aplikace implementována.
3. Přesná specifikace operačního systému, v případě implementace do prostředí VZP uvést zdrojový image (včetně data instalace), na němž bylo postaveno (pokud
4. Seznam nasazených/vyžadovaných patchů proti standardnímu image VZP.
5. Seznam všech unixových účtů (dle strojů), jež aplikace vyžaduje.
6. Seznam všech komponent (a systémů), které musí pro správný chod aplikace současně běžet (včetně komponent FailOver). Startovací parametry těchto prostředí pro
7. V případě clusterového řešení seznam nodů, jejich funkce, umístění, postupy pro start a stop clusteru, přepnutí do druhé lokality, popis nutných skriptů, kompletní postupy
8. Specifikace aplikačních komunikačních toků včetně způsobu autentizace/autorizace mezi unix uživateli a strojů, na nichž je aplikace implementována.
9. Seznam doplňkového SW (SW mimo standardní image), jež aplikace vyžaduje (tj. seznam všeho, co bylo instalováno mimo adresáře dedikované aplikaci)
10. Pro doplňkový SW způsob administrace, zálohování, monitoringu funkčnosti, pokud není součástí popisu aplikace.
11. Popis adresářů dedikovaných aplikaci a popis jejich obsahu, přístupová práva.
12. Přehled souborových vstupů/výstupů.
13. Specifikace nároků na datová úložiště – aktuální a s predikcí v horizontu 5 let.
14. Přesná specifikace databázového systému a souvisejícího software (aplikačních serverů…), seznam konfiguračních souborů, jejich proměnných a možných hodnot.
15. Popis a schémata DB instancí (tablespace, tabulky, indexy, uživatelé, role…).
16. Požadované LAN, WAN, SAN spojení.

**C. Administrativní nástroje**
1. Uvést popis administrativních nástrojů, specifických pro aplikaci. Pokud existuje v aplikaci sekce pro administrátory, podrobný popis funkcionality (je možné nahradit
2. Uvést odkaz na standardní administrativní nástroje určené ke správě aplikace.
3. Uvést popis akcí, prováděných administrátorem (start/stop systému, maintenance aplikace…) včetně nutných omezení s ohledem na vazby na okolí.

**D. Diagnostika a monitoring**
1. Seznam logových souborů - důležité (klíčové) logy aplikačních činností zdůraznit.
2. Výčet takových kritických objektů, které je potřeba umět skontrolovat (tj. jak, čím apod.) a umět na nich identifikovat problém (tj. proč).
3. Seznam pracovních oblastí, kde může docházet k nárůstu dat a zaplnění filesystémů.
4. Návod, jak ověřit zdraví aplikace a její funkčnost např. podle následujícího schématu:
   i. Podívejte se tam a tam jestli to vypadá tak a tak - definovat co je běžný stav a co indikuje problém.
   ii. Sepsat doporučené postupy, jak řešit problémy tj. zastavte to a to, udělejte to a to a zase to nastartujte tak a tak a ověřte, že je to ve stavu tom a tom
   iii. Uvést jaké množství logů, front, generovaných souborů v jednotlivých filesystémech, plnění pracovních oblastí je ještě v normálu a kdy už je systém přetížen (nestíhá).
   iv. Standardní DB a OS procesy – aby se dalo odlišit, jestli je db v klidu nebo na ní někdo pracuje (z pohledu aplikace, ne standardní procesy DB instance – aby bylo jasné, co je běžná aktivita na pozadí a co je spuštěná akce kterou není radno přerušit).
5. Popis ověření funkčnosti integračních vazeb na ostatní aplikace.

**E. Pravidelná údržba a profylaxe, upgrade a nasazování patchů**
1. Doporučení profylaktických aktivit a jejich časového režimu (jak sledovat logy apod).
2. Doporučené intervaly/termíny odstávky pro upgrady, patchování systému.
3. Doporučený interval rebootu.

**F. Typické chybové stavy a jejich popis nejčastějších nebo nejzávažnějších chybových stavů s výstižným popisem jejich identifikace, doporučený postup řešení.**

**G. Zálohování a obnovení**
1. Požadavky na zálohování a archivaci dat:
   i. periodicita
   ii. kapacita aktuální a s predikcí v horizontu 5 let.
2. Použité specifické zálohovací nástroje, podrobný popis použití a nastavení.
3. Uvést odkaz na použité standardní zálohovací nástroje.
4. Recovery plán pro kompletní zálohu a obnovu prostředí a dat.

**H. Integrace**
1. Popis komunikačních a datových toků.
2. Popis integračních vazeb s ostatními aplikacemi, komunikace s integrační platformou, popis souvisejících BPEL procesů…

**I. Monitoring**
1. Popis monitoringu.
2. Doporučení, které procesy mají být monitorovány a jakým způsobem.
3. Popis vazeb na dohledové nástroje a seznam monitorovaných událostí a stavů.

| Název aplikace | *Aplikace č.1 (např. CVOFF)* | START+1Q | | START+2Q | | START+3Q | | START+4Q | | START+5Q | | START+6Q | | START+7Q | | START+8Q | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Typ kapacitního požadavku | Specifikace kapacitního požadavku - START | TVS | PROD | TVS | PROD | TVS | PROD | TVS | PROD | TVS | PROD | TVS | PROD | TVS | PROD | TVS | PROD |
| Servery [počet, typ, parametry] | *2x DL380G6 (2xCPU, 500GB RAM)* | | | | | | | | | | | | | | | | |
| Virtualizace | *Ano (VMware, HPVM)* | | | | | | | | | | | | | | | | |
| HW Architektura | *x86, IA64* | | | | | | | | | | | | | | | | |
| HA řešení | *Vmware, Oracle RAC, ServiceGuard* | | | | | | | | | | | | | | | | |
| Datová centra [Rack Units] | *2U DC Orlická*<br>*2U DC Perštýn* | | | | | | | | | | | | | | | | |
| Sítě [počet Ethernet portů] | *4x1Gb* | | | | | | | | | | | | | | | | |
| SAN [počet FC portů] | *2x2porty 8Gb* | | | | | | | | | | | | | | | | |
| SAN diskové prostory [TB] | *1TB rychlé disky*<br>*0,5TB pomalé disky* | | | | | | | | | | | | | | | | |
| Lokální diskové prostory [TB] | *8x 300GB SAS* | | | | | | | | | | | | | | | | |
| Zálohování | */appl_xxx, /vzp_xxx* | | | | | | | | | | | | | | | | |
| Licence DB | *1x Oracle Enterprise DB* | | | | | | | | | | | | | | | | |
| Licence APL | *1x WebLogic* | | | | | | | | | | | | | | | | |
| Licence OS | *1x Red Hat Enterprise Linux* | | | | | | | | | | | | | | | | |
| Licence BACKUP | *1x DataProtector agent* | | | | | | | | | | | | | | | | |
| Licence MON | *1x BSC agent* | | | | | | | | | | | | | | | | |
| Datum, kdy má být kapacita připravena | DD.MM.RRRR | | | | | | | | | | | | | | | | |
| Plán podpisu smlouvy o dílo/realizaci | DD.MM.RRRR | | | | | | | | | | | | | | | | |
| Plán zahájení projektu | DD.MM.RRRR | | | | | | | | | | | | | | | | |

| Název aplikace | *Aplikace č.2 (např. IPF)* | START+1Q | | START+2Q | | START+3Q | | START+4Q | | START+5Q | | START+6Q | | START+7Q | | START+8Q | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Typ kapacitního požadavku | Specifikace kapacitního požadavku - START | TVS | PROD | TVS | PROD | TVS | PROD | TVS | PROD | TVS | PROD | TVS | PROD | TVS | PROD | TVS | PROD |
| Servery [počet, typ, parametry] | *2x DL380G6 (2xCPU, 500GB RAM)* | | | | | | | | | | | | | | | | |
| Virtualizace | *Ano (VMware, HPVM)* | | | | | | | | | | | | | | | | |
| HW Architektura | *x86, IA64* | | | | | | | | | | | | | | | | |
| HA řešení | *Vmware, Oracle RAC, ServiceGuard* | | | | | | | | | | | | | | | | |
| Datová centra [Rack Units] | *2U DC Orlická*<br>*2U DC Perštýn* | | | | | | | | | | | | | | | | |
| Sítě [počet Ethernet portů] | *4x1Gb* | | | | | | | | | | | | | | | | |
| SAN [počet FC portů] | *2x2porty 8Gb* | | | | | | | | | | | | | | | | |
| SAN diskové prostory [TB] | *1TB rychlé disky*<br>*0,5TB pomalé disky* | | | | | | | | | | | | | | | | |
| Lokální diskové prostory [TB] | *8x 300GB SAS* | | | | | | | | | | | | | | | | |
| Zálohování | */appl_xxx, /vzp_xxx* | | | | | | | | | | | | | | | | |
| Licence DB | *1x Oracle Enterprise DB* | | | | | | | | | | | | | | | | |
| Licence APL | *1x WebLogic* | | | | | | | | | | | | | | | | |
| Licence OS | *1x Red Hat Enterprise Linux* | | | | | | | | | | | | | | | | |
| Licence BACKUP | *1x DataProtector agent* | | | | | | | | | | | | | | | | |
| Licence MON | *1x BSC agent* | | | | | | | | | | | | | | | | |
| Datum, kdy má být kapacita připravena | DD.MM.RRRR | | | | | | | | | | | | | | | | |
| Plán podpisu smlouvy o dílo/realizaci | DD.MM.RRRR | | | | | | | | | | | | | | | | |
| Plán zahájení projektu | DD.MM.RRRR | | | | | | | | | | | | | | | | |

**Tabulka - 1 - základní údaje**
**(vyplývající ze schválených investic)**

| **Hardware** | | |
|---|---|---|
| požadovaný počet serverů | | |
| umístění HW (Orlická - Perštýn - jiná lokalita) | | |
| HW / virtuální server | | |
| Failover aplikace | ANO - NE | |
| Scripty pro Failover dodány | ANO - NE | |
| operační systém | | |
| odhadnutý požadovaný výkon - počet procesorů/počet jader v procesoru | | |
| odhadnutá velikost paměti | | |
| odhadnuté prostory na discích - lokálně/na SAN v GB | | |
| odhadnuté kapacity zálohovaných dat v GB | | |
| odhad celkové spotřeby energie v kW pro uvedenou lokalitu | | |

| **Požadované licence (db i apl)** | | |
|---|---|---|
| druh databáze, verze | | |
| počet a druh databázových licencí (včetně options) | | *RAC, partitioning, ….* |
| Počet a druh licencí aplikačního serveru | | |
| odhadovaný počet uživatelů používajících aplikaci | | |
| termín, ke kterému mají být licence k dispozici | | |
| **počet a typ dalších nutných licencí** | | |
| **Smlouva k nákupu licencí** | | *hypertextový odkaz přímo na poažadovaný dokument* |
| **počet a typ nutných certifikátů** | | |

| **Ostatní software** | |
|---|---|
| název software, verze | |
| využití tiskového subsystému **ANO - NE** | |

| **Provozní parametry, šedivě *označené řádky musí být vyplněny*** | |
|---|---|
| Dopady jednodenního výpadku služby v Kč: | |
| Požadovaná dostupnost v % (SLA): | |
| MTBF: | |
| Celkový počet uživatelů: | |
| Počet konkurenčních uživatelů: | |

| **Požadované dostupnosti, *vybírejte z nabídky*** | |
|---|---|
| Požadovaná dostupnost aplikací | |
| Požadovaná dostupnost infrastruktury (viz Standardy IS VZP ČR) | |
| Požadovaná doba obnovy (MTTR) / Akceptovatelná doba výpadku v řádu | |

| Tabulka - 2 - vytvoření prostředí pro aplikaci<br>(vyplývající z analytického projektu - spolupráce s dodavetelem) | |
|---|---|
| **Analytický projekt** | |
| | *hypertextový odkaz přímo na poažadovaný dokument* |

| **Aplikační a Databázový systém Oracle** | | |
|---|---|---|
| typ a verze použitého/tých aplikačního/ních serverů | | *př. WLS 11g - Forms a reports,* |
| verze databáze Oracle | | *! 11gR2 a vyšší verze, dlestandardů IT VZP ČR* |
| vždy definovat hodnoty inicializačních parametrů dB: | | |
| instance_name (SID) | | |
| code page (inicializační kódová stránka dB - nelze měnit) | | default ve VZP=EE8ISO8859P2 |
| sga_target | | |
| sga_max_size | | |
| processes | | |
| job_queue_processes | | |
| aq_tm_processes | | |
| názvy schémat (uživatelů-vlastníků objektů) a jejich minimální dB grants (výčet) | | mimo zde uvedená schémata nebude mít databáze jiné vlastníky objektů |
| výčet jmen dalších potřebných servisních účtů aplikace | | mimo zde uvedená jména nebude mít aplikace v databázi žádné uživatelské/servisní účty |
| další parametry, kde nevyhovují defaultní hodnoty | | |

| | | |
|---|---|---|
| **Diskové prostory pro ORACLE** | | |
| **Aplikační server** | | |
| velikost dačasného pracovního prostoru pro Forms a Reports (iastmp) | | |
| /app13w (v GB), adresář pro aplikační moduly | | |

| | | |
|---|---|---|
| **Databázový server** | | |
| /app1, aplikační data | | |
| /vzp.data, aplikační data | | *datové soubory, se kterými aplikace pracuje a ukládá na Filesystémy* |
| Inicializační velikost tablespaců | | |
| 1) data+indexy (celkem) | | |
| 2) temporary | | |
| 3) undo | | |

| **Systém Windows prostředí** | | Vyplňovat v případě Windows prostředí |
|---|---|---|
| **Komunikace s AD** | | *Uvést DC, s kterými bude probíhat komunikace* |
| LDAP dotaz | | |
| **Aplikační server** | | |
| operační systém přesná specifikace | | |
| systémový disk (GB) | | |
| datový disk/y (GB) | | |
| požadavky na SW | | |
| **Databázový server** | | |
| databázový systém MS SQL - přesná specifikace | | |
| inicializační velikost databází | | |
| data (GB) | | |
| transakční logy (GB) | | |

| **Hardware - typy serverů** | | *vyplnit pro požadovaný počet serverů* |
|---|---|---|
| **Typ serveru 1**, model, název provozované aplikace nebo služby | | |
| umístění HW (Orlická - Perštýn - jiná lokalita) | | |
| Identifikační číslo serveru (z "Tabulky_serverů_centralizace_vDC") | | |
| Operační systém a jeho verze | | |
| počet jader v procesoru | | |
| RAM - spotřeba pro všechny procesy aplikace včetně dB a OS | | |
| spotřeba energie v kW | | |

| | |
|---|---|
| **Typ serveru 2**, model, název provozované aplikace nebo služby | |
| umístění HW (Orlická - Perštýn - jiná lokalita) | |
| Identifikační číslo serveru (z "Tabulky_serverů_centralizace_vDC") | |
| Operační systém a jeho verze | |
| počet jader v procesoru | |
| RAM - spotřeba pro všechny procesy aplikace včetně dB a OS | |
| spotřeba energie v kW | |

| | |
|---|---|
| **Typ serveru 3**, model, název provozované aplikace nebo služby | |
| umístění HW (Orlická - Perštýn - jiná lokalita) | |
| Identifikační číslo serveru (z "Tabulky_serverů_centralizace_vDC") | |
| Operační systém a jeho verze | |
| počet jader v procesoru | |
| RAM - spotřeba pro všechny procesy aplikace včetně dB a OS | |
| spotřeba energie v kW | |

**Tabulka - 3a - síťová část požadavky na WAN**
**spolupráce s dodavatelem**

| **Jméno komponenty** | šířka pásma | latence | jiné specifické nastavení sítě (QoS, nastavení WAN akcelerátorů,apod.) | požadavky na testování/měření WAN komunikace | počet současný uživatelů z 1 pobočky |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| každý síťový list pro jeden server | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **ID jméno serveru** | | | | | |
| Vrstva | | | | | |
| zóna | | | | | |
| Prostředí | | | | | |
| Operační systém | | | | | |
| | | | | | |
| **Lokální aplikace** | | | | | |
| Název aplikace | Stickinrss | Keepalive URL | Protokol | Porty | Sezení (čas v sec) |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| **Komunikační toky** | | | | | |
| Název lokální aplikace | Cílový prvek | Protokoly | Porty | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| **Konfigurace serveru** | | | | | |
| | ILO | lan0 | | | |
| DNS jméno | | | | | |
| IP adresa | | | | | |
| maska | | | | | |
| GW | | | | | |
| VLAN ID | | | | | |
| MAC | | | | | |
| port sw | | | | | |
| switch | | | | | |
| DNS | | | | | |
| | | | | | |
| Interface: | | | | | |
| lan n | lan1 | lan2 | lan3 | lan4 | lan5 |
| DNS název | | | | | |
| způsob konfigurace | | | | | |
| | | | | | |
| IP Adresa | | | | | |
| maska | | | | | |
| Gateway | | | | | |
| VLAN ID | | | | | |
| MAC | | | | | |
| Port switche | | | | | |
| switch | | | | | |

| Název položky | Vysvětlivka | | | Kdo vyplní |
|---|---|---|---|---|
| ID jméno serveru | Číslo serveru (číslo z "Tabulky_serverů_centralizace_vDC") na kterém bude služba/aplikace/databáze provozována) | | | **Doplní projektový vedoucí** |
| Vrstva | aplikační, databázová, prezentační (u služeb), management, perímeter | | | **Doplní projektový vedoucí** |
| Prostředí | Produkční, vývojové testovací | | | **Doplní projektový vedoucí** |
| Operační systém | HP UX, Linux | | | **Doplní projektový vedoucí** |
| | | | | |
| **Lokální aplikace** | Popis aplikací prozovaných na serveru, pokud jich bude více je nutné vyplnit pro každou aplikaci | | | **Doplní projektový vedoucí** |
| Název aplikace | Jméno aplikace dle jmenné konvence VZP | | | **Doplní projektový vedoucí** |
| Stickiness | **Ano**-v případě rozložení zátěže při zpracování aplikace na více serverů je požadavek na komunikaci se stále stejným serverem se kterým byla komunikace navázána<br>**Ne**- každý požadavek klienta na aplikaci je možné zasílat na jiný aplikační server | | | **Doplní projektový vedoucí** |
| Keepalive URL | URL jež je kontrolováno na dostupnost služby | | | **Doplní projektový vedoucí** |
| Sezení (čas v s) | Čas sezení udávaný v sekundách | | | **Doplní projektový vedoucí** |
| Protokol | Síťový protokol, který používá aplikace (TCP, UDP, HTTP, ….) | | | **Doplní projektový vedoucí** |
| Port | Číslo (název) síťového portu, na kterém poslouchá aplikace | | | **Doplní projektový vedoucí** |
| Nestandardní požadavky | Požadavky aplikace, které nejsou v souladu s dokumentem "Standardy IS VZP ČR", např. požadavek přímé komunikace s jinou aplikací, s objektem mimo DC a pod | | | **Doplní projektový vedoucí** |
| | | | | |
| **Komunikační toky** | Popis komunikačních toků, tkeré navazuje aplikace směrem pryč ze serverů (nutné pro konfiguraci prostupů na FW) | | | **Doplní projektový vedoucí** |
| Název lokální aplikace: | | | | **Doplní projektový vedoucí** |
| Cílové zařízení | Cílové zařízení, kde je provozovaná externí (jiná) aplikace. Cílové zařízení se zadává pomocí jedné z následujících možností:<br>IP adresa<br>VIP - virtuální IP adresa<br>DNS jméno | | | **Doplní projektový vedoucí** |
| Protokol | Síťový protokol (TCP, UDP, HTTP,….) použitý pro komunikaci s externí aplikací | | | **Doplní projektový vedoucí** |

| **Konfigurace serveru** | **ILO** | **lan0** | | **Kdo vyplní** |
|---|---|---|---|---|
| DNS jméno | | | | **doplní síťaři** |
| IP adresa | | | | **doplní síťaři** |
| maska | | | | **doplní síťaři** |
| gateway | | | | **doplní síťaři** |
| MAC | | | | **doplní síťaři** |
| ID_VLAN | | | | **doplní síťaři** |
| switch | | | | **doplní síťaři** |
| DNS server (do resolv.conf) | | | | **doplní síťaři** |
| | | | | |
| Interface: | Pro každý interface zvlášť | | | **Kdo vyplní** |
| lan (1 -n) | | | | **doplní servraři** |
| DNS název | | | | **doplní servraři** |
| konfigurace | teaming, heard beat, APA,…. | | | **doplní servraři** |
| | | | | |
| IP Adresa | | | | **doplní síťaři** |
| maska | | | | **doplní síťaři** |
| Gateway | | | | **doplní síťaři** |
| VLAN ID | (pro informaci) | | | **doplní síťaři** |
| MAC | (pro kontrolu) | | | **doplní síťaři** |
| Port switche | (pro kontrolu) | | | **doplní síťaři** |

## Oracle Infrastruktura

| | |
|---|---|
| | (doplň k existenci notifikačních pravidel definovaných v OEM, která mají zapnutou integraci spolu do OMU) |

| Host/Instance/Cluster | Jména instancí zahrnutých v NP | Typ | Notifikační pravidlo v OEM |
|---|---|---|---|

## Obecné zadání monitoringu

(popis pod nakresele pod tabulkou; standardy monitoringu UNIX, Windows OS a virtualizace vnitřní jsou popsány zvlášť níže)

| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Zdroj | | | | Kontrola | | | | | | | | | | | Zpracování | | | | Output | |
| 10 | 15 | 17 | 20 | 30 | | 50 | 65 | 70 | 85 | 90 | 105 | 110 | 115 | 130 | 140 | 170 | 180 | 210 | 240 | |
| ID | Nástroj | Stav implementace | Host / Instance | Popis typ instance | Typ objektu, popis | Sledovaný objekt | Metoda kontroly | Operátor | Hodnota (prahová hodnota) | Interval kontroly | Počet chybných po sobě jdoucích | Závažnost | Text (kontrolovaný / chybný/dobrý stav) | Zpráva v NL | Instrukce | Eskalace (kdy) | Notifikace (kdo) | Operační podmínky (kdy/jak) | Poznámky | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |

### Popis vyplňovaných polí

(Rozšíření verze tabulky)

| | |
|---|---|
| 10 | ID |
| 15 | Nástroj - Nástroj |
| 17 | Stav implementace |
| 20 | Host / Instance |
| 30 | Popis typ instance |
| 40 | Typ objektu, popis |
| 50 | Sledovaný objekt |
| 65 | Metoda kontroly |
| 70 | Operátor |
| 85 | Hodnota (prahová hodnota) |
| 90 | Interval kontroly |
| 105 | Počet chybných po sobě jdoucích |
| 110 | Závažnost |
| 115 | Text (kontrolovaný / chybný/dobrý stav) |
| 130 | Zpráva v NL |
| 140 | Instrukce |
| 170 | Eskalace (kdy) |
| 180 | Notifikace (kdo) |
| 210 | Operační podmínky (kdy/jak) |
| 240 | Poznámky |

### Popis závažností (severities)

| | |
|---|---|
| Critical | ucelená chyba způsobující nedostupnost aplikace nebo dat, která bez zásahu povede k nedostupnosti |
| Major | ucelená chyba způsobující SOO nefunkčnost nebo ztrátu clients aplikace |
| Minor | SOO chyba nezpůsobující nedostupnost |
| Warning | varování, že se blíží kritické hodnoty, ale systém ještě nefunguje chyb aplikace |
| Normal | informační stav nebo návrat do plně fungujícího stavu |

## Standardní monitoring HP-UX serverů

### Seznam sada templates pro monitoring UNIX serverů

| Template | | Fyziká servery | | | |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| TOP_OS_HPUX_MC/SG1128 | /var/adm/syslog/syslog.log | x | x | x | x |
| TOP_OS_HPUX | Kernelová konfigurace | x | x | x | x |
| TOP_OS_HPUX-Boot-Logs | /var/adm/sw/swlog | x | x | x | x |
| TOP_OS_HPUX-Boot.log | /var/adm/boot.log | x | x | x | x |
| TOP_OS_HPUX-Cron.log | /var/adm/cron/log | x | x | x | x |
| TOP_OS_HPUX-Dmesg | /dev/crl/mesg | x | x | x | x |
| TOP_OS_HPUX-Syslog | /var/adm/syslog/* | x | x | x | x |
| TOP_OS_HPUX-Sulog | /var/adm/sulog | x | x | x | x |
| TOP_OS_HPUX-Swlog | /var/adm/sw/swlog.log | x | x | x | x |
| TOP_OS_HPUX-Vxmsg | /var/vxvm/vxmsg/vxmsg.log | x | x | x | x |
| TOP_OS_HPUX-mailq | /var/adm/syslog/mail.log | x | x | x | x |
| TOP_OS_HPUX-Mail-Queue | Delaktnost length of sendmail mail queue (unsent email) | x | x | x | x |
| TOP_OS_HPUX-Mail-Queue | Delaktnost length of sendmail mail queue (unsent email) | x | x | x | x |
| TOP_OS_HPUX-Mount | TOP HP-UX Mount of the filesystems | x | x | x | x |
| TOP_OS_HPUX-mount/df | TOP HP-UX Filemount of mount related directories and files | x | x | x | x |
| TOP_OS_HPUX-mount/quota2 | Disk/mount usgimeni aktivace ve /var/opt/ov/log/quota | x | x | x | x |
| TOP_OS_HPUX-mount/quota3 | Disk/mount limity mající ve /var/opt/ov/log/quota | x | x | x | x |
| TOP_OS_HPUX-mount/quota4 | Disk/mount limity mající ve /var/opt/ov/log/quota | x | x | x | x |
| TOP_OS_HPUX-ntp | Stav přístupu/ntp/ntp.conf | x | x | x | x |
| Monitoring Tripplebo: /etc/ | Misc: 75% Warning, 80% Minor, 85% Major, 90% Critical | x | x | x | x |
| Monitoring Tripplebo: /var/ | Secur: 50% Major, 75% Critical | x | x | x | x |
| Monitoring Tripplebo: /tmp/ | Misc: 50% Major, 75% Critical | x | x | x | x |
| Monitoring Tripplebo: /var/tmp/ | Misc: 50% Major, 75% Critical | x | x | x | x |
| Monitoring Tripplebo: /var/opt/ (var, /, /tmp, /home, /var, | Misc: 50% Major, 90% Critical | x | x | x | x |
| Monitoring procesy: | sendmail | x | x | x | x |
| | cron | x | x | x | x |
| | inetd | x | x | x | x |
| | syslog | x | x | x | x |
| | ntpd | x | x | x | x |
| | mqio | x | x | x | x |
| | ovcd | x | x | x | x |
| | ovbbccb | x | x | x | x |
| | lpsfog | x | x | x | x |
| | ovtrace | x | x | x | x |

Výkonnostní parametry - HP Performance Agent (v rozsah základních statistických metrik)

| | | | | | |
|---|---|---|---|---|---|
| GBL_CPU_TOTAL_UTIL - CODA GBL_CPU_TOTAL_UTIL | % využití CPU | x | x | x | x |
| TBL_FILE_TABLE_UTIL - TBL_FILE_TABLE_UTIL | % využití tabulky otevřených souborů | x | x | x | x |
| GBL_MEM_PAGEOUT_RATE | počet stránek na disk za sekundu | x | x | x | x |
| TBL_NFS_TABLE_UTIL - TBL_NFS_TABLE_UTIL | % využití tabulky NFS souborů | x | x | x | x |
| GBL_NET_COLLISION_RATE | počet kolizí za sekundu na všech síťových rozhraní | x | x | x | x |
| TBL_PROC_TABLE_UTIL - TBL_PROC_TABLE_UTIL | % aktivních procesů z tab. procesů | x | x | x | x |
| TBL_SEM_TABLE_UTIL - TBL_SEM_TABLE_UTIL | % aktivních monostabilních z užívání | x | x | x | x |
| TBL_SHMEM_TABLE_UTIL - TBL_SHMEM_TABLE_UTIL | % segmentů sdílené paměti monostabilní z užívání | x | x | x | x |
| GBL_SWAP_SPACE_UTIL - GBL_SWAP_SPACE_UTIL | % nevyužívaného prostoru k stránkování | x | x | x | x |

## Standardní monitoring Windows serverů

### Seznam instalovaných management packů

| Management Pack | Verze | Fyziká servery | | | |
|---|---|---|---|---|---|
| | | | | | |
| Active Directory Server 2003 (Diagnosis) | 6.0.6242.0 | x | x | x | x |
| Active Directory Server 2003 (Diagnosis) | 6.0.6243.0 | x | x | x | x |
| Active Directory Server 2008 and above (Diagnosis) | 6.0.6243.0 | x | x | x | x |
| Active Directory Server 2008 and above (Monitoring) | 6.0.6243.0 | x | x | x | x |
| Active Directory Server Core (Monitoring) | 6.0.6243.0 | x | x | x | x |
| Active Directory Server Common Library | 6.0.6242.0 | x | x | x | x |
| Exchange Server 2010 | 14.3.38.4 | x | x | x | x |
| Exchange Server 2010 Report Library | 14.3.38.2 | x | x | x | x |
| Hewlett-Packed ProLiant Advanced Management Pack | 5.2.0.0 | x | x | x | x |
| Hewlett-Packed ProLiant Agentless Management Pack | 5.2.0.0 | x | x | x | x |
| Hewlett-Packed ProLiant Monitoring Library Management Pack | 5.1.0.0 | x | x | x | x |
| Hewlett-Packed ProLiant Servers Base | 2.1.0.3 | x | x | x | x |
| Hewlett-Packed ProLiant Servers SNMP Management Pack | 2.1.0.0 | x | x | x | x |
| Hewlett-Packed ProLiant Servers Library | 2.1.0.0 | x | x | x | x |
| JEE Application Server Library | 7.0.1038.0 | x | x | x | x |
| JEE Template Configuration Views | 7.0.1038.0 | x | x | x | x |
| JEE Templates Library | 7.0.1038.0 | x | x | x | x |
| JEE Tomcat 5.x Web Application Server | 7.0.1038.0 | x | x | x | x |
| JEE Tomcat 6.x Web Application Server | 7.0.1038.0 | x | x | x | x |
| JEE Tomcat 7.x Web Application Server | 7.0.1038.0 | x | x | x | x |
| JEE Tomcat 8.x Web Application Server | 7.0.1038.0 | x | x | x | x |
| JEE Tomcat Web Application Server Library | 7.0.1038.0 | x | x | x | x |
| Microsoft SharePoint 2010 Management Pack Update for SCOM 2012 | 1.0.0.0 | x | x | x | x |
| Microsoft SharePoint 2010 Library | 6.0.4734.1000 | x | x | x | x |
| Microsoft SharePoint Foundation 2010 | 6.0.4734.1000 | x | x | x | x |
| Microsoft SQL Server 2008 (Diagnosis) | 6.3.1.0 | x | x | x | x |
| Microsoft SQL Server 2008 (Monitoring) | 6.3.1.0 | x | x | x | x |
| Microsoft SQL Server 2008 (Discovery) | 6.3.1.0 | x | x | x | x |
| Microsoft SQL Server 2008 Analysis Services (Diagnosis) | 6.3.2.0 | x | x | x | x |
| Microsoft SQL Server 2008 Analysis Services (Monitoring) | 6.3.2.0 | x | x | x | x |
| Microsoft SQL Server 2008 Analysis Services (Presentation) | 6.3.2.0 | x | x | x | x |
| Microsoft SQL Server 2008 Analysis Services (Views) | 6.3.2.0 | x | x | x | x |
| Microsoft SQL Server 2008 Reporting Services (Monitoring, Native Mode) | 6.3.2.0 | x | x | x | x |
| Microsoft SQL Server 2008 Reporting Services (Monitoring, Native Mode) | 6.3.2.0 | x | x | x | x |
| Microsoft SQL Server 2008 Reporting Services (Presentation, Native Mode) | 6.3.2.0 | x | x | x | x |
| Microsoft SQL Server 2008 Reporting Services (Views, Native Mode) | 6.3.2.0 | x | x | x | x |
| Microsoft SQL Server 2011 (Discovery) | 6.3.1.0 | x | x | x | x |
| Microsoft SQL Server 2011 (Monitoring) | 6.3.1.0 | x | x | x | x |
| Microsoft SQL Server 2011 (Presentation) | 6.3.1.0 | x | x | x | x |
| Microsoft SQL Server Core Library | 6.3.1.0 | x | x | x | x |
| Microsoft SQL Server Generic Dashboards | 6.3.2.0 | x | x | x | x |
| Microsoft SQL Server Reporting Services | 6.3.2.0 | x | x | x | x |
| Microsoft SQL Server Visualization Library | 6.3.2.0 | x | x | x | x |
| Microsoft System Center Application Monitoring 360 SLA | 1.0.0.0 | x | x | x | x |
| Microsoft System Center Configuration Manager 2007 | 6.0.6000.0 | x | x | x | x |
| Microsoft Windows Hyper-V 2008 (Discovery) | 6.0.6033.0 | x | x | x | x |
| Microsoft Windows Hyper-V 2008 (Monitoring) | 6.0.6033.0 | x | x | x | x |
| Microsoft Windows Hyper-V 2012 R2 (Discovery) | 7.1.10107.0 | x | x | x | x |
| Microsoft Windows Hyper-V 2012 R2 Monitoring | 7.1.10107.0 | x | x | x | x |
| Microsoft Windows Hyper-V Library | 7.1.10107.0 | x | x | x | x |
| Microsoft Windows Server 2012 Internet Information Services 8 | 7.0.10185.0 | x | x | x | x |
| Microsoft Windows Server Internet Monitoring | 7.0.10185.0 | x | x | x | x |
| Network Management Library | 7.1.10226.0 | x | x | x | x |
| Operations Manager APM Infrastructure | 7.1.10226.0 | x | x | x | x |
| Operations Manager APM Infrastructure Monitoring | 7.1.10226.0 | x | x | x | x |
| Operations Manager APM Library | 7.1.10226.0 | x | x | x | x |
| Operations Manager APM Web Application Resources (ENU) | 7.1.10226.0 | x | x | x | x |
| Operations Manager APM Reports Library | 7.1.10226.0 | x | x | x | x |
| Operations Manager APM WCF Library | 7.1.10226.0 | x | x | x | x |
| Operations Manager APM Web | 7.1.10226.0 | x | x | x | x |
| Operations Manager APM Web Core 2 | 7.1.10226.0 | x | x | x | x |
| Operations Manager APM Web OS 8 | 7.0.8038.0 | x | x | x | x |
| Operations Manager APM Windows Services | 7.1.10226.0 | x | x | x | x |
| Operations Manager Application Monitoring Library | 7.1.10226.0 | x | x | x | x |
| Operations Manager Library | 6.2.1100.0 | x | x | x | x |
| System Center 2012 R2 Data Protection Manager Diagnostic And Monitoring | 4.2.1104.0 | x | x | x | x |
| System Center 2012 R2 Data Protection Manager Library | 4.2.1104.0 | x | x | x | x |
| System Center 2012 R2 Data Protection Manager Scale Out/HA Management Pack | 1.0.0.0 | x | x | x | x |
| System Hardware Library | 7.0.8443.0 | x | x | x | x |
| System Center Core Monitoring Library | 7.0.8443.0 | x | x | x | x |
| UNIX/Linux Core Customizations Library | 7.1.1005.0 | x | x | x | x |
| UNIX/Linux Core Library | 7.0.1005.0 | x | x | x | x |
| UNIX/Linux Log File Monitoring Library | 7.0.1005.0 | x | x | x | x |
| UNIX/Linux Process Monitoring Library | 7.0.1005.0 | x | x | x | x |
| UNIX/Linux Shell Command Library | 7.0.1005.0 | x | x | x | x |
| UNIX/Linux Files Library | 7.0.1005.0 | x | x | x | x |
| Web Application Availability Monitoring Library | 7.1.10226.0 | x | x | x | x |
| Web Application Availability Monitoring Solutions Library Resources (ENU) | 7.1.10226.0 | x | x | x | x |
| Web Application Monitoring Library | 7.1.10226.0 | x | x | x | x |
| Windows Azure Library | 1.0.0.0 | x | x | x | x |
| Windows Azure SQL Database Monitoring | 1.0.4.0 | x | x | x | x |
| Windows Azure SQL Database Utah Monitoring | 1.0.4.0 | x | x | x | x |
| Windows Client Network Discovery | 7.1.10226.0 | x | x | x | x |
| Windows Client Operating Systems Library | 6.0.6729.0 | x | x | x | x |
| Windows Cluster Library | 6.0.7291.0 | x | x | x | x |
| Windows Cluster Management Library | 6.0.7291.0 | x | x | x | x |
| Windows Cluster Management Monitoring | 6.0.7291.0 | x | x | x | x |
| Windows Server 2003 Operating System | 6.0.7230.0 | x | x | x | x |
| Windows Server 2003 Operating System Library | 6.0.7230.0 | x | x | x | x |
| Windows Server 2008 Cluster Management Library | 6.0.7291.0 | x | x | x | x |
| Windows Server 2008 Cluster Management Monitoring | 6.0.7291.0 | x | x | x | x |
| Windows Server 2008 Internet Information Services 7 | 6.0.7909.0 | x | x | x | x |
| Windows Server 2008 Operating System (Discovery) | 6.0.7230.0 | x | x | x | x |
| Windows Server 2008 Operating System (Monitoring) | 6.0.7230.0 | x | x | x | x |
| Windows Server 2008 R2 Best Practice Analysis Monitoring | 6.0.7230.0 | x | x | x | x |
| Windows Server 2012 Cluster Management Library | 6.0.7291.0 | x | x | x | x |
| Windows Server 2012 Cluster Management Monitoring | 6.0.7291.0 | x | x | x | x |
| Windows Server 2012 Operating System (Discovery) | 6.0.7230.0 | x | x | x | x |
| Windows Server 2012 Operating System (Monitoring) | 6.0.7230.0 | x | x | x | x |
| Windows Server 2012 R2 Cluster Management Library | 6.0.7291.0 | x | x | x | x |
| Windows Server 2012 R2 Cluster Management Monitoring | 6.0.7291.0 | x | x | x | x |
| Windows Server 2012 R2 Operating System (Discovery) | 6.0.7230.0 | x | x | x | x |
| Windows Server 2012 R2 Operating System (Monitoring) | 6.0.7230.0 | x | x | x | x |
| Windows Server Cluster Shared Volumes | 7.0.10226.0 | x | x | x | x |
| Windows Server Internet Information Services Library | 7.0.10185.0 | x | x | x | x |
| Windows Server Network Discovery | 7.1.10226.0 | x | x | x | x |
| Windows Server Operating System Library | 6.0.7230.0 | x | x | x | x |
| Windows Server Operating System Reports | 6.0.7230.0 | x | x | x | x |
| Windows Service Library | 7.0.10226.0 | x | x | x | x |

## Standard pro Integraci zpráv z VMWare vCenter do OMU

(použitá na v instanci, na které není možné aplikovat monitoring Intalaci agenta, např. v virtuálních appliancích

Pro jistotu nastavit TTR (time to recovery) na 15min, co třeba (kdybych nezávisely z případně upgrade linuxu, přikazuje nebo odebrané metriky

| Instance | Metrika | Warning | Minor | Major | |
|---|---|---|---|---|---|
| | VM CPU Usage% is above | 75 for 5 min | | | 90 for 5 min |
| | VM Disk Abort/s is above | 10 for 5 min | | | 25 for 5 min |
| | VM Disk Reset is above | 10 for 5 min | | | 25 for 5 min |
| | VM Disk Usage% is equal to | Moderate | High | | |
| | VM Max Total is above | 50 for 5 min | | | 75 for 5 min |
| | VM Memory is above | 75 for 5 min | | | 90 for 5 min |
| | VM Network is above | 1000 for 5 min | | | 3000 for 5 min |
| | VM State is equal to | None | Powered off | | |

**Tabulka - 5 - konfigurace zálohování**
**tuto tabulku používat i pro veškeré změny**
**Tabulka zálohování musí být součástí SP**

| | | |
|---|---|---|
| **Datum poslední aktualizace:** | | *vyplní žadatel* |
| **Datum nasazení změny:** | | *vyplní OSUS* |
| kontaktní aplikační administrátor | | |
| kontaktní databázový administrátor | | |

**Servery**

| Server (hostname) | OS | Typ (DB/AS/Exch/…) | Poznámky |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Databáze**

| SID[1] | RMAN[2] (A/N) | ArchMod[3] (A/N) | Typ[4] (on/off/arch/fs) | Cluster[5] (RAC/SG/No) | Host[6] (VIP/hostname) | PFILE[7] (umiště ní) | Plán[8] (f+t) | Retence[9] | Archivace[10] (F+T) | Poznámky |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

[1] ORACLE_SID

[2] Má být použita integrace pro RMAN (ANO/NE)? Vyžaduje licenci pro integraci DP-RMAN. Integrace DP-RMAN je licencována na server, tj. stačí jedna licence pro zálohu všech databází na jednom serveru. V clusteru je nutné mít samostatnou licenci pro DP-RMAN integraci pro každý server.

[3] Je databáze v archivním módu (ANO/NE)?

[4] Typ zálohy (více viz Dokumentace):

- online/offline/archlog/fs pokud má být využita RMAN integrace
- onlinefs/offlinefs/archlogfs pokud nemá být využita RMAN integrace

[5] Typ clusteru:

- RAC cluster – databázové instance běží v režimu aktiv/aktiv na více serverech v clusteru
- SG – databázová instance běží v režimu aktiv/pasiv vždy na jednom serveru v clusteru
- No – databázová instance běží na single serveru mimo cluster

[6] Host na kterém poslouchá listener pro danou databázi:

- RAC – VIP adresy pro všechny servery v clusteru
- SG – VIP adresa aplikačního balíku pro databázi
- No – hostname serveru

[7] Cesta k PFILE/SPFILU databáze.

[8] **f** – frekvence provádění záloh. Standardně budou zálohy typů online/offline/onlinefs/offlinefs prováděny jedenkrát denně a záloha typu fs bude prováděna 1x týdně (více viz Dokumentace). **t** – čas zálohy. Standardně ji určí administrátor zálohovacího systému (více viz Dokumentace).

[9] Doba po kterou budou data na páskách chráněna. Standardně budou data zálohy typů online/offline/archlog/onlinefs/offlinesfs/archlogfs chráněna 1 týden a data zálohy typu fs budou chráněna 2 týdny (více viz Dokumentace).

[10] F – frekvence odkládání pásek do trezoru. T – doba uložení pásek v trezoru. Standardně nejsou data archivována, tj. pásky zůstávají v knihovně a data jsou na páskách chráněna po dobu uvedenou ve sloupci Retence.

**SAP systém**

| SID[11] | BRTOOLS[12] (A/N) | ArchMod[13] (A/N) | Typ[14] (on/off/arch/fs) | Cluster[15] (SG/No) | Host[16] (VIP/hostname) | Plán[17] (f+t) | Retence[18] | Archivace[19] (F+T) | Poznámky |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

[11] SAPSID

[12] Má být použita integrace pro BRTOOLS (ANO/NE)? Vyžaduje licenci pro integraci DP-BRTOOLS. Integrace DP-BRTOOLS je licencována na server, tj. stačí jedna licence pro zálohu všech SAP systémů na jednom serveru. V clusteru je nutné mít samostatnou licenci pro DP-BROOLS integraci pro každý server.

[13] Je databáze SAP systému v archivním režimu (ANO/NE)?

[14] Typ zálohy (více viz Dokumentace):

- saponline/sapoffline/saparchlog/sapfs pokud má být využita BRTOOLS integrace
- onlinefs/offlinefs/archlogfs pokud nemá být využita BRTOOLS integrace (analogie ke standardní databázové záloze bez využití RMAN integrace)

[15] Typ clusteru:

- SG – SAP systém běží v režimu aktiv/pasiv vždy na jednom serveru v clusteru
- No – SAP systém běží na single serveru mimo cluster

[16] Host na kterém poslouchá listener pro daný SAP systém:

- SG – VIP adresa aplikačního balíku pro SAP systém
- No – hostname serveru

[17] **f** – frekvence provádění záloh. Standardně budou filesystémové zálohy prováděny jedenkrát týdně. **t** – čas zálohy. Standardně ji určí administrátor zálohovacího systému.

[18] Doba po kterou budou data na páskách chráněna. Standardně budou data filesystémových záloh 2 týdny.

[19] F – frekvence odkládání pásek do trezoru. T – doba uložení pásek v trezoru. Standardně nejsou data archivována, tj. pásky zůstávají v knihovně a data jsou na páskách chráněna po dobu uvedenou ve sloupci Retence.

**Exchange**

| Host (VIP/hostname) | Typ[20] (IS/KMS/SRS/SM) | Full/Incr[21] (Full/Incr/Incr1) | Plán[22] (f+t) | Retence[23] | Archivace[24] (F+T) | Poznámky |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

[20] Typ zálohy (více viz Dokumentace):

- IS – záloha Microsoft Information Store
- KMS – záloha Microsoft Key Management Service
- SRS – záloha Microsoft Site Replication Service
- SM – záloha Single Mailboxes

Standardně je prováděna záloha typu IS a jsou zálohovány všechny databáze v daném datastore. V případě že některá má být vynechána, uveďte ji do poznámek. V případě požadavku na zálohu typu SM uveďte vybrané mailboxy do poznámek.

Všechny typy záloh (IS, KMS, SRS a IS) vyžadují licenci pro integraci DP-EXCHANGE. Integrace DP-EXCHANGE je licencována na server, tj. stačí jedna licence pro zálohu všech EXCHANGE systémů na jednom serveru. V clusteru je nutné mít samostatnou licenci pro DP-EXCHANGE integraci pro každý server.

[21] Úrovně záloh (Full/Incremental). Jednotlivé úrovně mají následující význam:

- Full – kompletní záloha
- Incr – inkrementální záloha
- Incr1 – inkrementální záloha úrovně 1

U záloh typu IS, KMS a SRS je standardně prováděna Full záloha. Incr záloha v těchto případech znamená, že budou zálohovány pouze transakční logy.
U zálohy typu SM je standardně prováděna Full záloha. Incr záloha v tomto případě znamená, že budou zálohovány všechny změny v mailboxu od poslední zálohy, Incr1 znamená, že budou zálohovány všechny změny v mailboxu od poslední Full zálohy.

[22] **f** – frekvence provádění záloh. Standardně budou zálohy typů saponline/sapoffline/onlinefs/offlinesfs prováděny jedenkrát denně a záloha typu sapfs bude prováděna 1x týdně. **t** – čas zálohy. Standardně ji určí administrátor zálohovacího systému.

[23] Doba po kterou budou data na páskách chráněna. Standardně budou data filesystémových záloh 2 týdny.

[24] F – frekvence odkládání pásek do trezoru. T – doba uložení pásek v trezoru. Standardně nejsou data archivována, tj. pásky zůstávají v knihovně a data jsou na páskách chráněna po dobu uvedenou ve sloupci Retence.

**Filesystém**

| Host (VIP/hostname) | Filesystém[25] | Full/Incr[26] (Full/Incr/Incr1-9) | Skript[27] (pre/post) | Plán[30] (f+t) | Retence[31] | Archivace[32] (F+T) | Poznámky |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

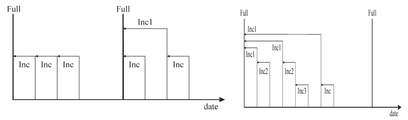
[25] Filesystém který má zálohován. Standardně jsou zálohovány:

- HPUX os – /, /stand, /var - kromě /var/tmp a /var/spool/sockets , /usr, /tmp, /opt, /home a /oracle
- HPUX db – /appl/*, /vzpdata/data/*, /vzpdata/temp/* a /vzpdata/temp/PSi/*
- HPUX as – /lastmp a /app2lwi*
- Linux os – /
- Windows os – C:

[26] Úrovně záloh (Full/Incremental). Jednotlivé úrovně mají následující význam:

- Full – kompletní záloha
- Incr – inkrementální záloha
- Incr1 až Incr9 – inkrementální záloha úrovně 1-9

Incr záloha se vždy vztahuje k poslední provedené záloze. Incr1 záloha se vždy vztahuje k poslední Full záloze, Incr2 záloha se vztahuje k poslední Incr1 záloze atd.
Typy inkrementálních záloh a jejich vzájemná souvislost jsou naznačeny na následujícím obrázku.







**Pre-exec a post-exec skripty**

Prosím, zde vložte aplikační pre-exec a post-exec skripty (např skripty pro mazání starých souborů po jejich záloze, skripty po přepnutí aplikace do 'backup' režimu před její zálohou apod.)

Pre-exec a post-exec skripty které mají být použity před zálohou filesystému.
Standardně nebude použit žádný pre-exec ani post-exec skript. Případný pre-exec a post-exec skript musí dodány aplikací a administrátor zálohovacího systému pouze provede jejich revizi a integraci do DP (více viz Dokumentace).

**Ostatní**

Prosím, zde vložte další informace, které se nevešly do připravených tabulek

**Mimořádná archivace**

Evidence a archivace zdrojových kódů IS VZP ČR - na základě PNUICT0315 - Detailní bezpečnostní politika
přílohy č. 2 - Evidence a archivace zdrojových kódů IS VZP ČR;
http://intranetvzp.vzp.cz/vnitrni_predpisy_2008/metodicke_pokyny/PNUICT0315p02.docx

| | |
|---|---|
| Zdrojový kód k aplikaci | ANO/NE |
| Vlastník zdrojového kódu VZP | ANO/NE |
| Archivace zdrojového kódu umístěna | |
| | |
| | |
| | |
| | |

Prosím, zde vložte další informace o mimořádné archivaci (VIP/hostname, SID, RMAN A/N, ArchMod A/N, Filesystem, atd.).

**Tabulka - 6 - požadavky na diskové kapacity**

**tuto tabulku používat i pro veškeré změny**

**Tabulka diskových kapacit musí být součástí SP**

**řídí se dle pokynu: http://intranetvzp.vzp.cz/u_it/otp/predavaci_otp_tabulky/Postupy%20OTP%20x%20Projektová%20kancelář/Proces%20CaM%20-%20žádosti%20o%20diskové%20kapacity%20v3.pdf**

| Požadavek na diskové kapacity (Disková pole/SAN) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Aplikace | Server | Filesystem | Stávající velikost (GB) | Nová velikost (GB) | Žadatel | Zdůvodnění požadavku | Poznámky | |
| *PUZP* | *h019a52.vzp.cz* | */puzp_appl* | *100* | *200* | *Novák, mobil 731……* | | | *příklad* |
| *IPF* | *d1ipfdb1, d2ipfdb1* | */ipf_data09_new* | | *200* | *Novotný, tel. 2735...* | | *Cluster* | *příklad* |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

# TESTOVACÍ PROSTŘEDÍ

## IDENTIFIKACE APLIKACE - TESTOVACÍ /ŠKOLÍCÍ PROSTŘEDÍ

| Název aplikce |
| --- |
| |

| Zkratka názvu aplikace |
| --- |
| |

| Jméno projektového managera |
| --- |
| |

| Datum |
| --- |
| |

| | |
| --- | --- |
| správce aplikace v testovacím prostředí | |
| administrátor aplikace v testovacím prostředí | |
| administrátor databáze testovacího prostředí | |
| administrátor operačního systému testovacího prostředí | |
| administrátor sítí testovacího prostředí | |
| administrátor monitoringu testovacího prostředí | |

*pokud je monitoring v testovacím prostředí vyžadován??*

## Tabulka - 2 - vytvoření testovacího prostředí pro aplikaci

| Požadované licence (db i apl) | | |
|---|---|---|
| druh databáze, verze | | |
| počet a druh databázových licencí (včetně options) | | *Př. ODI pro 4CPU, Partitioning, RAC, BPEL, BI suite pro 8CPU apod.* |
| Počet a druh licencí aplikačního serveru | | |
| odhadovaný počet uživatelů používajících aplikaci | | |
| termín, ke kterému mají být licence k dispozici | | |
| **počet a typ dalších nutných licencí** | | |
| **Smlouva k nákupu licencí** | | *hypertoxtový odkaz přímo na poažadovaný dokument* |
| **počet a typ nutných certifikátů** | | |

| Aplikační a Databázový systém Oracle | | |
|---|---|---|
| typ a verze použitého/tých aplikačního/ních serverů | | *př. WLS 11g - Forms a reports,* |
| verze databáze Oracle | | *! 11gR2 a vyšší verze, dlestandardů IT VZP ČR* |
| vždy definovat hodnoty inicializačních parametrů dB: | | |
| instance_name (SID) | | |
| code page (inicializační kódová stránka dB - nelze měnit) | | default ve VZP=EE8ISO8859P2 |
| sga_target | | |
| sga_max_size | | |
| processes | | |
| job_queue_processes | | |
| aq_tm_processes | | |
| názvy schémat (uživatelů-vlastníků objektů) a jejich minimální dB grants (výčet) | | mimo zde uvedená schémata nebude mít databáze jiné vlastníky objektů |
| výčet jmen dalších potřebných servisních účtů aplikace | | mimo zde uvedená jména nebude mít aplikace v databázi žádné uživatelské/servisní účty |
| další parametry, kde nevyhovují defaultní hodnoty | | |

| | |
|---|---|
| **Diskové prostory pro ORACLE** | |
| **Aplikační server** | |
| velikost dačasného pracovního prostoru pro Forms a Reports (iastmp) | |
| /app13w (v GB), adresář pro aplikační moduly | |

| | | |
|---|---|---|
| **Databázový server** | | |
| /app1, aplikační data | | |
| //vzp.data, aplikační data | | *datové soubory, se kterými aplikace pracuje a ukládá na Filesystémy* |
| Inicializační velikost tablespaců | | |
| 1) data+indexy (celkem) | | |
| 2) temporary | | |
| 3) undo | | |

| Systém Windows prostředí | | Vyplňovat v případě Windows prostředí |
|---|---|---|
| **Komunikace s AD** | | *Uvést DC, s kterými bude probíhat komunikace* |
| LDAP dotaz | | |
| **Aplikační server** | | |
| operační systém přesná specifikace | | |
| systémový disk (GB) | | |
| datový disk/y (GB) | | |
| požadavky na SW | | |
| **Databázový server** | | |
| databázový systém MS SQL - přesná specifikace | | |
| inicializační velikost databází | | |
| data (GB) | | |
| transakční logy (GB) | | |

| Hardware | |
|---|---|
| počet reálných HW serverů | |
| počet virtuálních serverů | |
| operační systém (jsou-li různé - přiřaďte k jednotl. serverům) | |
| odhadnutý požadovaný výkon - počet procesorů/počet jader v procesoru | |
| odhadnutá velikost paměti | |
| odhadnuté prostory na discích - lokálně/na SAN v GB | |
| odhadnuté kapacity zálohovaných dat v GB | |

| Hardware - typy serverů | | |
|---|---|---|
| **Typ serveru 1**, model, název provozované aplikace nebo služby | | *test* |
| umístění v TVS1-n | | |
| Operační systém a jeho verze | | |
| počet jader v procesoru | | |
| RAM - spotřeba pro všechny procesy aplikace včetně dB a OS | | |

| | | |
|---|---|---|
| **Typ serveru 2**, model, název provozované aplikace nebo služby | | *test* |
| umístění v TVS1-n | | |
| Operační systém a jeho verze | | |
| počet jader v procesoru | | |
| RAM - spotřeba pro všechny procesy aplikace včetně dB a OS | | |

| | | |
|---|---|---|
| **Typ serveru 3**, model, název provozované aplikace nebo služby | | *školící* |
| umístění v TVS1-n | | |
| Operační systém a jeho verze | | |
| počet jader v procesoru | | |
| RAM - spotřeba pro všechny procesy aplikace včetně dB a OS | | |

| | | |
|---|---|---|
| **Typ serveru 4**, model, název provozované aplikace nebo služby | | *školící* |
| umístění v TVS1-n | | |
| Operační systém a jeho verze | | |
| počet jader v procesoru | | |
| RAM - spotřeba pro všechny procesy aplikace včetně dB a OS | | |

| Ostatní software | |
|---|---|
| název software, verze | |
| využití tiskového subsystému **ANO - NE** | |

| Dokumentace | | |
|---|---|---|
| datový model - popis obsahující řešení v testovacím prostředí | | *hypertoxtový odkaz přímo na poažadovaný dokument* |
| datový model - popis obsahující řešení školícího prostředí | | *hypertoxtový odkaz přímo na poažadovaný dokument* |

| | 1 | 2 | 3 | 4 | | 5 | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | |
| **ID jméno serveru** | | | | | | | | | | | | | | | | | | | | |
| Vrstva | | | | | | | | | | | | | | | | | | | | |
| Prostředí | | | | | | | | | | | | | | | | | | | | |
| Operační systém | | | | | | | | | | | | | | | | | | | | |
| Aplikační blok | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| **Lokální aplikace** | | | | | | | | | | | | | | | | | | | | |
| Název aplikace | Stickiness | Keepalive URL | Protokol | Porty | URI | FQDN | Sezení (čas v sec) | Zdroj. IP adresy (odkud se komunikuje) | Nestandardní požadavky | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| **Komunikační toky** | | | | | | | | | | | | | | | | | | | | |
| Název lokální aplikace | Cílový prvek | Protokoly | Porty | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| **Konfigurace serveru** | **ILO** | **lan0** | | | | | | | | | | | | | | | | | | |
| DNS jméno | | | | | | | | | | | | | | | | | | | | |
| IP adresa | | | | | | | | | | | | | | | | | | | | |
| ILO - DNS alias | | | | | | | | | | | | | | | | | | | | |
| ILO - password | | | | | | | | | | | | | | | | | | | | |
| maska | | | | | | | | | | | | | | | | | | | | |
| gateway | | | | | | | | | | | | | | | | | | | | |
| MAC | | | | | | | | | | | | | | | | | | | | |
| ID VLAN | | | | | | | | | | | | | | | | | | | | |
| switch | | | | | | | | | | | | | | | | | | | | |
| Port switche | | | | | | | | | | | | | | | | | | | | |
| DNS server (do resolv.conf) | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| Interface: | | | | | | | | | | | | | | | | | | | | |
| lan n | lan1 | lan2 | lan3 | | | | | | | | | | | | | | | | | |
| DNS název | | | | | | | | | | | | | | | | | | | | |
| způsob konfigurace | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| IP Adresa | | | | | | | | | | | | | | | | | | | | |
| maska | | | | | | | | | | | | | | | | | | | | |
| Gateway | | | | | | | | | | | | | | | | | | | | |
| VLAN ID | | | | | | | | | | | | | | | | | | | | |
| MAC | | | | | | | | | | | | | | | | | | | | |
| Port switche | | | | | | | | | | | | | | | | | | | | |
| Switch | | | | | | | | | | | | | | | | | | | | |

| | 1 | 2 | 3 | 4 | 5 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | |
| **Hostname serveru** | | | | | | | | | | | | | | | | |
| ID fyzického serveru | | | | | | | | | | | | | | | | |
| ID virtuálního serveru | | | | | | | | | | | | | | | | |
| Vrstva | | | | | | | | | | | | | | | | |
| Prostředí (TVS1-TVS6) | | | | | | | | | | | | | | | | |
| Aplikace | | | | | | | | | | | | | | | | |
| Operační systém | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| **Lokální aplikace** | | | | | | | | | | | | | | | | |
| Název aplikace | Stickiness | Keepalive URL | Protokol | Porty | Sezení (čas v sec) | Nestandardní požadavky | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| **Komunikační toky** | | | | | | | | | | | | | | | | |
| Název lokální aplikace | Cílový prvek | Protokol | Porty | | | Poznámka | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | |

# Monitorování testovacího prostředí aplikace - pouze v případě požadavku

## Oracle infrastruktura

| Host/Instance/Cluster | Jméno instance | Typ | Notifikační pravidlo v OEM |
|---|---|---|---|

## Obecné zadání monitoringu

(popis polí naleznete pod tabulkou, standardy monitoringu UNIX a Windows OS jsou popsány ještě níže)

| | Zdroj | | | | Metrika | | | | | Zpracování | | | | | | | | Service Oriented Architecture | | | | Ostatní | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100 | 110 | 120 | 130 | 140 | 150 | 160 | 170 | 180 | 190 | 200 | 210 | 220 | 230 | 240 |
| **ID** | Host / Instance | Popis / typ instance | **Typ objektu, popis** | **Sledovaný objekt** | **Název metriky** | **Operátor** | **Hodnota (prahová hodnota)** | **Interval sledování** | **Popis sledované události** | **Závažnost** | Kvantitativní korelace / deduplikace | Zpracování, korelace | **Instrukce** | Automatická akce | Operátorem inicivaná akce | **Eskalace (komu)** | **Notifikace (jak)** | **Aplikace** | Služba | Nadřazená služba | Přenos závažnosti | Podmínky sledování | Poznámky |
| | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | |

### Popis vyplňovaných polí
**(Rozbalit skryté řádky)**

| | | |
|---|---|---|
| **10** | ID | Jednoznačná identifikace monitorované události v rámci tabulky (listu). Doporučuje se číslování s větším krokem, aby bylo možno v budoucnu ukládat další záznamy. |
| 20 | Host / Instance | FQDN serveru, případně jednoznačné jméno instance (u clusterů) |
| 30 | Popis / typ instance | Upřesnění instance vzhledem ke sledované události, tedy např. Server+OS+verze, router, UPS+typ, Oracle DB, Oracle Cluster DB, HTTP Server, Listener apod. |
| **40** | **Typ objektu, popis** | Uveďte typ sledovaného objektu, zda se jedná o proces, logfile, uživatelskou metriku, tablespace, URL, LDAP server apod. |
| **50** | **Sledovaný objekt** | Klíčové pole tabulky - uveďte jednoznačně sledovaný objekt, tj. log (s celou cestou), název tablespace, jednoznačný název listeneru, OID MIB, URL, název procesu, případně uveďte celý SQL |
| **60** | **Název metriky** | Specifikuje sledovanou hodnotu nebo způsob jejího získání, např. "Tablespace Space Used %", "UPSDOWN Status", textová šablona (filtr) apod. |
| **70** | **Operátor** | Matematický, logický nebo jiný operátor pro porovnání sledované hodnoty s prahovou hodnotou , např. "=", "<", ">", "<>", obsahuje, NEobsahuje,… |
| **80** | **Hodnota (prahová hodnota)** | Uveďte porovnávanou/sledovanou hodnotu, tj. číslo, procenta, čas, hledaný řetězec,… |
| **90** | **Interval sledování** | Jak často má být hodnota přečtena (např. 30 sec, 5 min) |
| **100** | **Popis sledované události** | vysvětlující text (max 80 znaků) |
| **110** | **Závažnost** | Specifikuje míru dopadu na dostupnost služby; detailní popis následuje pod tabulkou |
| 120 | Kvantitativní korelace / deduplikace | Některou událost není nutné zpracovávat při každém výskytu, protože není tolik závažná. Kritickou se ale může stát v případě častějšího opakování. Např. >10 výskytů za 30 minut. -zde uveďte kvantitativní parametry, které přispějí uvedenou závažnost události |
| 130 | Zpracování, korelace | Některou událost není nutné zpracovávat při každém výskytu, protože není tolik závažná. Kritickou se ale může stát v případě vazby na jiné události -zde uveďte vazby, které přispějí uvedenou |
| **140** | **Instrukce** | Pokyny pro operátora a/nebo helfdeře, které určí postup odstranění incidentu nebo provedou detailnější diagnostiku (kontrola, spuštění skriptu, apod.) |
| 150 | Automatická akce | Např. spustit diagnostický script, restart služby apod. - bude provedené automaticky agentem HPOV |
| 160 | Operátorem inicivaná akce | Jako automatická, ale potvrzená operátorem - např. spustit diagnostický script, restart služby apod. - bude provedeno automaticky agentem HPOV |
| **170** | **Eskalace (komu)** | Adresát (role), komu operátor předá k řešení. |
| **180** | **Notifikace (jak)** | Uveďte seznam způsobů eskalace v požadovaném pořadí (mail - telefon - SD). Standardně bude předáváno operátorem, v odůvodněných případech lze žádat přímou automatickou |
| **190** | **Aplikace** | Funkční celek, poskytující službu nebo více služeb; uveďte všechny aplikace, které událost ovlivňuje |
| 200 | Služba | Jednoznačný identifikátor služby v SOA architektuře v rámci projektu |
| 210 | Nadřazená (závislá) služba | Zde se definují závislosti služeb pro tvorbu servisního stromu |
| 220 | Přenos závažnosti | Jakým způsobem ovlivňuje stav služby nadřazenou službu. Je možno definovat poměrem (1/1, 1/2,..) nebo procenty (100 %, 50 %, ...), případně zvýšením závažnosti (+1 = zvýšit závažnost, - |
| 230 | Podmínky sledování | Uveďte podřetězi certifikátu, uživatelských přístupů, síťových prostupů, umístění sledovacích zařízení v síťových segmentech apod., tedy všechny nadstandardní podmínky, které jsou nutné k |
| 240 | Poznámky | Zde uveďte vše podstatné, co nebylo možno vyplnit do definovaných polí |

### Popis závažnosti (severities)

| | |
|---|---|
| Critical | závažná chyba způsobující nedostupnost aplikace nebo stav, který bez zásahu povede nutně k nedostupnosti |
| Major | závažná chyba způsobující dílčí nefunkčnost nebo snížení výkonu aplikace |
| Minor | dílčí chyba nezpůsobující nedostupnost |
| Warning | událost vyžadující optimalizaci, která neomezuje chod aplikace |
| Normal | očekávaný stav nebo návrat do plně funkčního stavu |

### Standardní monitoring HP-UX serverů

**Základní sada templates pro monitoring UNIX serverů**

| Template | | FQDN serverů | | | | |
|---|---|---|---|---|---|---|
| | | | | | | |
| V2P_OS_HPUX_MCSG1119 | /var/adm/syslog/syslog.log | x | x | x | x | x |
| V2P_OS_HPUX-BadLogins | /var/adm/btmp logfile | x | x | x | x | x |
| V2P_OS_HPUX-BootLog | /etc/rc.log logfile | x | x | x | x | x |
| V2P_OS_HPUX-CronLog | /var/adm/cronlog | x | x | x | x | x |
| V2P_OS_HPUX-Dmesg | /sbin/dmesg | x | x | x | x | x |
| V2P_OS_HPUX-Logins | /var/adm/wtmp | x | x | x | x | x |
| V2P_OS_HPUX-Sulog | /var/adm/sulog | x | x | x | x | x |
| V2P_OS_HPUX-Syslog | /var/adm/syslog/syslog.log | x | x | x | x | x |
| V2P_OS_HPUX-Veritas | /var/vxvm/vxconfigd.log | x | x | x | x | x |
| V2P_OS_EMS-events | EMS Event Notification | x | x | x | x | x |
| Monitoring filesystému /arch | Meze: 75%-Warning, 80%-Minor, 85%-Major, 90%-Critical | x | x | x | x | x |
| Monitoring filesystému /oracle | Meze: 90%-Major, 93%-Critical | x | x | x | x | x |
| Monitoring filesystému /stand | Meze: 50%-Major, 70%-Critical | x | x | x | x | x |
| Monitoring filesystému /opt | Meze: 95%-Major, 98%-Critical | x | x | x | x | x |
| Monitoring filesystému - ostatní | Meze: 80%-Major, 90%-Critical | x | x | x | x | x |
| Monitoring procesů | cron | x | x | x | x | x |
| | inetd | x | x | x | x | x |
| | Mail | x | x | x | x | x |
| | NTP | x | x | x | x | x |
| | Print | x | x | x | x | x |
| | syslog | x | x | x | x | x |

**Výkonnostní parametry (CODA)**

| | | | | | | |
|---|---|---|---|---|---|---|
| GBL_CPU_TOTAL_UTIL | % využití CPU | x | x | x | x | x |
| BYDSK_UTIL | % využití času IO operace HD | x | x | x | x | x |
| TBL_FILE_TABLE_UTIL | % využití tabulky otevřených souborů | x | x | x | x | x |
| GBL_MEM_PAGEOUT_RATE | počet stránek na disk za sekundu | x | x | x | x | x |
| TBL_MSG_TABLE_UTIL | % front momentálně v užívání | x | x | x | x | x |
| GBL_NET_COLLISION_RATE | počet kolizí za sekundu ve všech síťových interface | x | x | x | x | x |
| BYNETIF_ERROR | počet chyb vzniklých na rozhraní během intervalu | x | x | x | x | x |
| TBL_PROC_TABLE_UTIL | % aktivních procesů v tab. procesů | x | x | x | x | x |
| TBL_SEM_TABLE_UTIL | % semaforů momentálně v užívání | x | x | x | x | x |
| TBL_SHMEM_TABLE_UTIL | % segmentů sdílené paměti momentálně v užívání | x | x | x | x | x |
| GBL_SWAP_SPACE_UTIL | % swapovaného prostoru k dispozici | x | x | x | x | x |

### Standardní monitoring Windows serverů

**Seznam instalovaných management packů**

| Management Pack | Verze | FQDN serverů | | | | |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Active Directory Server 2000 (Discovery) | 6.0.7065.0 | x | x | x | x | x |
| Active Directory Server 2000 (Monitoring) | 6.0.7065.0 | x | x | x | x | x |
| Active Directory Server 2003 (Discovery) | 6.0.7065.0 | x | x | x | x | x |
| Active Directory Server 2003 (Monitoring) | 6.0.7065.0 | x | x | x | x | x |
| Active Directory Server 2008 (Discovery) | 6.0.7065.0 | x | x | x | x | x |
| Active Directory Server 2008 (Monitoring) | 6.0.7065.0 | x | x | x | x | x |
| Active Directory Server Client (Monitoring) | 6.0.7065.0 | x | x | x | x | x |
| Active Directory Server Common Library | 6.0.7065.0 | x | x | x | x | x |
| Hewlett-Packard Integrity Servers Base | 1.0.33.0 | x | x | x | x | x |
| Hewlett-Packard Integrity Servers SNMP Management Pack | 1.0.33.0 | x | x | x | x | x |
| Hewlett-Packard ProLiant Servers Base | 1.2.1.0 | x | x | x | x | x |
| Hewlett-Packard ProLiant Servers SNMP Management Pack | 1.1.0.0 | x | x | x | x | x |
| Hewlett-Packard Servers Core Library | 1.0.33.0 | x | x | x | x | x |
| SQL Server 2005 (Discovery) | 6.0.6648.0 | x | x | x | x | x |
| SQL Server 2005 (Monitoring) | 6.0.6648.0 | x | x | x | x | x |
| SQL Server 2008 (Discovery) | 6.0.6648.0 | x | x | x | x | x |
| SQL Server 2008 (Monitoring) | 6.0.6648.0 | x | x | x | x | x |
| SQL Server Core Library | 6.0.6648.0 | x | x | x | x | x |
| Windows Cluster Management Library | 6.0.6720.0 | x | x | x | x | x |
| Windows Cluster Management Monitoring | 6.0.6720.0 | x | x | x | x | x |
| Windows 2003 Cluster Management Library | 6.0.6720.0 | x | x | x | x | x |
| Windows 2003 Cluster Management Monitoring | 6.0.6720.0 | x | x | x | x | x |
| Windows Server 2008 Cluster Management Library | 6.0.6720.0 | x | x | x | x | x |
| Windows Server 2008 Cluster Management Monitoring | 6.0.6720.0 | x | x | x | x | x |
| Windows Server Operating System Library | 6.0.6667.0 | x | x | x | x | x |
| Windows Server 2000 Operating System | 6.0.6667.0 | x | x | x | x | x |
| Windows Server 2003 Operating System | 6.0.6667.0 | x | x | x | x | x |
| Windows Server 2008 Operating System (Discovery) | 6.0.6667.0 | x | x | x | x | x |
| Windows Server 2008 Operating System (Monitoring) | 6.0.6667.0 | x | x | x | x | x |
| Windows Server Internet Information Services 2000 | 6.0.6539.0 | x | x | x | x | x |
| Windows Server Internet Information Services 2003 | 6.0.6539.0 | x | x | x | x | x |
| Windows Server Internet Information Services Library | 6.0.6539.0 | x | x | x | x | x |
| Windows Server Print Server 2000 and 2003 Management Pack | 6.0.6392.0 | x | x | x | x | x |
| Windows Server Print Server 2008 Management Pack | 6.0.6392.0 | x | x | x | x | x |
| Windows Server Print Server Library Management Pack | 6.0.6392.0 | x | x | x | x | x |

## Tabulka - 4 - konfigurace zálohování testovacího prostředí

### Servery v testovacím prostředí

| + hostname (jednoznačná identifikace) | OS | Typ (DB/AS/Exch/…) | Poznámky |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

### Databáze testovacího prostředí

| SID[1] | RMAN[2] (A/N) | ArchMód[3] (A/N) | Typ[4] (on/off/arch/fs) | Cluster[5] (RAC/SG/No) | Host[6] (VIP/hostname) | PFILE/SPFILE[7] (umístění) | Plán[8] (f+t) | Retence[9] | Archivace[10] (F+T) | Poznámky |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

[1] ORACLE_SID
[2] Má být použita integrace pro RMAN (ANO/NE)? Vyžaduje licenci pro integraci DP-RMAN. Integrace DP-RMAN je licencována na server, tj. stačí jedna licence pro zálohu všech databází na jednom serveru. V clusteru je nutné mít samostatnou licenci pro DP-RMAN integraci pro každý server.
[3] Je databáze v archivním módu (ANO/NE)?
[4] Typ zálohy (více viz Dokumentace):

- online/offline/archlog/fs pokud má být využita RMAN integrace
- onlinefs/offlinefs/archlogfs pokud nemá být využita RMAN integrace

[5] Typ clusteru:

- RAC cluster – databázové instance běží v režimu aktiv/aktiv na více serverech v clusteru
- SG – databázová instance běží v režimu aktiv/pasiv vždy na jednom serveru v clusteru
- No – databázová instance běží na single serveru mimo cluster

[6] Host na kterém poslouchá listener pro danou databázi:

- RAC – VIP adresy pro všechny servery v clusteru
- SG – VIP adresa aplikačního balíku pro databázi
- No – hostname serveru

[7] Cesta k PFILU/SPFILU databáze.

[8] **f** – frekvence provádění záloh. Standardně budou zálohy typů online/offline/onlinefs/offlinefs prováděny jedenkrát denně a záloha typu fs bude prováděna 1x týdně (více viz Dokumentace). **t** – čas zálohy. Standardně ji určí administrátor zálohovacího systému (více viz Dokumentace).

[9] Doba po kterou budou data na páskách chráněna. Standardně budou data záloh typů online/offline/archlog/onlinefs/offlinesfs/archlogfs chráněna 1 týden a data zálohy typu fs budou chráněna 2 týdny (více viz Dokumentace).

[10] **F** – frekvence odkládání pásek do trezoru. **T** – doba uložení pásek v trezoru. Standardně nejsou data archivována, tj. pásky zůstávají v knihovně a data jsou na páskách chráněna po dobu uvedenou ve sloupci Retence.

### SAP systém testovacího prostředí

| SID[11] | BRTOOLS[12] (A/N) | ArchMód[13] (A/N) | Typ[14] (on/off/arch/fs) | Cluster[15] (SG/No) | Host[16] (VIP/hostname) | Plán[17] (f+t) | Retence[18] | Archivace[19] (F+T) | Poznámky |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

[11] SAPSID

[12] Má být použita integrace pro BRTOOLS (ANO/NE)? Vyžaduje licenci pro integraci DP-BRTOOLS. Integrace DP-BRTOOLS je licencována na server, tj. stačí jedna licence pro zálohu všech SAP systémů na jednom serveru. V clusteru je nutné mít samostatnou licenci pro DP-BROOLS integraci pro každý server.

[13] Je databáze SAP systému v archivním režimu (ANO/NE)?
[14] Typ zálohy (více viz Dokumentace):

- saponline/sapoffline/saparchlog/sapfs pokud má být využita BRTOOLS integrace
- onlinefs/offlinefs/archlogfs pokud nemá být využita BRTOOLS integrace (analogie ke standardní databázové záloze bez využití RMAN integrace)

[15] Typ clusteru:

- SG – SAP systém běží v režimu aktiv/pasiv vždy na jednom serveru v clusteru
- No – SAP systém běží na single serveru mimo cluster

[16] Host na kterém poslouchá listener pro daný SAP systém:

- SG – VIP adresa aplikačního balíku pro SAP systém
- No – hostname serveru

[17] **f** – frekvence provádění záloh. Standardně budou filesystémové zálohy prováděny jedenkrát týdně. **t** – čas zálohy. Standardně ji určí administrátor zálohovacího systému.

[18] Doba po kterou budou data na páskách chráněna. Standardně budou data filesystémových záloh 2 týdny.

[19] **F** – frekvence odkládání pásek do trezoru. **T** – doba uložení pásek v trezoru. Standardně nejsou data archivována, tj. pásky zůstávají v knihovně a data jsou na páskách chráněna po dobu uvedenou ve sloupci Retence.

### Exchange testovacího prostředí

| Host (VIP/hostname) | Typ[20] (IS/KMS/SRS/SM) | Full/Incr[21] (Full/Incr/Incr1) | Plán[22] (f+t) | Retence[23] | Archivace[24] (F+T) | Poznámky |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

[20] Typ zálohy (více viz Dokumentace):

- IS – záloha Microsoft Information Store
- KMS – záloha Microsoft Key Management Service
- SRS – záloha Microsoft Site Replication Service
- SM – záloha Single Mailboxes

Standardně je prováděna záloha typu IS a jsou zálohovány všechny databáze v daném datastore. V případě že některá má být vynechána, uveďte ji do poznámek.
V případě požadavku na zálohu typu SM uveďte vybrané mailboxy do poznámek.

Všechny typy záloh (IS, KMS, SRS a IS) vyžadují licenci pro integraci DP-EXCHANGE. Integrace DP-EXCHANGE je licencována na server, tj. stačí jedna licence pro zálohu všech EXCHANGE systémů na jednom serveru. V clusteru je nutné mít samostatnou licenci pro DP-EXCHANGE integraci pro každý server.
[21] Úrovně záloh (Full/Incremental). Jednotlivé úrovně mají následující význam:

- Full – kompletní záloha
- Incr – inkrementální záloha
- Incr1 – inkrementální záloha úrovně 1

U zálohy typu IS, KMS a SRS je standardně provadena Full zaloha. Incr zaloha v těchto pripadech znamena, ze budou zálohovány pouze transakční logy.
U zalohy typu SM je standardne provadena Full zaloha. Incr zaloha v tomto pripade znamena, ze budou zalohovany všechny změny v mailboxu od poslední zálohy, Incr1 znamená, že budou zálohovány všechny změny v mailboxu od poslední Full zálohy.

[22] **f** – frekvence provádění záloh. Standardně budou zálohy typu saponline/sapoffline/onlinefs/offlinesfs prováděny jedenkrát denně a záloha typu sapfs bude prováděna 1x týdně. **t** – čas zálohy. Standardně ji určí administrátor zálohovacího systému.
[23] Doba po kterou budou data na páskách chráněna. Standardně budou data záloh typů online/offline/archlog/onlinefs/offlinesfs/archlogfs chráněna 1 týden a data zálohy typu fs budou chráněna 2 týdny.

[24] **F** – frekvence odkládání pásek do trezoru. **T** – doba uložení pásek v trezoru. Standardně nejsou data archivována, tj. pásky zůstávají v knihovně a data jsou na páskách chráněna po dobu uvedenou ve sloupci Retence.

### Filesystém testovacího prostředí

| Host (VIP/hostname) | Filesystém[25] | Full/Incr[26] (Full/Incr/Incr1-9) | Skript[27] (pre/post) | Plán[30] (f+t) | Retence[31] | Archivace[32] (F+T) | Poznámky |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

[25] Filesystém který má zálohován. Standardně jsou zálohovány:

- HPUX os – /, /stand, /var - kromě /var/tmp a /var/spool/sockets , /usr, /tmp, /opt, /home a /oracle
- HPUX db – /appli*, /vzpdata/data/*, /vzpdata/temp/* a /vzpdata/temp/PSi/*
- HPUX as – /astmp a /appli3w/*
- Linux os – /
- Windows os – C:

[26] Úrovně záloh (Full/Incremental). Jednotlivé úrovně mají následující význam:

- Full – kompletní záloha
- Incr – inkrementální záloha
- Incr1 až Incr9 – inkrementální záloha úrovně 1-9

Incr záloha se vždy vztahuje k poslední provedené záloze. Incr1 záloha se vždy vztahuje k poslední Full záloze, Incr2 záloha se vztahuje k poslední Incr1 záloze atd. Typy inkrementálních záloh a jejich vzájemná souvislost jsou naznačeny na následujícím obrázku.

### Pre-exec a post-exec skripty

| |
|---|
| Prosím, zde vložte aplikační pre-exec a post-exec skripty (např.skripty pro mazání starých souborů po jejich záloze, |
| skripty po přepnutí aplikace do 'backup' režimu před její zálohou apod.) |
| |
| |

Pre-exec a post-exec skripty které mají být použity před zálohou filesystému.
Standardně nebude použit žádný pre-exec ani post-exec skript. Případný pre-exec a post-exec skript musí dodány aplikací a administrátor zálohovacího systému pouze provede jejich revizi a integraci do DP (více viz Dokumentace).

### Ostatní

| |
|---|
| Prosím, zde vložte další informace, které se nevešly do připravených tabulek |
| |
| |

| | |
|---|---|
| kontaktní aplikační administrátor | |
| kontaktní databázový administrátor | |

**Tabulka - 5 - požadavky pro testovací prostředí na diskové kapacity**
**tuto tabulku používat i pro veškeré změny v testovacím prostředí**

**Požadavek na diskové kapacity (Disková pole/SAN)**

| Aplikace | Server | Filesystem | Stávající velikost (GB) | Nová velikost (GB) | Žadatel | Poznámky | | |
|---|---|---|---|---|---|---|---|---|
| *PUZP* | *h019a52.vzp.cz* | */puzp_appl* | *100* | *200* | *Novák, mobil 731……* | | *příklad* | TESTOVACÍ |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

| Aplikace | Server | Filesystem | Stávající velikost (GB) | Nová velikost (GB) | Žadatel | Poznámky | | |
|---|---|---|---|---|---|---|---|---|
| *PUZP* | *h019a52.vzp.cz* | */puzp_appl* | *100* | *200* | *Novák, mobil 731……* | | *příklad* | ŠKOLÍCÍ |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |