Univerzita Pardubice

Fakulta ekonomicko-správní

Efektivní monitoring databáze pro zvýšení výkonnosti IS

Ondřej Šprync

Bakalářská práce

2010

Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky
Akademický rok: **2009/2010**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Ondřej ŠPRYNC**

Studijní program: **B6209 Systémové inženýrství a informatika**

Studijní obor: **Informatika ve veřejné správě**

Název tématu: **Efektivní monitoring databáze pro zvýšení výkonnosti IS**

Zásady pro vypracování:

Cílem práce je nakonfigurovat monitoring databáze tak, aby správce IS získal rychlý přehled důležitých informací, které by vedly k efektivnímu řešení kritických situací IS

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 40 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

SCHMIDT, K. *High Availability and Disaster Recovery: Concepts, Design, Implementation.* **Berlin: Springer, 2006. 410 s. ISBN 3-540-24460-3.**

BACKMAN, A. *OpenEdge Revealed: Mastering the OpenEdge Database with OpenEdge Management.* **[s.l.]: Progress Software Corporation, 2008. 266 s. ISBN 0-923562-08-7.**

BASL, J., BLAŽÍČEK, R. *Podnikové informační systémy: Podnik v informační společnosti.* **2. přeprac. vyd. [s.l.]: Grada Publishing, a.s., 2007. 288 s. ISBN 978-80-247-2279-5.**

MERRETT, D. *OpenEdge Revealed: Achieving Server Control with OpenEdge Management.* **OpenEdge Management [online]. Dostupný z WWW: <http://communities.progress.com/pcom/servlet/JiveServlet/download/10341-2-9815/asc.pdf>.**

Šimonová

Vedoucí bakalářské práce: **Ing. Stanislava Šimonová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **30. dubna 2010**

Termín odevzdání bakalářské práce: **30. dubna 2010**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

doc. Ing. Jiří Křupka, Ph.D.
vedoucí ústavu

V Pardubicích dne 5. října 2009

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 23. 06. 2010

Ondřej Šprync

Poděkování

Rád bych poděkoval vedoucí práce Ing. Stanislavě Šimonové, Ph.D. za ochotu, trpělivost a za všechny cenné rady a připomínky při zpracování této bakalářské práce. Také bych chtěl poděkovat mé rodině a kolegům za podporu během studia.

Anotace

Bakalářská práce se zaměřuje na návrh efektivního monitoringu databáze informačního systému pomocí modelování a ověření tohoto návrhu v reálném provozu s použitím nástroje OpenEdge Management. Dále se zabývá problematikou dostupnosti informačního systému a plánováním, jak předcházet výpadkům byznys procesů a informačních a komunikačních technologií.

Klíčová slova

Monitoring, sledovaný zdroj, informační systém, výpadek, dostupnost, plánování, outsourcing, návrh, model.

Title

Efficacious monitoring of IS

Annotation

Bachelor thesis focuses on designing an effective database monitoring of an information system. The objective is realized through modelling and designing the verification method of real operation by the use of OpenEdge Management tool. Among others, the work deals with issues of information system availability and planning how to avoid outages of business processes and information and communication technologies.

Keywords

Monitoring, monitored resource, information systém, outage, availability, outsourcing, concept, model.

Obsah

Seznam použitých zkratek

AI	After-Image
BCP	Business continuity planning
BI	Before-Image
BS	British Standard
CPU	Central Processing Unit
ČSN	Česká státní norma
DBMS	Database management system
DRP	Disaster recovery planning
GB	Gigabyte
HP	Hewlett Packard
HTTP	Hypertext Transfer Protocol
HW	Hardware
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IS	Informační systém
ISO	International Organization for Standardization
MS	Microsoft
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
OE	OpenEdge
OEM	OpenEdge Management
PING	Packet InterNet Groper
RAS	Reliability, Availability, Serviceability
SLA	Service Level Agreement
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SW	Software
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UUID	Universal Unique Identifier

Seznam obrázků

Seznam tabulek

Seznam příloh

1. Úvod

Investice do informačních a komunikačních technologií (dále jen ICT) se stále zvyšují, neboť neustále rostoucí náročnost koncových uživatelů, globální konkurence a vznik nových trhů kladou stále vyšší důraz na kvalitu informací. Dochází také k nárůstu uživatelských požadavků kladených na informační systémy (dále jen IS). Požadavky se ale zdaleka netýkají pouze nových služeb a maximalizace výkonů. Stále větší důraz je kladen také na stabilitu a dostupnost systémů. Proto se vedle uživatelských aplikací prosazují na trhu další softwarové nástroje, které slouží k monitorování, správě a údržbě podnikových systémů [16].

„Co nejde měřit a sledovat, to nejde ani dobře a efektivně řídit“, neboli monitorování se stává nezbytnou podmínkou úspěšného provozu jakékoliv ICT infrastruktury. Kritická rozhodnutí jsou závislá na dostupnosti aktuálních dat, tzn. ICT organizace, která se snaží zajistit kvalitu svých služeb, musí také integrovat správu chyb a výkonnosti. Dříve byla oblast monitorování vnímána především jako podpora pro zajištění elementární funkčnosti systému. V současné době se spektrum služeb posouvá více do oblasti specifických požadavků koncových uživatelů. Primárním cílem monitorovacího systému ale zůstává proaktivní přístup ke správě problémů a zejména snaha o řešení problémů dříve, než se projeví koncovému uživateli.

Lze si představit situaci, kdy některý z kritických informačních systémů havaruje. Všechny závislé obchodní procesy nebudou rovněž fungovat, a to minimálně do doby, než bude havárie vyřešena. Většinou provázanost mezi informačními systémy a obchodními procesy dosahuje takové míry, že nelze udržet obchodní proces při životě alternativním způsobem. Nemožnost vykonávat obchodní proces znamená přímou finanční ztrátu, která v důsledku může vést až k úpadku společnosti. Je jasné, že čím kratší, profesionálnější a více odzkoušená bude reakce odpovědného personálu, tím kratší dobu bude trvat vlastní náprava havarijního stavu do normálního režimu. Navíc, pokud se někdo dopředu zamyslí, jaké hrozby jsou pro jeho informační systém relevantní a jaká je pravděpodobnost jejich výskytu, může řadu těchto takzvaných rizik eliminovat formou preventivních opatření.

Cílem bakalářské práce je nakonfigurovat monitoring databáze tak, aby správce IS získal rychlý přehled důležitých informací, které by vedly k efektivnímu řešení kritických situací IS. Podstatou je vytvořit takovou konfiguraci monitorovaných zdrojů pomocí SW nástroje, která by poskytovala co nejefektivnější a nejpřehlednější stav informačního systému a zmenšit tak riziko neočekávané odstávky.

2. Podniková a informační strategie organizace

Podniková strategie definuje způsob, jakým chce firma dosáhnout svých cílů, tj. co chce, kam směřuje a jak toho dosáhne. Formuluje tak pomocí otázek - proč?, kdo a kdy?, jak?, co?, hlavní zaměření podniku, podnikové cíle a jejich priority, definuje zdroje pro realizaci cílů, způsob ověřování jejich naplňování a zodpovědnost osob za jejich naplnění [23].

Informační strategie rozpracovává vize a cíle podnikové strategie z pohledu jejich podpory nebo zajištění informačním systémem a technologiemi. Informační strategie by měla obsahovat vizi, cíle a hlavní charakteristiky budoucího stavu IS/ICT firmy a mimo to by měla účinně přispívat k omezení chaotické řízení jejich vývoje a provozu [9].

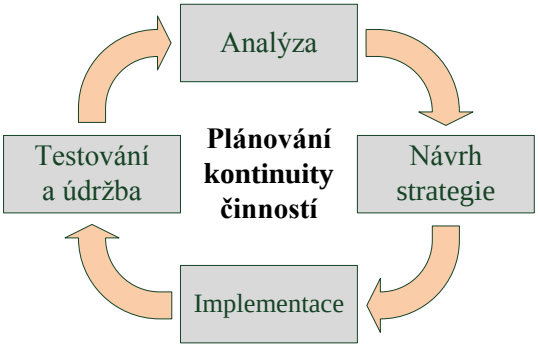
2.1. Kontinuita podnikání (Business Continuity)

Velká část této práce se zabývá architekturami a technologiemi, aby bylo dosaženo nepřetržitého provozu i navzdory vzniku ICT výpadku. Nesmí být zapomenuto, že ICT operace jsou pouze prostředkem k dosažení jiných cílů. V konečném výsledku je potřeba podpořit Business Continuity (Kontinuita podnikání). Z toho vyplývá, že všechny podnikové procesy a nejen ty ICT musí být připravené, přizpůsobené a robustní v případě výskytu nějakého problému. Business Continuity není pouze cíl, ale místo toho se stává nástrojem, který se zaměřuje na podnikové procesy a jejich trvalá zlepšení a ICT se musí na těchto zlepšeních podílet. Pokud podnikové procesy závisejí na ICT službách, tak je nutné zvládnou i ICT Service Continuity (kontinuitu činnosti IT služeb). Pokud podnikové procesy nevyužívají ICT služeb, je nutné zkontrolovat, jestli se nedá zlepšit jejich výkon, robustnost nebo snížit jejich náklady pomocí ICT podpory. Kontinuitu činnosti ICT služeb má tedy za úkol podporovat cíle Business Continuity a vysoká dostupnost a zotavení po havárii jsou dva prostředky, aby tyto cíle plnily[9] [17].

2.1.1. Řízení kontinuity podnikání

Řízení/plánování kontinuity podnikání/činností (Business Continuity Planning, dále jen BCP) je relativně novou disciplínou řízení, která se stává stále důležitější v souvislosti s neklidným prostředím, v němž se organizace nyní nacházejí. BCP je souhrn preventivních opatření, která firma nebo organizace realizuje, aby nebyla zaskočena nečekanými událostmi a zachovala si při nich svou provozuschopnost. Události mohou být nejrůznějšího druhu – od živelných katastrof, přes odchody důležitých manažerů, až po výpadek firemní počítačové sítě.

Při přípravě BCP se podrobně mapují veškeré procesy v organizaci a jsou identifikována případná rizika. Poté jsou navrženy a simulovány možné scénáře dalšího vývoje. Výsledkem jsou plány alternativních postupů všech klíčových procesů včetně plánu pro návrat do původního stavu. Dalším důvodem, proč se zabývat sledováním, kontrolou a bezpečností informačních systémů ve firmě (vedle tak přízemních aspektů, jakým je udržení provozuschopnosti) je stále častěji vyžadovaná nutnost přizpůsobit se požadavkům různých mezinárodních norem. V tomto případě se rovnou nabízí norma BS ISO/IEC 17799:2000 (u nás známější ve své předchozí verzi jako BS 7799:1999), která se zabývá řízením informační bezpečnosti ve firmách. Vzhledem ke stále větší závislostí organizací na informačních systémech roste jejich zranitelnost vůči různým bezpečnostním hrozbám. Je tedy třeba stále dohlížet na důvěrnost, integritu a dostupnost informací [16]. Na Obrázku 1 je zobrazen životní cyklus BCP.



Obrázek 1: Životní cyklus BCP v SW MS Visio (zdroj: vlastní - přepracováno na základě [21])

2.1.2. Plánování obnovy po havárii (Disaster Recovery Planning)

Jak bylo v předešlé kapitole řečeno, BCP je proces, který pomáhá společnostem identifikovat kritické business procesy a zavést pravidla, procesy a plány k zabezpečení klíčových firemních procesů v případě nepředvídatelných událostí s negativním dopadem na organizaci. Základní součástí BCP je Disaster Recovery plánování (dále jen DRP). DRP je zpravidla omezeno na činnost ICT systémů a ICT infrastruktury a klade si za cíl plné obnovení činnosti těchto systémů v definovaném časovém rozpětí. Úkolem DRP je předvídat, analyzovat a omezit následky událostí, které mohou významně narušit funkčnost ICT procesů nebo za zvláště závažných okolností způsobit až jejich likvidaci. Cílem vytvoření havarijních plánů je připravit organizaci na zvládnutí možných havárií, na zvládnutí krizové situace a na uvedení procesů do normálního režimu. Vypracovaný DRP poskytuje návod, jak v co nejkratším čase s minimem výdajů a rizik obnovit chod kritických aplikací. Tím se předchází

především potenciálním obchodním ztrátám vzniklých v důsledku havárie. Existující osvědčené recovery procesy jsou kompletovány a integrovány do komplexního manuálu postupů. DR plán musí obsahovat nejen řetězec konkrétních recovery kroků, ale i definice týmu pro analýzu problému, recovery týmu pro obnovení zpracování, management týmu pro řízení procesu, specifikace rolí, jmenovité seznamy, telefonní kontakty, rozhodovací procesy, metody eskalací problémů, logování procesu a další důležité části minimalizující možnosti chyby lidského faktoru v kritické situaci. DR plán je velmi úzce spjat s organizací ICT a technologickou infrastrukturou. Proto je důležitá pravidelná aktualizace DR plánu a testování procesů v reálném prostředí. Problematika testování recovery procesů v provozu s vysokou dostupností je složitá a nevhodně konstruované a provedené testování může samo o sobě fungování ohrozit. Proto je součástí DR plánu i metodika testování recovery procesů [4] [5].

2.2. Informační systém

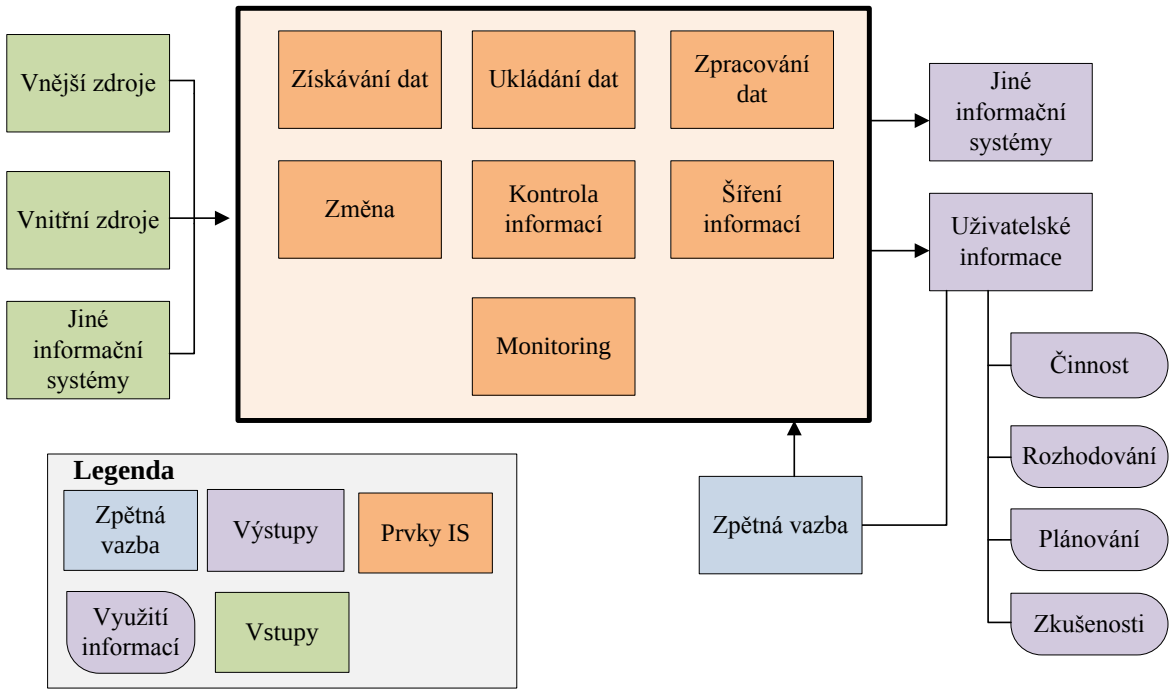
„Pravou hodnotu informačního systému si uvědomíme teprve až v okamžiku, kdy o něj přijdeme.“ [12]

Z hlediska obecné teorie systémů lze definovat systém stručně tak, že se jedná o množinu vzájemně propojených prvků, které formují celek a které slouží společnému cíli (účelu). Informační systém musí být tedy rovněž množina vzájemně propojených prvků, které formují celek a slouží společnému cíli. Prvky, celek a cíl mají však již v tomto případě specifický charakter [18]:

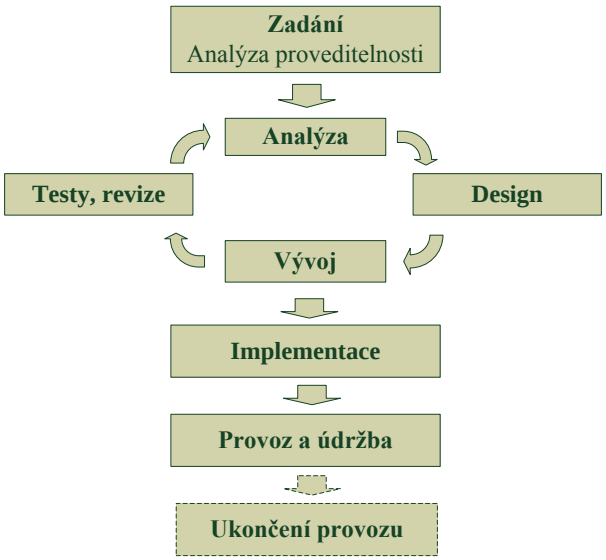
- Prvky představuje množina vzájemně propojených lidských, technických a programových (metodických) prvků (prostředků).
- Celek představuje podnikový informační systém.
- Cílem informačního systému je sběr, přenos, zpracování a uchování dat za účelem prezentace informací pro podporu základních procesů v organizacích.

Pro naše potřeby definujeme informační systém jako funkční propojení lidí, dat, procesů, rozhraní, sítí a technologií. Jednotlivé prvky spolupracují tak, aby podporovaly a zlepšovaly každodenní operace v organizaci a zároveň, aby podporovaly řešení problémů a proces rozhodování v rámci managementu. Informační systémy se často člení na systémy zpracování dat a komunikační systém.

Schéma informačního systému je znázorněno na Obrázku 2. V silném rámečku je vyobrazen samotný informační systém, v levé části jsou vstupy a vpravo výstupy. Zpětná vazba zajišťuje předání informací od uživatele do systému [10].



Obrázek 2: Schéma IS; SW MS Visio (zdroj: vlastní – přepracováno na základě [10]



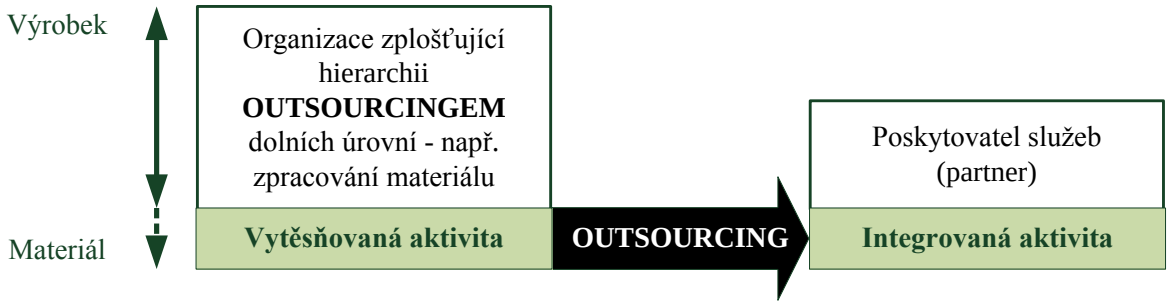
Obrázek 3: Životní cyklus IS; SW MS Visio (zdroj: vlastní - přepracováno na základě [9] [10])

Životní cyklus vytyčuje jednotlivé základní etapy IS (Obrázek 3) a podchycuje tak jeho „život“ od začátku do konce. Vývoj IS s použitím informačních technologii je velmi nákladná a komplikovaná činnost a může probíhat pomocí vlastních prostředků nebo dodavatelských firem (Outsourcing) [10] [11].

- **Zadání (analýza proveditelnosti)** – definice cílů a zjištění realizovatelnosti – hledání odpovědí na otázky *proč* a *co*.
- **Analýza** – specifikují se požadavky, termíny řešení, ceny, stanovují se zdroje, formulují se přesné odpovědi na otázky *proč* a částečně na otázky *jak*.
- **Design** – návrh systému, volba hardware a software, návrh rozhrání a struktury dat.
- **Vývoj –** kódování a tvorba programové části informačního systému.
- **Testy, Revize –** testování jednotlivých částí a funkcí, předávací testovaní, revize a případná úprava již existujících funkcí a částí.
- **Implementace –** zavádění do provozu, instalace hardware a základního software, předávací testy a zkušební provoz.
- **Provoz a údržba** – odstraňování chyb zjištěných za provozu, vylepšování a rozvoj funkcí.
- **Ukončení provozu** – Informační systém je většinou nahrazen novým a modernějším systémem nebo tato etapa IS nemusí vůbec nastat, protože systém je neustále vylepšován. Z tohoto důvodu je tato etapa na Obrázku 3 provedena přerušovanou čarou.

2.2.1. Outsourcing IS

Jak již bylo v předešlé kapitole zmíněno, lze jednotlivé etapy životního cyklu informačního systému realizovat i pomocí služeb dodavatelských firem tzv. outsourcing. Pojem outsourcing pochází z angličtiny a skládá se ze dvou slov – out (=vně) a source (=zdroj). K tomuto pojmu není v češtině relevantní výraz, a proto se používá přímo anglické slovo. Outsourcingem lze zjednodušeně označovat ty případy, kdy dochází k zajištění podnikových aktivit pomocí externích služeb a zdrojů poskytovatelem, který se specializuje na ucelené bloky poskytované služby.[15] Na Obrázku 4 je zobrazen princip outsourcingu.



Obrázek 4: Princip outsourcingu; SW MS Visio (zdroj: vlastní – přepracováno na základě [15])

Podnik využívá ke své činnosti zdroje, které na základě své potřeby a legislativy obhospodařuje tak, aby poskytovaly vstupy včas a v takové kvalitě i kvantitě, jaká je požadována pro plnění cílů podniku. Outsourcing je pak takový stav (nebo činnost k němu vedoucí), kdy vstup, který by firma jinak získala z takového zdroje, koupí od jiného (podnikatelského) subjektu jako službu (nebo zboží). Tím odstraní interní činnosti související s obhospodařováním zdroje. Podnik takto tedy od sebe zdroj odsune (out). Vloží mezi sebe a zdroj další subjekt. Outsourcingem je označován (výše uvedený) stav, činnost k tomuto stavu vedoucí (dále outsourcing jako proces) a také permanentní činnost, která tento stav udržuje [2].

Oblasti využití outsourcingu jsou různé, nejčastěji se jedná o sféry podnikové informatiky, mezi něž se řadí plánování a strategie, konzultace, údržba a podpora, vývoj softwaru pro potřeby společnosti, provoz operačních systémů, provoz aplikací, provoz podnikových informačních systémů, provoz koncových stanic, webové služby, webhosting, helpdesk, hotline, call centra, školení a vzdělávání v ICT [6].

2.2.2. SLA – Servis Level Agreement

Přechod na outsourcing vyžaduje provést audit současného stavu, zmapovat informační potřeby, vypracovat projektový plán a definovat SLA pro jednotlivé oblasti a návrhy nastavit konkrétní metriky a jejich prahové hodnoty, nakonec pak připravit zákazníky, aby došlo k naplnění jejich přání v souladu s realitou outsourcingu [7].

"Dohoda o úrovni poskytovaných služeb" (SLA) je portfoliem metrik, které je nástrojem řízení informatiky, a to jak ve vztahu k externímu poskytovateli, tak ve vztahu k internímu útvaru informatiky. SLA je pojem, který primárně vzniknul jako nástroj měření úrovně poskytovaných služeb externím poskytovatelem, v rámci outsourcing, resp. v rámci jiného typu smluvního vztahu, jako je např. servisní smlouva. Naměřené hodnoty SLA potom podmiňují výši plateb, resp. uplatnění sankcí, ve vztahu k externímu poskytovateli [22].

Obsah SLA je dán charakterem služby. Některé složky SLA mají obecnou platnost a jsou uváděny u všech typů služeb, některé se vztahují pouze k dané službě. Současně platí, že SLA může mít rozdílné parametry pro různé kategorie koncových uživatelů [22].

SLA jako portfolio metrik sestává z následujících částí [22]**:**

- Základní specifikace, podmínky a pravidla.
- Kategorie příjemců.

- Přesné vymezení počtu a umístění příjemců dané kategorie.
- Poskytovatel - bližší určení (uvádí se, má-li smysl, resp. je-li uživatelů více).
- Měření - postup, způsob, periodicita, odpovědnost a vykazování výsledků.
- Ověřování - postup, způsob, periodicita, odpovědnost a vykazování výsledků ověřování správnosti měření.
- Určení a způsobu realizace podpory (např. fyzicky na místě, vzdáleně apod.).
- Návazné podpůrné služby spojené s danou službou (např. trénink na místě, resp. na učebně).
- Cena služby.
- Platební podmínky.
- Pravidlo pro změny služby.
- Práva a povinnosti obou stran - podmínky součinnosti.
- Ostatní podmínky pro realizaci SLA (právo informovanosti, odpovědnost za vady a škody apod.).
- Tvrdé metriky.
- Dostupnost (v % vyjádřený skutečný čas disponibility aplikace na daném zařízení uživatele ve vztahu k celkovému efektivnímu fondu pracovní doby za určenou časovou jednotku).
- Běžná a maximální přípustná (kritická) doba odezvy na požadavek, tzv. incident (v členění na jednotlivé typy požadavků, jako je např. hlášení poruchy aplikace, poruchy HW, přemístění koncové stanice, apod.).
- Běžná a maximální přípustná (kritická) doba řešení požadavků (v členění na jednotlivé typy požadavků).
- Průměrná a mezní odezva aplikace v rámci služby.
- Měkké metriky.
- Ostatní metriky pro danou službu (kvalitativní ukazatele typu "akceptace", "zápis", "potvrzení realizovaného školení a prezenční listina", "hodnocení lektora školení", "hodnocení účastníka školení", apod.).

V souvislosti s tvrdými metrikami SLA, jako je odezva, dostupnost apod., jsou v některých případech stanovovány až tři úrovně tohoto parametru [22]:

- **Servisní úroveň** - požadovaná hodnota parametru za standardních podmínek (např. dostupnost na úrovni 0,97 a vyšší).

- **Minimální servisní úroveň** - pod tuto mez nesmí hodnota daného parametru nikdy klesnout (např. dostupnost 0,94).
- **Motivační (incentive) servisní úroveň** - má motivovat poskytovatele k poskytování nadstandardní úrovně služeb (např. dostupnost nad 0,99).

Nedosažení "servisní úrovně" vede ke snížením plateb za služby. Nedosažení ani minimální servisní úrovně je událostí, která způsobí uplatnění předem definovaných sankcí. Dosažení motivační úrovně naopak zakládá nárok poskytovatele na bonus [22].

Tabulka 1: Doby maximálních výpadků při různých úrovních SLA (zdroj: vlastní přepracováno na základě [17]

SLA (%)	24 x 7		24 x 6		14 x 5	
	měsíčně	**ročně**	**měsíčně**	**ročně**	**měsíčně**	**ročně**
94,0	1,8 dne	21,9 dne	1,6 dne	18,8 dne	18,3 hod	9,1 dne
97,0	21,9 hod	11 dne	18,8 hod	9,4 dne	9,1 hod	4,6 dne
99,0	7,3 hod	3,7 dne	6,3 hod	3,1 dne	3 hod	1,5 dne
99,9	43,8 min	8,8 hod	37,6 min	7,5 hod	18,3 min	3,7 hod
99,99	4,4 min	56,6 min	3,8 min	45,1 min	1,8 min	21,9 min
99,999	26,3 sek	5,3 min	26,6 sek	4,5 min	11 sek	2,2 min

Pokud nějaká např. outsourcingová nebo dodavatelská společnost deklaruje ve svých marketingových materiálech dostupnost v hodnotě 99,999%, tak z hodnot z Tabulky 1 vyplývá, že se jedná pouze o reklamní slogan, který lze v praxi jen těžko uplatit. Existují zde dva problémy, proč neslibovat svému zákazníkovi „několika devítkové“ číslo záruk. Prvním jsou výluky, mezi něž patří například plánovaná údržba operačního systému, upgrade softwaru, pravidelně se opakující inicializace počítače apod. Tyto zdánlivě nepříliš náročné operace se opakují většinou minimálně jednou týdně, mohou trvat 15–30 minut, a tak v podstatě zabraňují dodavatelům outsourcingových služeb dávat záruky typu 99,999%. Druhým problémem je, že různí zákazníci mají různé hardwarové a softwarové vybavení, různé datové sklady, různé rychlosti sítí apod., nemluvě o tom, že i vybavení uživatelů u jednotlivých zákazníků může být značně odlišné. Z těchto důvodů je možno říci, že záruka 99,999% je dnes velmi nereálná nebo velmi nákladná, protože jak roste hodnota SLA, tak se zvyšují náklady na dodržení těchto podmínek [7].

Dokument SLA by měl být strukturován tak, aby motivoval obě smluvní strany k rozvoji a vzájemné podpoře. Často se v literatuře setkáváme s pojmem „win-win agreement“, který v podstatě znamená, že oba partneři by měli těžit ze vzájemné spolupráce a díky

synergickému efektu plynoucímu ze strategického partnerství dosahovat vyšší produktivity a těžit z větší konkurenceschopnosti na dnešním globalizujícím se trhu. SLA patří mezi nejdůležitější body procesu outsourcingu, je velmi důležitým nástrojem k eliminaci nevýhod outsourcingu ICT, a proto by mu měla být věnována zvláštní pozornost managementu obou budoucích smluvních partnerů [7].

2.2.3. Reálné přínosy outsourcingu

Omezit se při hledání přínosů outsourcingu pouze na snížení nákladů původně související se mzdami, když se zájemce o outsourcing často dozví o vyšší ceně služby. Při širším a úplnějším pojetí nákladů, včetně zahrnutí ohodnocení měkkých hodnot, však musíme dojít k ekonomické výhodnosti, pokud je správně tato služba definována. Úspora nákladů, totiž představuje ve skutečnosti velice zúžený pohled. Největší sílu outsourcingu je třeba vidět v zajištění IS/ICT na takové úrovni, která firmě umožňuje výrazně změnit svou konkurenční pozici. Mezi typické přínosy outsourcingu patří například definovaná odezva systému (definovaný výkon), řešení havarijních stavů, nepřetržitý dispečink, rozvoj aplikací, garance plnění stanovených podmínek, zastupitelnost operátorů, administrátorů atd., dostupnost týmu expertů pro různé oblasti ICT, jejich znalost nejnovějších technologií, zkušenosti s problematikou informačních systémů, snižuje se riziko výpadku informačního systému na výběr nových technologií a zprůhledňuje se transparentnost nákladů [6].

2.3. Zajištění dostupnosti informačního systému

Dostupnost je dlouhodobě kritickou součástí informačních systémů, protože pokud je IS mimo provoz, tak podnikové procesy nemohou být dále prováděny. Například ve světě elektronického obchodu, kdy je dostupnost důležitá z důvodu poptávky klientů po okamžitém přístupu k obchodnímu místu. A jestliže je toto místo nedostupné, tak konkurence je pouze o jedno kliknutí myše vedle. Každé přerušení nabízené služby je měřitelné nejen v penězích, ale možná důležitější, reputací [24].

2.3.1. Obchodní hledisko

Potřeba ochrany proti odstávkám systému je zřejmá, ale neměla by se přepokládat za samozřejmou. Nejprve se musí být zmapovány firemní potřeby, které potřebují vysoce dostupné systémy a zotavení po havárii (Disaster Recovery). Poté se vytvoří ucelený pohled na obchodní důsledky a dopady na společnost, jestliže nastane odstávka systému. Jenom s finančními vyjádřeními těchto dopadů a důsledků, se můžou ospravedlnit výdaje na zvýšení

dostupnosti a ochrany proti výpadkům systémů. Pro obchod nejsou ICT odstávky reálnou záležitostí, ale reálné jsou finanční důsledky, které jsou s tím spojené. Obrázek 5 ukazuje, jak výpadek ovlivní výnosy či náklady, které se dají určit přímo nebo je odhadnout [17].

	Známé	**Odhadnuté**
Zisky	Ztráta zisků	Ztracené pracovní hodiny
Náklady	Přímé náklady	Dodatečné pracovní hodiny

Obrázek 5: Obchodní důsledky odstávky IS; MS Visio (zdroj: vlastní - přepracováno na základě [17])

Přímé náklady jsou spojeny s opravou ICT poruch, aby pomohly dále pokračovat ICT operace. Jsou to například opravy zařízení, přeprava zařízení, případně náklady za externí specialisty. Další přímé náklady jsou finanční sankce, které vyplývají ze smluvních závazků, jestliže odstávka způsobí opoždění dodání objednané služby [17].

Dodatečné pracovní hodiny jsou režijní náklady, které jsou přisuzovány nějakému incidentu. ICT personál odpracuje hodiny, které jsou nutné pro nápravu ICT poruchy, místo toho, aby pracoval na vylepšeních ICT služeb. Tyto hodiny musí zaplatit společnost pro, kterou pracují. Je jasné, že odstávka systému může zapříčinit dodatečné pracovní hodiny i v jiných oblastech (odděleních) společnosti. Například pracovníci expedičního oddělení, by mohli potřebovat dodatečné pracovní hodiny, jestliže je systém zásobování nedostupný. Nebo úředníci budou muset pracovat přes čas, protože během pracovní doby nebyly přístupné služby, které potřebují pro svoji práci – adresy, sdílené soubory či emaily. Mohlo by se najít spousta jiných příkladů, které se dotýkají skoro každého odvětví společnosti, ale téměř všechny podnikové procesy v dnešní době závisí na nějakých ICT procesech [17].

Ztracené pracovní hodiny jsou nepřímý indikátor toho, že se sníží výnosy. Když například 100 pracovníků nemůže pracovat, protože nějaký server je mimo provoz a během této doby nemůže být doručeno zboží, tak prodeje, které mohly být během odstávky vytvořeny, jsou nenávratně ztracené. I, za tyto ztracené hodiny je potřeba vyplatit mzdu pracovníkům, kteří nemohli pracovat a vytvářet zisk společnosti [17].

Ztráta zisků se může, také připisovat na vrub odstávce systému. Jestliže, jsou obchodní systémy mimo provoz a společnost prodává zboží či služby přes internet a výpadek těchto systémů může způsobit, že zákazníci přejdou ke konkurenci, jejíž systémy jsou stalé funkční. Dlouhodobě můžou výpadky, které se dotýkají zákazníků způsobit snížením reputace a odliv klientů [17].

2.3.2. Klasifikace systémových odstávek

Systémové odstávky lze klasifikovat podle následujících hledisek [24]:

Neplánované systémové odstávky (poruchy) jsou výsledkem nekontrolovaných a náhodných poruch systému spojených s chybami, které se vyskytují uvnitř hardwarových a softwarových součástí. Jsou nejvíce nákladné a mohou být minimalizovány pomocí redundance komponent nebo monitoringu.

Plánované systémové odstávky (údržba) by měly být naplánovány tak, aby měly co nejmenší dopad na dostupnost systému. Do tohoto typu odstávky patří např. opravy hardware, zálohování nebo aktualizační operace. Opravy jsou určené pro odstranění vadných hardwarových komponent a obnovení systému do funkčního stavu. Zálohy jsou určené pro uchování důležitých dat na paměťová média (disky, pásky), aby se vyhnulo jejich ztrátě. Aktualizace jsou prováděny z důvodu výměny aktuálního stavu hardware nebo programového vybavení na novější verzi.

2.3.3. RAS (Reliability, Availability, Servicebility)

Tato kapitola se zabývá o měřitelnosti dostupnosti (availability). Nejprve se definuje pojem dostupnost, a co to vůbec znamená. S touto definicí budou následně spojeny výrazy spolehlivost (reliability) a obslužnost (serviceability). Dohromady tvoří akronym RAS, který se užívá pro popsání kvality informačních systémů. Spolehlivost a obslužnost přispívají k vyšší dostupnosti systému [17] [19].

Dostupnost (Availability) je míra, jak často či jak dlouho je služba nebo systémová komponenta k dispozici pro její využití. Výpadek komponenty je významný pro dostupnost služby, jestliže komponenta je důležitá k poskytování služby. Například vyřazením síťové karty počítače se ukončí dostupnost síťové služby, zatím co lokálních služeb se to nedotkne. Dostupností se vyjadřují také vlastnosti, které pomáhají systému, aby zůstal v provozním stavu, i když se vyskytla porucha. Například zrcadlení disků zlepšuje dostupnost. Základní míra dostupnosti je poměr doby provozu k celkovému uplynulému času[17].

$$Dostupnost = \frac{doba\ provozu}{doba\ provozu + doba\ nečinnosti} \quad (2.1)$$

Celkový uplynulý čas zahrnuje plánované stejně tak i neplánované doby nečinnosti provozu. Poněkud diskutabilní rozhodnutí je to, zda celkový uplynulý čas provozu je reálný čas nebo doba provozu. Když je použito reálného času, který je ideální pro vysoce dostupné systémy, to má za efekt, že pravidelné, preventivní údržbové činnosti sníží dostupnost. Stejná dostupnost může být vyjádřená v absolutních číslech (např. 239 z 240 hodin za poslední měsíc) nebo v procentech (např. 99,6% za poslední měsíc). Jestliže je známá průměrná doba bezporuchového provozu (MTBF – Mean Time Between Failures) a průměrná doba opravy (MTTR – Mean Time To Repair), tak se může vyjádřit plánovaná nebo očekávaná dostupnost jako:

$$Plánovaná\ (očekávaná) dostupnost = \frac{MTBF}{MTBF + MTTR} \quad (2.2)$$

Tento vzorec ukazuje jasně, že MTTR nejvíce ovlivní dostupnost. Například snížením doby opravy MTTR o jednu desetinu má stejný účinek jako desetinásobné zvýšení MTBF. V realitě je tento vztah více nákladný, někdy až nemožný k tomu, aby se takto hodně MTBF zvýšilo, zatím co čas oprav MTTR se může snížit lepšími procesy, jako např. náhradní součásti jsou na místě a nemusí se dopravovat [17].

Spolehlivost (Reliability) je funkce pomáhající detekovat chyby a předcházet jim. Jiný slovy je to pravděpodobnost, že systém pracuje v čase *t+1*, jestliže pracoval v době *t*. Spolehlivost neměří plánované či neplánované odstávky systému. Vlastnosti spolehlivosti pomáhají předejití a zjištění chyby. Detekce chyb je velice důležitá, ale velmi často opomíjená. Nejhorší chování systému je, když pokračuje v provozu i po vzniku chyby. Tím může tvořit špatné výstupy nebo poškozovat data [17].

Obslužnost (Serviceability) vyjadřuje míru, jak je systém snadno servisovatelný a opravitelný. Např. systém je modulární s použitím hot-swappových[1] součástí. Dále to může

[1] Jedná se o vkládání a vyjímání HW součásti za chodu systému, aniž by se musel provést jeho restart nebo vypnutí [8].

být vyjádřeno jako obrácené množství doby údržby a množství havárií po celou dobu životnosti systému. Obslužnost se skládá ze dvou měrných složek: plánovaná a aktuální [17].

Plánovaná obslužnost je požadavek, který vstupuje do architektury systému jako finální projekt. Dobrý architekt vezme všechny svoje zkušenosti a použije technologii k tomu, aby vytvořil aktuální obslužnost menší než je plánovaná [17].

Vlastnosti obslužnosti pomáhají diagnostikovat systém, když nastanou problémy, a schopnost servisu komponenty v systému bez ukončování celého provozu. Mezi možnosti diagnostikování systému patří programy na obnovu a ladění a diagnostické nástroje. Dobrá obslužnost zvyšuje jak dostupnost, tak i spolehlivost [17].

3. Proaktivní monitoring

Jednou ze základních součástí DRP je proaktivní monitoring. Lze ho charakterizovat tak, že správce IS nečeká na to, až mu uživatelé zavolají, že systém nebo jeho část nefunguje, ale že nefunkčnost zaznamená on sám. Proaktivní monitoring tedy zjišťuje a reaguje na problémy informačního systému předtím, než jeho koncový uživatel zjistí, že skutečně nějaký problém nastal. Používá se zvláště pro ty informační systémy, které se významně podílí na tvorbě zisku (elektronický obchod aj.); v takových případech je to běžný systémový požadavek. Většina správců informačních systému chápe potřebu aplikačního a systémového monitorování pro zvýšení dostupnosti IS. Pracovníci ICT oddělení standardně monitorují základní zdroje aplikačních serverů, jaké jsou např. využití CPU, využití paměti atd. Nicméně je zde celá škála dalších zdrojů na monitoring a je nutné porozumět jejich parametrům a zjistit, které jsou efektivní pro rozpoznávání problémů a jejich eskalaci. Jaké jsou tedy možnosti odhalení problému? První možnosti je ta, že správce systému bude mít spuštěné všechny aplikace, bude s nimi pracovat, a když zjistí nějaký problém, bude ho řešit. Tato možnost pro velké množství různých aplikací a systémů v IT prostředí organizace je zcela nereálná. Druhou možností je využití softwarových nástrojů, které sledují vybrané zdroje a automaticky hlásí při překročení nastavených mezí. Správce může těmito nástroji sledovat jejich stav, nastavovat meze, při kterých bude informován a předcházet tak výpadkům ICT služeb [8] [14].

3.1. Monitoring pomocí nástroje OpenEdge Management

Pro ověření modelů byl vybrán softwarový nástroj OpenEdge Management (dále jen OEM) a to z toho důvodu, že monitorovaný informační systém využívá databázového prostředí Progress. OpenEdge Management je tedy systémový nástroj pro správu, údržbu a zajištění stálé kvality provozu aplikací založených na databázovém prostředí Progress. Umožňuje nepřetržitě a proaktivně monitorovat technologickou infrastrukturu, stejně jako zobrazovat a analyzovat získané soubory informací popisující stav i trendy (historii stavů) daného systému [16].

OpenEdge Management lze využívat jak při řízení zdrojů či při kapacitním plánování, tak pro budování schopností firmy zvládat nepředvídané události. Jeho pomocí je možné efektivně řídit zdroje, snižovat provozní náklady a přitom zvyšovat dostupnost systémů. Díky tomu může být organizace stále k dispozici svým klientům (zákazníci, pacienti, občané atd.) i obchodním partnerům, což zvyšuje její prestiž a důvěryhodnost [16].

3.1.1. OpenEdge Management lokálně i vzdáleně

OpenEdge Management sleduje podporované procesy dvojím způsobem. Za prvé monitoruje kritické (prahové) hodnoty veličin a spouští poplach v případě, že jich je dosaženo. Poplach se objeví na konzoly administrátora a je k němu možné definovat úkony, které by měly následovat (např. zaslání zprávy na helpdesk). Za druhé OE Management provádí tzv. trendové sledování. V tomto případě jde o zaznamenávání historie hodnot sledovaných veličin do další progressovské databáze. S takto získanými informacemi lze následně pracovat – provádět analýzy, vytvářet reporty a na základě zjištěných faktů upravovat systém. Software lze nasadit ve dvou základních konfiguracích. Lokální konfigurace předpokládá instalaci přímo na serveru, na kterém je umístěna databáze a monitorované zdroje. Administrace je prováděna prostřednictvím jednoduchého webového serveru. OE Management může monitorovat i více databází současně, vyžaduje však pro každou z nich instalaci tzv. databázového konektoru. Je schopný také komunikovat s jinými systémy pro správu (např. HP Open-View) a zasílat jim prostřednictvím SNMP klienta zprávu o zachycených událostech. Může se tak stát součástí jiného správcovského systému, který dokáže sledovat celý informační systém (od různých výrobců) na jedné centrální konzoly dohledového centra. V dohledových centrech se obvykle používá vzdálená konfigurace OE Managementu. Výhodou je minimální zatížení serverů u zákazníků a sledování více zakázek zároveň na jedné konzoly. Nevýhodou je nemožnost využívat všech funkcionalit systému, jako je

monitorování souborů a jejich obsahů, spouštění plánovaných úloh i analytické sledování. Sledují se pouze základní vlastnosti systémových zdrojů (procesorů, pamětí apod.) [16].

3.1.2. Monitoring zdrojů

OE Management je určen k monitorování progressovského databázového prostředí a provozování administrativních činností s tím spojených. Zároveň však umožňuje monitorovat i další prvky, na kterých je provoz databázového prostředí závislý. Sem patří jednak používaný operační systém a jednak hardwarové komponenty serverů. OEM monitoruje databáze, soubory, sítě, prostředí OpenEdge a systémové zdroje. Při práci se soubory dokáže sledovat obsah souborů a jejich vlastnosti (stáří, velikost, rychlost růstu a modifikace). OEM také umožňuje definovat pravidla pro prohledávání textových souborů, což je důležité pro automatizovanou analytickou činnost a detekci chyb. U síťových zdrojů OEM zjišťuje jejich dostupnost pomocí protokolů HTTP, TCP, UDP a ICMP. Dále dokáže sledovat provoz a interaktivně ovládat prostředky OpenEdge, jako jsou AppServer, NameServer a WebSpeed. Zároveň kontroluje jejich nastavení, sleduje výkonové charakteristiky a monitoruje logy [16].

4. Modelování a modelovací nástroje

Účelem modelování je vytvoření takové abstrakce procesu, která umožňuje pochopení všech jeho aktivit, souvislostí mezi těmito aktivitami a rolemi reprezentovaných schopnostmi lidí a zařízení zapojených do daného procesu. V současné době lze nalézt celou řadu metod postavených na různých technologiích, které jsou používány k sestavování modelů podnikových procesů. Tyto metody však mají společný abstraktní rámec, který vyplývá z postupu návrhu byznys procesu [26].

Vlastní modelování je iterací následujících kroků – výchozí formulace problémové oblasti, analýza modelu, návrh a vytvoření modelu, ověření správnosti části modelu i správnosti modelu jako celku, dále simulace a vyhodnocení výsledků. Výstupem je model, jehož vnější podoba je různorodá [20].

Pro tvorbu modelů jsou v bakalářské práci využity zejména prvky vývojového diagramu. Vývojový diagram slouží pro nejjednodušší modelování procesů v systému. Používá všem dobře známou grafickou notaci (ČSN ISO 5807), ale pro modelování v této bakalářské práci bude využita grafická notace SW nástroje MS Visio. Vývojový diagram vyjadřuje logickou strukturu procesu nebo operace tj. člení proces na jednotlivé činnosti. Graficky jsou zde vyjádřeny jednotlivé operace, data, toky, řízení atd. [10]. Vývojový diagram stojí z hlediska formalizace na vyšší úrovni než přirozený jazyk, ale stále však není dostatečně přesný. Vývojový diagram tedy spadá spíše do oblasti semi-formálních popisů [26].
V případě bakalářské práce jsou pro modely využity objekty vývojového diagramu, dále jsou dle potřeby doplněny jednak vlastními objekty a jednak plaveckými drahami („swimlanes“), aby bylo patrné, kdo za jakou činnost zodpovídá.

5. Návrh postupu řešení

Výchozí situace: Výchozí modelová situace je, že v současné době není ve firmě prováděn v rámci Disaster Recovery plánování žádný proaktivní monitoring informačního systému ani jeho součástí. V případě výpadku ICT procesu informuje o této skutečnosti správci IS jeho uživatel, tím vznikají časové prostoje, kdy už se mohl tento výpadek řešit či obnovit. Tento fakt je nejvíce zřejmý, kdy klienti zákazníka musí čekat, protože výpadek brání jejich odbavení na přepážkách poboček organizace.

Požadovaný stav: Vytvořit takový seznam monitorů, který by pokrýval zdroje nutné pro chod IS organizace a jeho součástí. Tato služba bude prováděna pomocí outsourcingové smlouvy, kdy dohled a řešení případných ICT výpadků bude provádět dodavatelská firma. Cílem je získat rychlý přehled informací pro efektivní řešení kritických situací IS.

NÁVRH POSTUPU ŘEŠENÍ JE NÁSLEDUJÍCÍ:

- Analýza a tvorba modelu monitoru:
    - Klasifikace sledovaných zdrojů podle vybraných hledisek.
    - Tvorba modelu procesu pro vytváření monitoru podle požadavku zákazníka.
    - Návrh monitorů sledovaných zdrojů.
    - Tvorba modelu postupu při vytváření monitoru.
    - Identifikace / klasifikace zákazníka a zkoumání jeho vlivu na tvorbu monitoru.
    - Základní nastavení monitorů podle kategorií.
- Verifikace modelu – iterativní postup:
    - Vyhodnocení a návrh monitorů.
    - Ověření postupu a případná korekce modelu monitoru.

Nejdříve je důležité vytvoření specifických technologických kategorií, do kterých budou jednotlivé monitory rozděleny. Dalším krokem bude vytvořit stupně závažnosti, které by klasifikovaly monitory podle dopadu na IS, v případě výpadku monitorovaného zdroje. Pomocí modelovacích technik vytvořit model znázorněný vývojovým digramem, podle kterého by se vytvořil seznam monitorů zdrojů na základě požadavků zákazníka. Pro modelování bude použit SW nástroj MS Visio. Dále bude nutné ověřit, zda má vliv na model, jestliže požadavek pochází od externího či interního zákazníka. Následujícím krokem se provede ověření správnosti části modelu, tak i celého modelu. Po ověření se prohlásí buďto za vyhovující nebo v případě nedostatků se v něm provedou změny.

6. Analýza a tvorba modelu monitoru

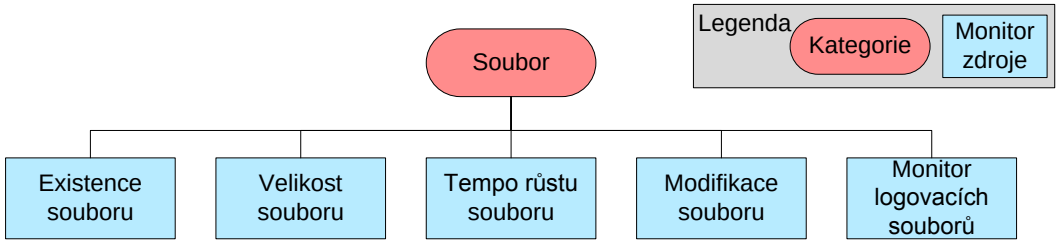
6.1. Klasifikace sledovaných zdrojů

Jednotlivé monitory sledovaných zdrojů se dají rozdělit podle technologických kategorií a podle stupně závažnosti dopadu na informační systém

6.1.1. Rozdělení podle technologických kategorií

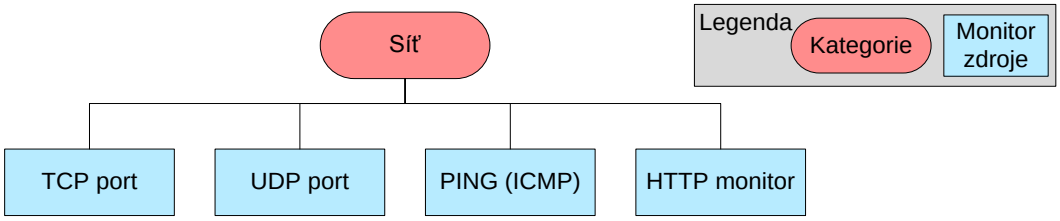
Rozdělení monitorů dle tohoto hlediska zahrnuje skupiny – soubor, síť, OpenEdge a systém.

Soubor: Do této skupiny patří monitory, které sledují fyzické soubory patřící jak do IS (např. databáze, produkční aplikace), tak i soubory, které jsou součástí operačního systému. Tyto monitory jsou schopny sledovat, jak fyzické vlastnosti souboru (existence, velikost, modifikace, tempo růstu), tak i prohledávat textové soubory (logy) a sledovat výskyt hledaných klíčových slov a informovat o tom obsluhu dohledu.



Obrázek 6: Monitory kategorie soubor; SW MS Visio [zdroj: vlastní]

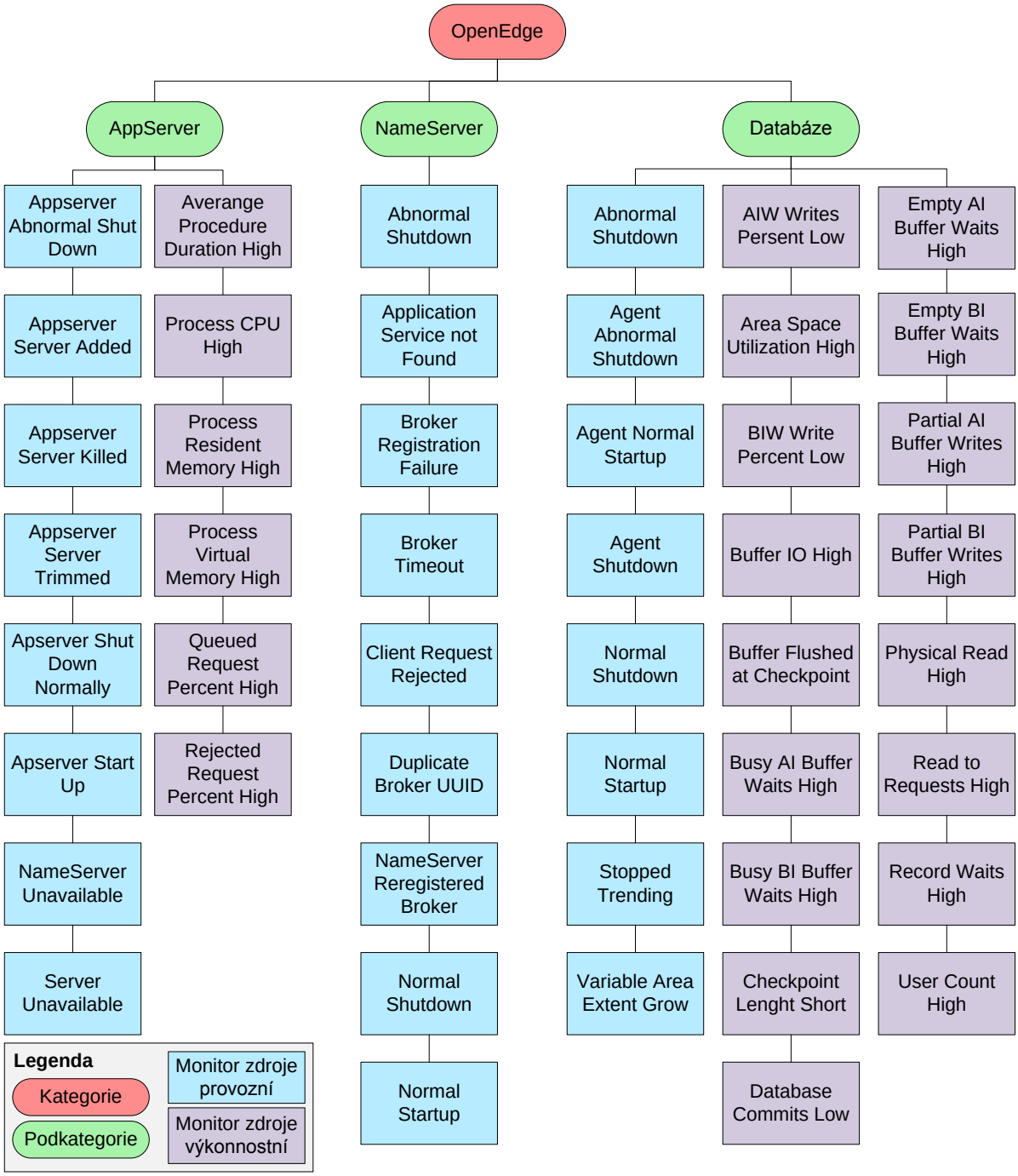
Síť: V této skupině jsou monitory, které sledují síťové rozhraní jak samotného systému, tak i ostatních prvků a externích systémů připojených na síť, které jsou důležité pro chod IS.



Obrázek 7: Monitory kategorie síť; SW MS Visio [zdroj: vlastní]

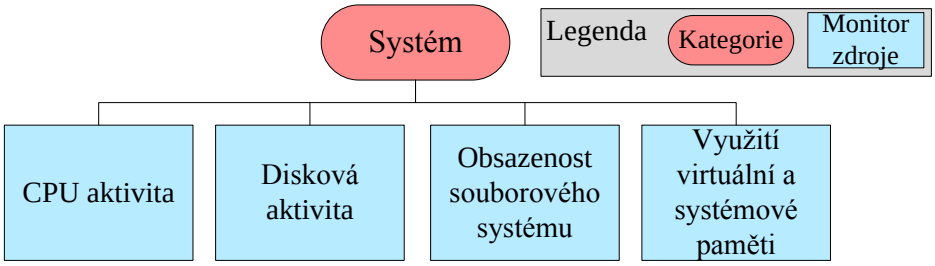
OpenEdge: Tato největší skupina monitorů sleduje procesy, které jsou spojeny s OpenEdge DBMS. Hlavním principem je analýza dat v systémových tabulkách provozní databáze, v které korespondují s jejím aktuálním stavem. Dále sleduje logové souborech databáze, AppServeru (aplikační server), NameServeru a dalších procesů spojených s DBMS,

ve kterých hledá klíčová slova a tak informovat obsluhu dohledu o jejich případných výskytech.



Obrázek 8: Monitory kategorie OpenEdge; SW MS Visio [zdroj: vlastní]

Systém: Další skupinou jsou monitory základních systémových prostředků serveru, na kterém běží IS. Jedná se hlavně o využití souborových systémů, vytížení CPU, disků a využití paměti.



Obrázek 9: Monitory kategorie systém; SW MS Visio [zdroj: vlastní]

6.1.2. Rozdělení podle stupně závažnosti dopadu na informační systém

Pro rozdělení bylo použito čtyř již předdefinovaných úrovní nástroje OEM. To dovoluje si vybrat úroveň závažnosti vzhledem k tomu, jak vysoký bude dopad výpadku monitorovaného zdroje na IS a jeho součástí. Jednotlivé úrovně jsou seřazeny od nejnižšího dopadu na IS po nejvyšší. [1] [13]:

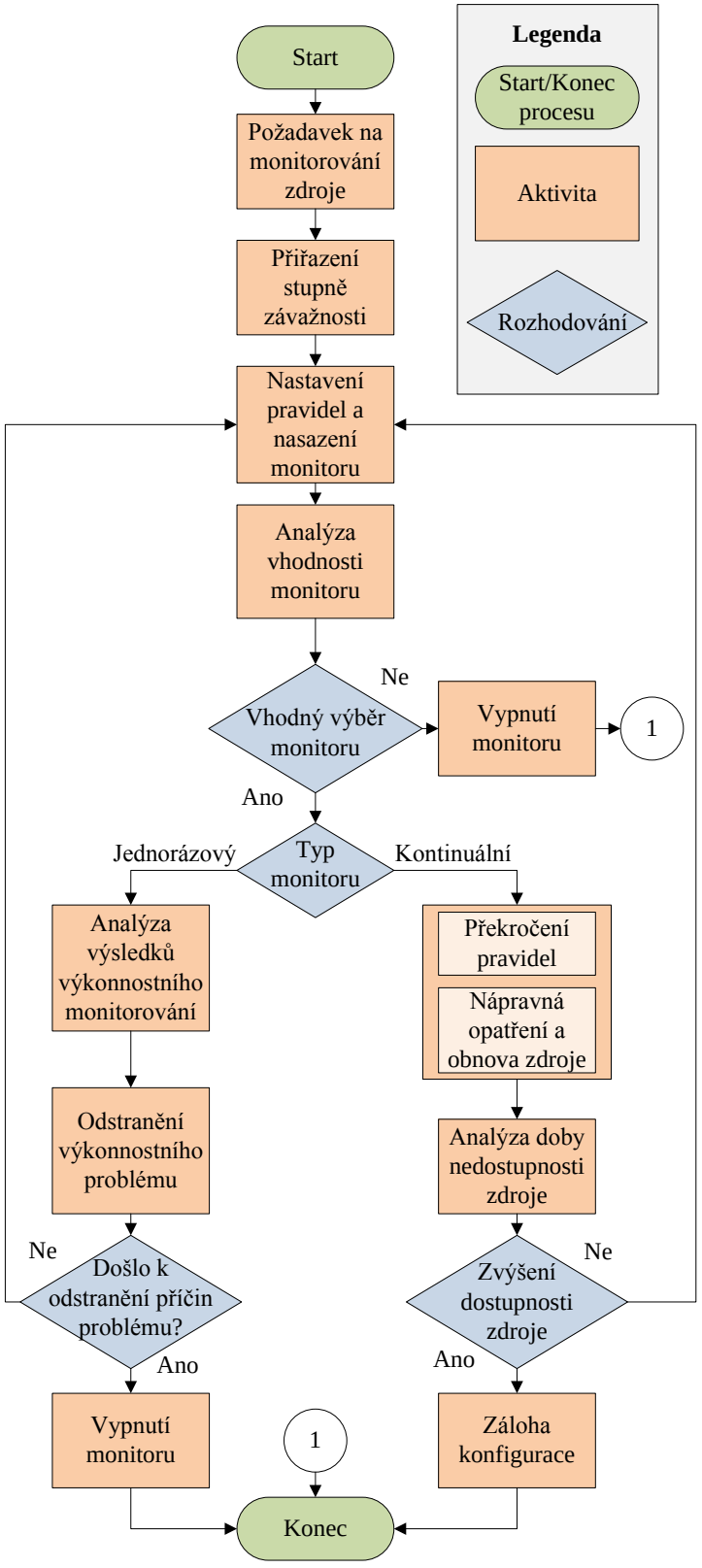
Informace (Information): První stupeň závažnosti má pouze informační charakter a nemá vliv na dostupnost informačního systému. Jedná se většinou o hlášení o úspěšném dokončení nějakého procesu nebo plánované akce. Forma oznámení obsluhy monitoringu je pomocí emailové zprávy.

Varování (Warning): Druhý stupeň závažnosti představuje varování při překročení určité nastavené hranice sledovaného zdroje nebo výpadky zdrojů bez vlivu na základní provoz systému. Forma oznámení obsluhy monitoringu je pomocí emailové zprávy a SMS zprávy. Při výskytu Obsluha monitoringu spolu se správcem IS musí zabránit odstávce nebo chybě, která by byla způsobená výpadkem sledovaného zdroje.

Chyba (Error): Třetí stupeň závažnosti představuje chyby, které mohou způsobit nefunkčnost systému nebo jeho větší části. Forma oznámení obsluhy monitoringu je pomocí emailové zprávy a SMS zprávy. Obsluha monitoringu ve spolupráci se správcem IS musí ihned provést nápravná opatření pro obnovu všech ICT procesů co s nejnižším dopadem na chod organizace a business procesů.

Závažné (Severe): Čtvrtý stupeň závažnosti představuje nezávažnější chyby tj. havárie a nefunkčnost celého systému. Forma oznámení obsluhy monitoringu je pomocí emailové zprávy a SMS zprávy. Obsluha monitoringu a správce IS musí ihned provést nápravná opatření pro obnovu všech ICT procesů co s nejnižším dopadem na chod organizace a business procesů.

6.2. Model procesu „Vytvoření monitoru podle požadavku zákazníka“



Obrázek 10: Model procesu vytvoření monitoru podle požadavku zákazníka; SW MS Visio (zdroj: vlastní)

Model průběhu procesu „Vytvoření monitoru podle požadavku zákazníka“ (Obrázek 10) znázorňuje aktivity, které je potřeba realizovat v případě zákazníkova požadavku na monitorování jím určeného zdroje. Model se skládá ze dvou samostatných částí. První část se zaměřuje na kontinuální monitory, které budou fungovat po celou dobu sledovaného zdroje např. obsazenost souborového systému. Druhá část se orientuje na jednorázové monitory, které budou fungovat do té doby, kdy bude např. odstraněna chyba nebo problémy s výkonností IS.

6.3. Návrh monitorů sledovaných zdrojů

Podle modelu procesu „Vytvoření monitoru podle požadavku zákazníka“ byl vypracován prvotní seznam monitorů, které postihují základní známé zdroje, které jsou nutné pro standardní provoz informačního systému.

Tabulka 2: Monitor obsazenosti svazků [zdroj: vlastní]

Monitor:	Obsazenosti souborového systému
Kategorie:	Systém
Stupeň závažnosti:	Chyba
Měřitelné kritérium:	Volba hraniční hodnoty
Popis:	Je posláno hlášení, jestliže se obsazenost svazku dostane nad 80% hranici celkové kapacity

Tabulka 3: Monitor vytížení diskových jednotek [zdroj: vlastní]

Monitor:	Disková aktivita
Kategorie:	Systém
Stupeň závažnosti:	Varování
Měřitelné kritérium:	Volba hraniční hodnoty a stupně závažnosti
Popis:	Je posláno hlášení, jestliže je vytížení diskových jednotek čtecími a zápisovými operacemi nad 90%

Tabulka 4: Monitor využití systémové a virtuální paměti [zdroj: vlastní]

Monitor:	Využití virtuální a systémové paměti
Kategorie:	Systém
Stupeň závažnosti:	Varování
Měřitelné kritérium:	Volba hraniční hodnoty a stupně závažnosti
Popis:	Je posláno hlášení, jestliže je využití systémové paměti na 100% a virtuální na 80%

Tabulka 5: Monitor vytížení CPU [zdroj: vlastní]

Monitor:	CPU aktivita

Kategorie:	Systém
Stupeň závažnosti:	Varování
Měřitelné kritérium:	Volba hraniční hodnoty a stupně závažnosti
Popis:	Je posláno hlášení, jestliže dojde k využití procesoru na 80%

Tabulka 6: Monitor dostupnosti emailového serveru [zdroj: vlastní]

Monitor:	TCP - Dostupnost emailového serveru
Kategorie:	Síť
Stupeň závažnosti:	Chyba
Měřitelné kritérium:	Volba hraniční hodnoty
Popis:	Je posláno hlášení, jestliže je doba odpovědí větší než 500ms nebo odpověď nedorazí do 2000ms

Tabulka 7: Monitor dostupnosti záložního clusterového uzlu [zdroj: vlastní]

Monitor:	PING - Dostupnost záložního clusterového uzlu
Kategorie:	Síť
Stupeň závažnosti:	Chyba
Měřitelné kritérium:	Volba hraniční hodnoty
Popis:	Je posláno hlášení, jestliže je doba odpovědí větší než 500ms nebo odpověď nedorazí do 2000ms

Tabulka 8: Monitor velikosti Before-Image souboru [zdroj: vlastní]

Monitor	Velikost Before-Image souboru
Kategorie	Soubor
Stupeň závažnosti	Varování
Měřitelné kritérium	Volba hraniční hodnoty a stupně závažnosti
Popis:	Je posláno hlášení, jestliže velikost BI souboru překročí 4GB

Tabulka 9: Monitor velikosti After-Image souboru [zdroj: vlastní]

Monitor:	Velikost After-Image souboru
Kategorie:	Soubor
Stupeň závažnosti:	Varování
Měřitelné kritérium:	Volba hraniční hodnoty a stupně závažnosti
Popis:	Je posláno hlášení, jestliže velikost AI souboru překročí 4GB

Tabulka 10: Monitor abnormální ukončení produkční databáze [zdroj: vlastní]

Monitor:	Abnormální ukončení produkční databáze
Kategorie:	OpenEdge – Databáze
Stupeň závažnosti:	Závažné
Měřitelné kritérium:	Procentuální míra dostupnosti
Popis:	Je posláno hlášení, jestliže se do databázového logu zapíše

	abnormální ukončení databáze

Tabulka 11: Monitor normální ukončení produkční databáze [zdroj: vlastní]

Monitor:	Normální ukončení produkční databáze
Kategorie:	OpenEdge – Databáze
Stupeň závažnosti:	Informace
Měřitelné kritérium:	Volba stupně závažnosti a nutnost monitorování
Popis:	Je posláno hlášení, jestliže se do databázového logu zapíše normální ukončení databáze

Tabulka 12: Monitor normální start produkční databáze [zdroj: vlastní]

Monitor:	Normální nastartování produkční databáze
Kategorie:	OpenEdge – Databáze
Stupeň závažnosti:	Informace
Měřitelné kritérium:	Volba stupně závažnosti a nutnost monitorování
Popis:	Je posláno hlášení, jestliže se do databázového logu zapíše normální nastartování databáze

Tabulka 13: Monitor abnormální ukončení monitorovacího agenta [zdroj: vlastní]

Monitor:	Abnormální ukončení monitorovacího agenta
Kategorie:	OpenEdge – Databáze
Stupeň závažnosti:	Varovaní
Měřitelné kritérium:	Volba stupně závažnosti
Popis:	Je posláno hlášení, jestliže se do databázového logu zapíše abnormální ukončení monitorovacího agenta

Tabulka 14: Monitor normální ukončení monitorovacího agenta [zdroj: vlastní]

Monitor:	Normální ukončení monitorovacího agenta
Kategorie:	OpenEdge – Databáze
Stupeň závažnosti:	Informace
Měřitelné kritérium:	Volba stupně závažnosti a nutnost monitorování
Popis:	Je posláno hlášení, jestliže se do databázového logu zapíše normální ukončení monitorovacího agenta

Tabulka 15: Monitor normální start monitorovacího agenta [zdroj: vlastní]

Monitor:	Normální start monitorovacího agenta
Kategorie:	OpenEdge – Databáze
Stupeň závažnosti:	Informace
Měřitelné kritérium:	Volba stupně závažnosti a nutnost monitorování
Popis:	Je posláno hlášení, jestliže se do databázového logu zapíše normální start monitorovacího agenta

Tabulka 16: Monitor abnormální ukončení aplikačního serveru [zdroj: vlastní]

Monitor:	Abnormální ukončení aplikační serveru
Kategorie:	OpenEdge – AppServer
Stupeň závažnosti:	Chyba
Měřitelné kritérium:	
Popis:	Je posláno hlášení, jestliže se do logu aplikační serveru zapíše abnormální ukončení AppServeru

Tabulka 17: Monitor normální ukončení aplikačního serveru [zdroj: vlastní]

Monitor:	Normální ukončení aplikační serveru
Kategorie:	OpenEdge – AppServer
Stupeň závažnosti:	Informace
Měřitelné kritérium:	Volba stupně závažnosti a nutnost monitorování
Popis:	Je posláno hlášení, jestliže se do logu aplikační serveru zapíše normální ukončení AppServeru

Tabulka 18: Monitor normální start aplikačního serveru [zdroj: vlastní]

Monitor:	Normální start aplikačního serveru
Kategorie:	OpenEdge – AppServer
Stupeň závažnosti:	Informace
Měřitelné kritérium:	Volba stupně závažnosti a nutnost monitorování
Popis:	Je posláno hlášení, jestliže se do logu aplikační serveru zapíše normální start AppServeru

Tabulka 19: Monitor nedostupný nameserver [zdroj: vlastní]

Monitor:	Nedostupný nameserver
Kategorie:	OpenEdge – AppServer
Stupeň závažnosti:	Chyba
Měřitelné kritérium:	Redundance monitoru - nameserver
Popis:	Je posláno hlášení, jestliže se v logu aplikačního serveru objeví zápis o nedostupnosti nameserveru

Tabulka 20: Monitor nedostupný aplikační server [zdroj: vlastní]

Monitor:	Nedostupný aplikační server
Kategorie:	OpenEdge – AppServer
Stupeň závažnosti:	Varování
Měřitelné kritérium:	Volba stupně závažnosti
Popis:	Je posláno hlášení, jestliže se na aplikačním serveru vyčerpá počet připojení

Tabulka 21: Monitor abnormální ukončení nameserveru [zdroj: vlastní]

Monitor:	Abnormální ukončení nameserveru

Kategorie:	OpenEdge – Nameserver
Stupeň závažnosti:	Chyba
Měřitelné kritérium:	Redundance monitoru - appserver
Popis:	Je posláno hlášení, jestliže se do logu nameserveru zapíše abnormální ukončení

Tabulka 22: Monitor normální ukončení nameserver [zdroj: vlastní]

Monitor:	Normální ukončení nameserveru
Kategorie:	OpenEdge – Nameserver
Stupeň závažnosti:	Informace
Měřitelné kritérium:	Volba stupně závažnosti a nutnost monitorování
Popis:	Je posláno hlášení, jestliže se do logu nameserveru zapíše normální ukončení

Tabulka 23: Monitor normální start nameserver [zdroj: vlastní]

Monitor:	Normální start nameserveru
Kategorie:	OpenEdge – Nameserver
Stupeň závažnosti:	Informace
Měřitelné kritérium:	Volba stupně závažnosti a nutnost monitorování
Popis:	Je posláno hlášení, jestliže se do logu nameserveru zapíše normální start

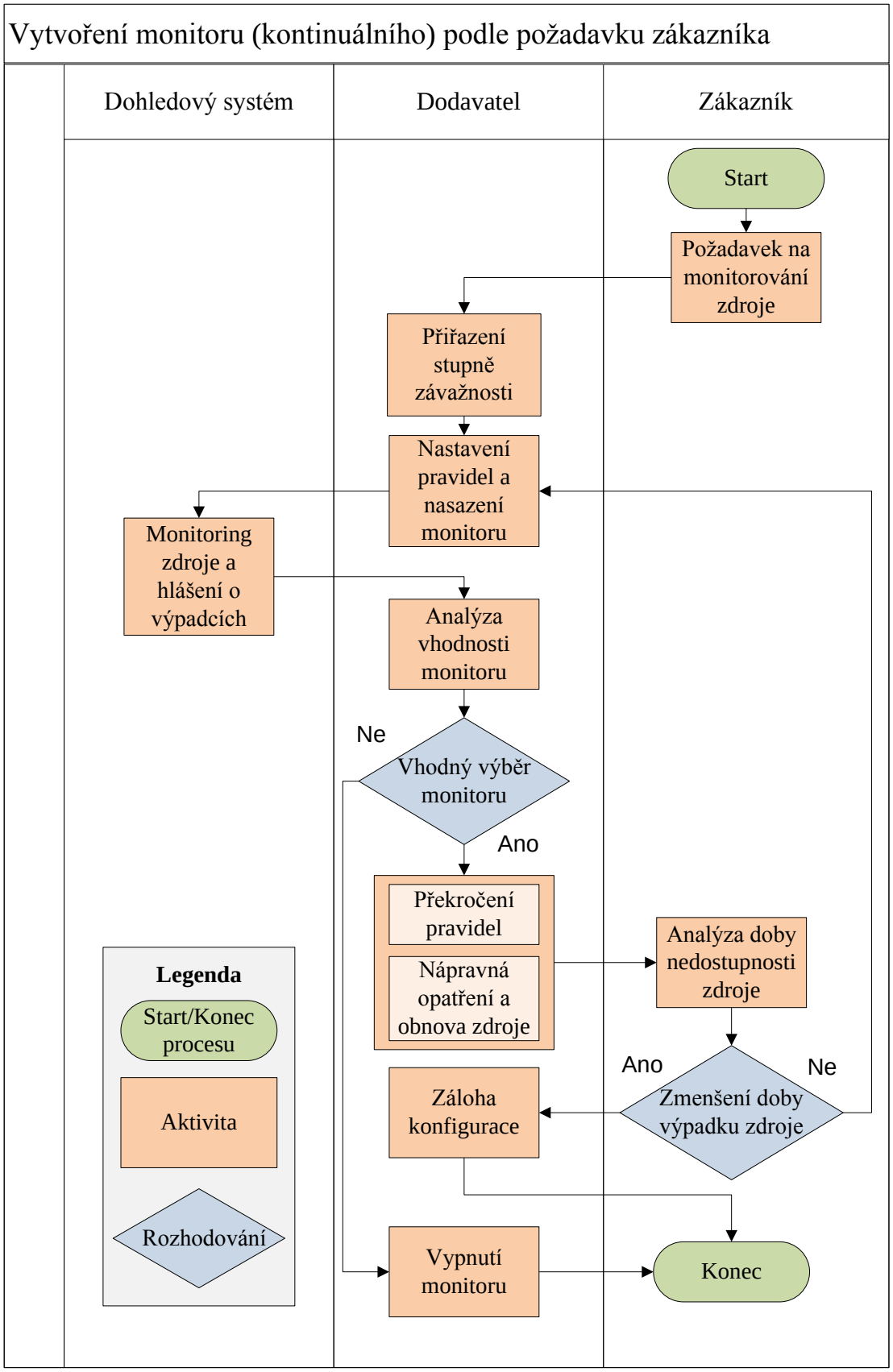
Tabulka 24: Monitor nameserver Broker se stejným UUID [zdroj: vlastní]

Monitor:	Nameserver Broker se stejným UUID (Universal Unique Identifier)
Kategorie:	OpenEdge – Nameserver
Stupeň závažnosti:	Varování
Měřitelné kritérium:	Volba stupně závažnosti
Popis:	Je posláno hlášení, jestliže se broker nameserveru snaží registrovat s již už použitým UUID

Tabulka 25: Monitor vypršení časového limitu odpovědi nameserveru [zdroj: vlastní]

Monitor:	Vypršení časového limitu odpovědi nameserveru
Kategorie:	OpenEdge – Nameserver
Stupeň závažnosti:	Varování
Měřitelné kritérium:	Volba stupně závažnosti, redundance monitoru
Popis:	Je posláno hlášení, jestliže se broker nameserveru neodpovídá, přičemž je nastartovaný

6.4. Model činností při postupu vytvoření monitoru



Obrázek 11: Modelu aktivit při postupu vytváření monitoru; SW MS Visio (zdroj: vlastní)

Z modelu aktivit (Obrázek 11) je vidět, kdo z jakých účastníků zodpovídá za jednotlivé aktivity od začátku procesu vytvoření nového monitoru po zálohu konfigurace či případně vypnutí špatně zvoleného monitoru.

6.5. Identifikace a rozdělení zákazníka

Nejprve je nutné identifikovat a rozdělit jednotlivé zákazníky, jakým způsobem přistupují k procesu požadavku vytvoření monitoru zdroje, který má být sledován.

Interní zákazník - je každý zaměstnanec organizace. Pro své aktivity přebírá jako vstupy výsledky aktivit svých spolupracovníků. Výsledek své práce předává dalším. Každý z nich má konkrétní požadavky, jejichž splnění je nezbytné pro provedení činnosti v rámci stanovených odpovědností. Pro interního zákazníka je typické, že je vždy zároveň zákazníkem i dodavatelem v jedné osobě. V našem případě se jedná o to, že požadavek na vytvoření monitoru vzejde od zaměstnance dodavatelské firmy, který bude v roli interního zákazníka. Jeho požadavky se mohou jednat o např. sledování z důvodu výkonnostních či ladění chodu informačního systému [25].

Externí zákazník - je subjekt přijímající produkt, který bezprostředně používá či bezplatně postupuje k užití dalším osobám nebo dále prodává pro účely dalšího zpracování a pro potřeby konečného užití. V našem případě to je společnost, která si objednala monitorování informačního systému a vytváří si požadavky na monitory zdrojů, které jsou nezbytné pro nepřetržitý chod informačního systému a byznys procesů společnosti[25].

Nutnost klasifikace zákazníka - závěr

Po důkladném rozboru všech informací o zákaznících se dospělo k názoru, že není nutné je rozdělovat na interního a externího. A to z důvodů, že oba mají stejné požadavky na monitorování zdrojů a požadují stejné výstupy monitoringu.

6.6. Základní nastavení monitorů podle jednotlivých kategorií

V základním nastavení monitorů jsou definována pravidla, podle kterých bude daný zdroj monitorován. Dále se určí interval, v kterém se bude pravidlo opakovat a zjišťovat stav zdroje. Počet hlášení znamená, kolikrát se může vyskytnout překročení pravidel, než se vygeneruje zpráva pro obsluhu dohledu. A v poslední řadě se nastaví stupeň závažnosti monitoru.

Tabulka 26: Nastavení pravidel pro kategorii systém [zdroj: vlastní]

Monitor	Pravidlo	Interval	Hlášení	Závažnosti
Souborový systém /zpone/data	obsazenost 90% a více	5 minut	1	chyba
Souborový systém /zpone/idx	obsazenost 90% a více	5 minut	1	chyba
Souborový systém /zpone/ai	obsazenost 90% a více	5 minut	1	chyba
Souborový systém/zpone/bi	obsazenost 90% a více	5 minut	1	chyba
Souborový systém /zpone/apl	obsazenost 90% a více	5 minut	1	chyba
Souborový systém /zpone/pscwrk	obsazenost 90% a více	5 minut	1	chyba
Disková aktivita	vytížení na 90% a více	5 minut	2	varování
Využití virtuální a systémové paměti	systémová paměť na 100%; virtuální na 80% a více	5 minut	2	varování
CPU aktivita	vytížení CPU na 80% a více	5 minut	2	varování

Tabulka 27: Nastavení pravidel pro kategorii síť [zdroj: vlastní]

Monitor	Pravidlo	Interval	Hlášení	Závažnosti
SMPT_MAIL (TCP)	odpověď větší než 500ms nebo bez odpovědi 2000ms	2 minut	1	chyba
PING_cluster_node	odpověď větší než 500ms nebo bez odpovědi 2000ms	2 minut	1	chyba

Tabulka 28: Nastavení pravidel pro kategorii soubor [zdroj: vlastní]

Monitor	Pravidlo	Interval	Hlášení	závažnosti
Velikost souboru /zpone/ai/zpone.a1	Kontrola velikosti AI souboru větší než 4 GB	5 minut	1	Informace
Velikost souboru /zpone/ai/zpone.a2	Kontrola velikosti AI souboru větší než 4 GB	5 minut	1	Informace
Velikost souboru /zpone/ai/zpone.a3	Kontrola velikosti AI souboru větší než 4 GB	5 minut	1	Informace
Velikost souboru /zpone/bi/zpone.b1	Kontrola velikosti BI souboru větší než 4 GB	5 minut	1	informace

Tabulka 29: Nastavení pravidel pro kategorii OE - databáze [zdroj: vlastní]

Monitor	Pravidlo	Interval	Hlášení	závažnosti
Abnormální ukončení databáze	Výskyt klíčového slova v databázovém logu	5 minut	1	Závažné
Abnormální ukončení agenta	Výskyt klíčového slova v databázovém logu	5 minut	1	Varování
Normální ukončení databáze	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace
Normální ukončení agenta	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace
Normální start databáze	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace

Monitor	Pravidlo	Interval	Hlášení	závažnosti
Normální start agenta	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace

Tabulka 30: Nastavení pravidel pro kategorii OE - aplikační server [zdroj: vlastní]

Monitor	Pravidlo	Interval	Hlášení	závažnosti
Abnormální ukončení appserveru	Výskyt klíčového slova v databázovém logu	5 minut	1	Chyba
Normální ukončení appserveru	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace
Normální start appserveru	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace
Nedostupný nameserver	Výskyt klíčového slova v databázovém logu	5 minut	1	Chyba
Nedostupný appserver	Výskyt klíčového slova v databázovém logu	5 minut	1	Chyba

Tabulka 31: Nastavení pravidel pro kategorii OE - nameserver [zdroj: vlastní]

Monitor	Pravidlo	Interval	Hlášení	závažnosti
Abnormální ukončení nameserveru	Výskyt klíčového slova v databázovém logu	5 minut	1	Chyba
Normální ukončení nameserveru	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace
Normální start nameserveru	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace
Nameserver se stejným UUID	Výskyt klíčového slova v databázovém logu	5 minut	1	Varování
Vypršení časového limitu odpovědi ns	Výskyt klíčového slova v databázovém logu	5 minut	1	Varování

7. Verifikace modelu

7.1. Vyhodnocení a návrh monitorů č. 1

Po dvouměsíčním monitorování informačního systému vyšlo najevo, že je potřeba jednotlivá pravidla monitorů upravit, rozšířit resp. ukončit. Výsledky se vyhodnocují podle jednotlivých technologických kategorií.

Pro ověření modelu procesu „Vytvoření monitoru podle požadavku zákazníka“ byly vybrány takové požadavky, které pokrývají základní rozsah monitorovaných zdrojů a pocházejí, jak od externího, tak i od interního zákazníka. Tím to se ověří již zjištěná skutečnost, že není rozdíl mezi zákazníky.

7.1.1. Kategorie systém

Během monitorování došlo ke kritické situaci, kdy při provádění celoroční sestavy docházelo k enormnímu nárůstu velikosti AI a BI souborů (řadově 700mb za minutu). Tento stav byl zapříčiněn chybnou volbou datového typu databázové položky. Jelikož pravidlo na monitorování obsazenosti diskových svazku je nastaveno na 90%, tak zbývalo obsluze monitoringu velice krátký čas na řešení této vážné situace. Z tohoto důvodu bylo vytvořeno nové pravidlo monitoru, kde hranice pro hlášení je nastavena na 70%. Dále bylo toto pravidlo rozšířeno na všechny diskové svazky systému, které jsou bezprostředně nutné pro jeho chod.

Vytvoření nového pravidla

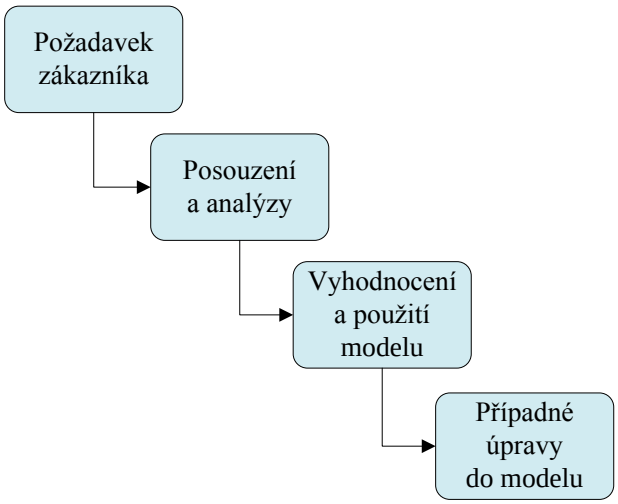
Tabulka 32: Nové pravidlo kategorie systém [zdroj: vlastní]

Monitor	Pravidlo	Interval	Hlášení	závažnosti
Souborové svazky systému	obsazenost 70% a více	5 minut	1	Varování

7.1.2. Ověření postupu vytváření nového monitoru podle modelu procesu vytvoření monitoru podle požadavku zákazníka

Od externího zákazníka byl podán požadavek na monitorování obsazenosti jednotlivých souborových svazků. Rozbor požadavku bylo zjištěno, že monitor spadá do technologické kategorie „Systém“ a do skupiny kontinuálních monitorů. Byl mu přiřazen třetí stupeň závažnosti tj. chyba a to proto, že výpadek tohoto zdroje může zapříčinit výpadek velké části informačního systému. Další krokem bylo nastavení pravidel monitoru. Analýzou výsledků, zda mají chybová hlášení vypovídající hodnotu, byl potvrzen vhodný výběr vhodného typu

monitoru. Pomocí druhé analýzy dostupnosti zdroje bylo zjištěno, že pravidla monitoru jsou nedostatečně nastavena a proto se vytvořilo nové pravidlo, které má parametry podle Tabulky 32. Po opětovném průběhu analýz, byl monitor shledán, jako vyhovují a byla provedena záloha jeho konfigurace. Z výsledků vyplívá, že v provozní větvi modelu procesu vytvoření monitoru podle požadavku zákazníka zafungovala zpětná vazba pro úpravu monitorovacích pravidel, ale bylo zjištěno, že v modelu chybí činnost, která provádí rozbor požadavků zákazníka. Dále zde chybí rozhodovací mechanismus, který na základě rozboru požadavku rozhodne, zda je monitor proveditelný nebo ne. Proto bude model o tyto činnosti rozšířen.



Obrázek 12: Postup ověření modelu procesu vytvoření monitoru podle požadavku zákazníka v SW MS Visio [zdroj: vlastní]

7.1.3. Kategorie síť

V této kategorii zatím nebyly zjištěny žádné nedostatky.

7.1.4. Kategorie soubor

Z důvodu, že zálohování produkční databáze během monitorování 3krát korektně neproběhlo a správce zákazníka nebyl dostatečně o tomto stavu informován, byl od zákazníka podán požadavek na vytvoření monitoru, který by řešil tuto situaci. Proto byl vytvořen monitor s pravidlem, které prohledává výstupní log zálohování a hledá v něm klíčová slova a v případě výskytu slovního spojení „backup status error“ bude posláno varovné hlášení.

Tabulka 33: Nové monitor kategorie soubor [zdroj: vlastní]

Monitor	Pravidlo	Interval	Hlášení	závažnosti
Kontrola zálohování databáze	Výskyt klíčového slova v logu zálohování	1 den	1	Varování

7.1.5. Kategorie OpenEdge

OpenEdge – Databáze:

Z důvodu přehlednosti se ukončily monitory na normální ukončení a start databáze a monitorovacího agenta. Tyto akce se provádějí plánovaně a není potřeba je proto monitorovat.

Tabulka 34: Zrušení monitorů kategorie OE - databáze [zdroj: vlastní]

Monitor	Pravidlo	Interval	Hlášení	závažnosti
Normální ukončení databáze	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace
Normální ukončení agenta	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace
Normální start databáze	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace
Normální start agenta	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace

OpenEdge – AppServer:

Z důvodu přehlednosti se ukončily monitory na normální ukončení a start aplikačního serveru. Tyto akce se provádějí plánovaně a není potřeba je proto monitorovat.

Tabulka 35: Zrušení monitorů kategorie OE - aplikační server [zdroj: vlastní]

Monitor	Pravidlo	Interval	Hlášení	závažnosti
Normální ukončení appserveru	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace
Normální start appserveru	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace

OpenEdge – Nameserver:

Z důvodu přehlednosti se ukončily monitory na normální ukončení a start nameserveru. Tyto akce se provádějí plánovaně a není potřeba je proto monitorovat.

Tabulka 36: Zrušení monitorů kategorie OE - nameserver [zdroj: vlastní]

Monitor	Pravidlo	Interval	Hlášení	závažnosti
Normální ukončení nameserveru	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace
Normální start nameserveru	Výskyt klíčového slova v databázovém logu	5 minut	1	Informace

7.2. Vyhodnocení dostupnosti provozní databáze a aplikačního serveru

Podle rovnice (2.1) se vypočítá dostupnost provozní databáze IS v kalendářním měsíci dubnu, jestliže je znám režim tj. 24 x 7. Z toho vychází celková doba provozu na 720 hodin. Celkový úhrn hodin očekávaných a neočekávaných odstávek provozní databáze za tento kalendářní měsíc se dostal na hodnotu 7 hodin. Tato hodnota se z velké části skládá z plánovaných odstávek, které byly způsobeny z důvodu úpravy datové struktury databáze. Nyní jsou známy všechny hodnoty a je možnou dosadit do rovnice.

$$0{,}9903 = \frac{720}{720 + 7} \tag{7.1}$$

Po vynásobení 100 a zaokrouhlení se dostává procentuální vyjádření dostupnosti databáze v hodnotě 99%. Tato hodnota splňuje motivační úroveň tvrdé metriky SLA (kapitola 2.2.2.).

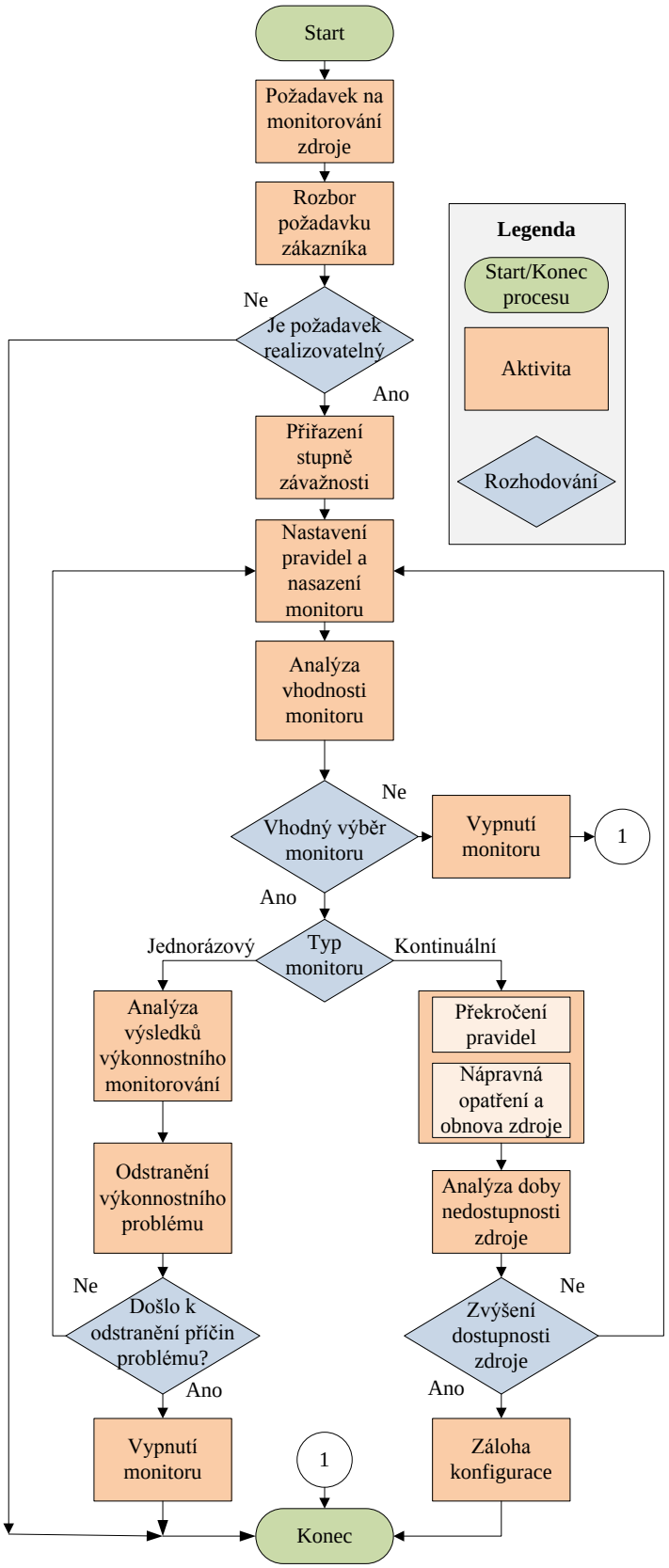
Celková suma hodin očekávaných a neočekávaných odstávek aplikačního serveru za měsíc duben je 9 hodin a 15 minut. Tato hodnota se z velké části tvoří plánované odstávky, které byly způsobeny z důvodu instalace nové verze uživatelského software. Nyní se hodnoty dosadí do rovnice (2.1).

$$0{,}9873 = \frac{720}{720 + 9{,}25} \tag{7.2}$$

Po vynásobení 100 a zaokrouhlení se dostává procentuální vyjádření dostupnosti aplikačního serveru v hodnotě 98,7%. Tato hodnota splňuje minimální úroveň tvrdé metriky SLA (kapitola 2.2.2.).

7.3. Upravený model vytvoření monitoru podle požadavku zákazníka

Upravený model průběhu procesu „Vytvoření monitoru podle požadavku zákazníka“ (obrázek č. 12) znázorňuje pozměněnou variantu aktivit, které je potřeba realizovat v případě zákazníkova požadavku na monitorování jím určeného zdroje. Jedná se o aktivity, které analyzují proveditelnost monitorovaní a případné ukončení procesu.



Obrázek 13: Inovovaný model vytvoření monitoru podle požadavku zákazníka; SW MS Visio [zdroj: vlastní]

7.4. Vyhodnocení a návrh monitorů č. 2

Po dalším dvouměsíčním monitorování informační systému vznikly od zákazníka požadavky na vytvoření monitoru na sledování konkrétního zdroje.

7.4.1. Síť

Během provozu informačního systému docházelo k výpadkům webové samoobsluhy, která slouží jako portál pro výpisy dat klientů zákazníka. Tento portál funguje na platformě Java Servlet. Z tohoto důvodu byl vytvořen monitor, který sleduje přístupnost TCP portu webového serveru, aby byl správce externího zákazníka informován o výpadku této služby.

Tabulka 37: Vytvoření nového monitoru kategorie síť [zdroj: vlastní]

Monitor	Pravidlo	Interval	Hlášení	závažnosti
Webová samoobsluha (TCP)	odpověď větší než 500ms nebo bez odpovědi 2000ms	2 minut	1	chyba

Ověření postupu vytváření nového monitoru podle modelu procesu vytvoření monitoru podle požadavku zákazníka

Od externího zákazníka byl podán požadavek na sledování činnosti webové samoobsluhy. Analýzou požadavku bylo zjištěno, že se jedná o monitor, který spadá do technologické kategorie „Síť“ a do skupiny kontinuálních monitorů. Tento požadavek je reálně proveditelný. Byl mu přiřazen druhý stupeň závažnosti tj. varování a to z toho důvodu, že výpadek toho zdroje neohrozí základní funkčnost celého informačního systému. Následně byla nastavena pravidla, která jsou uvedena v tabulce č. 36. Analýzou výsledků, zda mají chybová hlášení vypovídající hodnotu, byl potvrzen vhodný výběr vhodného typu monitoru. Druhou analýzou dostupnosti zdroje bylo zjištěno, že výpadek webové samoobsluhy se při monitorování pohyboval v řádově jednotkách minut. Zatím co při nemonitorovaném provozu to byly řádově desítky minut až hodin a většinou byl výpadek reklamován klienty zákazníka. Jako poslední krok byla provedena záloha a zadokumentování konfigurace monitoru. Vyhodnocením výsledků procesu vytváření nového monitoru se došlo k závěru, že inovovaný model procesu vytvoření monitoru podle požadavku zákazníka je vyhovující a není potřeba ho měnit.

7.4.2. Soubor

Byl podán požadavek od pracovníků z vývojového oddělení na vytvoření monitoru, který by sledoval výskyt dlouhých transakcí a to z důvodu, že od zákazníka přecházely hlášení o ztrátě

již vytvořených záznamů v databázi. Byl vytvořen program, který sleduje délku transakcí a výsledky vypisuje do výstupního logu, který je monitorován na výskyt klíčového slova.

Tabulka 38: Vytvoření nového monitoru kategorie soubor [zdroj: vlastní]

Monitor	Pravidlo	Interval	Hlášení	závažnosti
Kontrola dlouhých transakcí	Výskyt klíčového slova v logu transakcí	5 minut	1	Varování

Ověření postupu vytváření nového monitoru podle modelu procesu vytvoření monitoru podle požadavku zákazníka

Přijat požadavek o interního zákazníka (zaměstnanec dodavatelské společnosti) na sledování dlouhých transakcí. Analýzou požadavku bylo zjištěno, že monitor spadá do technologické kategorie „Soubor“ a do skupiny jednorázových monitorů. Tento požadavek je reálně proveditelný. Byl mu přiřazen první stupeň závažnost tj. informace a to z toho důvodu, že se jedná pouze o informativní hlášení bez jakéhokoliv dopadu na chod celého informačního systému. Pravidla byla nastavena podle Tabulky 38. Analýzou, zda mají chybová hlášení monitoru vypovídající hodnou, se dospělo k závěru, že byl zvolen vhodný typ monitoru. Na základě výsledků analýzy výsledků výkonnostního monitorování byla provedena opatření, která řeší výkonnostní problémy informačního systému. Následně byl monitor vypnut a provedena záloha jeho konfigurace. Vyhodnocením veškerých výsledků procesu vytváření nového monitoru se došlo k závěru, že inovovaný model procesu vytvoření monitoru podle požadavku zákazníka je vyhovující i včetně výkonnostní větve a není ho potřeba proto měnit.

7.5. Shrnutí

Po ověření první verze modelu procesu vytvoření monitoru podle požadavku zákazníka byly zjištěny nedostatky v chybějících činnostech. Jedná se zejména o činnost, která provádí rozbor zákaznických požadavků. Dále je zde chybějící rozhodovací mechanismus, který rozhodne, jestli požadavek na monitorování zdroje je reálně proveditelný v rámci možností monitorovacího systému. Dalším ověřením inovovaného modelu procesu vytvoření monitoru podle požadavku zákazníka (druhá verze modelu) nebyly shledány žádné nedostatky a tento model byl prohlášen za vyhovující.

8. Závěr

Cílem bakalářské práce bylo nakonfigurovat monitoring databáze tak, aby správce IS získal rychlý přehled důležitých informací, které by vedly k efektivnímu řešení kritických situací IS.

Zadání jsem si vybral záměrně, protože se v tomto oboru profesně pohybuji a problematika zvýšení dostupnosti IS, zvláště proaktivní monitoring, se v českých firmách velice opomíjí, i když jim může zachránit, jak jejich peníze, tak i jejich pověst.

Ve své bakalářské práci mám následující výstupy:

- Navrhnul jsem postup řešení pro tvorbu monitoru:
    - Na základě rozboru jsem provedl rozdělení monitorů do jednotlivých technologických kategorií.
    - Vytvořil jsem model pro vytvoření monitoru, podle kterého byla zhotovena prvotní konfigurace monitorů informačního systému.
- Provedl jsem verifikaci modelu:
    - Model jsem ověřil na monitorech, které sledují nejdůležitější oblast IS a implementace prvotní konfigurace do reálného provozu.
    - Na základě poznatků jsem provedl změny v modelu pro vytvoření monitoru a konfigurací monitorů.
    - Provedl jsem výpočet dostupnosti jednoho sledovaného zdroje.

Změny do modelu se provedl z důvodu, že v něm chyběly aktivity, které by analyzovaly, jestli je požadavek na monitorování od zákazníka realizovatelný nebo ne.

Pomocí upraveného modelu byla vytvořena taková konfigurace monitorů, která sleduje kritické zdroje IS a dává tak, obsluze dohledu, tak i zákazníkovi přesný přehled o stavu IS, tak zvýšit jeho dostupnost. Tento fakt byl ověřen výpočtem dostupnosti produkční databáze, jehož výsledkem byla hodnota 99%, přičemž tato hodnota spadá do motivační servisní úrovně metrik SLA. Proto konstatuji, že požadavky zadání a stanovený cíl byly v rámci bakalářské práce splněny.

9. Použitá literatura

[1.] BACKMAN, Adam. *OpenEdge Revealed : Mastering the OpenEdge Database with OpenEdge Management*. Release 3.1C. Bedford(Massachusetts) : Progress Software Corporation, 2008. 266 p. ISBN 978-0-923562-08-3.

[2.] BRUCKNER, Tomáš; VOŘÍŠEK, Jiří. *Outsourcing a jeho aplikace při řízení informačního systému podniku*. 1. vyd. Praha : Ekopress, 1998. 119 s. ISBN 80-86119-07-6.

[3.] *Convenio Consulting* [online]. 2006 [cit. 2010-06-22]. Business Continuity plán. Dostupné z WWW: <http://www.convenio.cz/documents/business_continuity.pdf>.

[4.] *Convenio Consulting* [online]. 2006 [cit. 2010-06-22]. Disaster Recovery plán. Dostupné z WWW: <http://www.convenio.cz/documents/DR_plan.pdf>.

[5.] *Havarijní plány* [online]. c2003 [cit. 2010-06-21]. It-security.cz. Dostupné z WWW: <http://www.it-security.cz/sluzby/havarijni-plany.html>.

[6.] HOFRICHTER, Kamil; JURČA , Radomír. Základní aspekty outsourcingu IT. *IT Systems* [online]. 2005, roč. 7, č. 4, [cit. 2010-06-21]. Dostupný z WWW: <http://www.systemonline.cz/outsourcing-ict/zakladni-aspekty-outsourcingu-it-1.htm>. ISSN 1802-615X.

[7.] HORA, Michal. Tajemství zkratky SLA : Service level agreement je klíčovým dokumentem při poskytování IT služeb. *IT Systems* [online]. 2005, roč. 7, č. 4, [cit. 2010-06-21]. Dostupný z WWW: <http://www.systemonline.cz/clanky/tajemstvi-zkratky-sla.htm>. ISSN 1802-615X.

[8.] KAČMAŘÍK, Radim. Citrix EdgeSight : proaktivní monitoring IT prostředí. *Read.me* [online]. 2007, roč. 2, č. 1, [cit. 2010-06-23]. Dostupný z WWW: <http://www.arrowecs.cz/web/infobaze.nsf/info/readme_1_2007/$file/Citrix%20EdgeSight.pdf>.

[9.] KOCH, Miloš; ONDRÁK, Viktor. *Informační systémy a technologie*. 1. vyd. Brno : Akademické nakladatelství CERM, 2004. 166 s. ISBN 80-214-2725-6.

[10.] KOMÁRKOVÁ, Jitka, et al. *Úvod do informačních systémů : pro kombinovanou formu studia*. 1. vyd. Pardubice : Univerzita Pardubice, 2006. 85 s. ISBN 80-7194-870-5.

[11.] KRÁL, Jaroslav. *Informační systémy : specifikace, realizace, provoz*. 1. vyd. Veletiny : Science, 1998. 358 s. ISBN 80-86083--00-4.

[12.] MOLNÁR, Zdeněk. *Efektivnost informačních systémů*. 2. rozš. vyd. Praha : Grada, 2001. 179 s. ISBN 80-247-0087-5.

[13.] *OpenEdge® Management : Alerts Guide and Reference* [online]. Release 10.2A. Bedford(Massachusetts) : Progress Software Corporation, 2009 [cit. 2010-06-22]. Dostupné z WWW: <http://communities.progress.com/pcom/servlet/JiveServlet/download/16371-1-15495/far.pdf>.

[14.] POLOZOFF, Alexandre. *IBM : Technical library* [online]. 09.04.2003 [cit. 2010-06-21]. Proactive Application Monitoring. Dostupné z WWW: <http://www.ibm.com/developerworks/websphere/library/techarticles/0304_polozoff/polozoff.html>.

[15.] RYDVALOVÁ, Petra; RYDVAL, Jiří. *Outsourcing ve firmě : průvodce pro manažera s tipy pro české prostředí*. 1. vyd. Brno : Computer Press, 2007. 102 s. ISBN 978-80-251-1807-8.

[16.] SABO, Jan. Dostupnost především. *Progress : Magazín profesionálních uživatelů Progressu* [online]. 2004, roč. 10, č. 1, [cit. 2010-06-22]. Dostupný z WWW: <http://www.progress.com/progress_software/worldwide_sites/cz/docs/casposis/070913d.pdf>.

[17.] SCHMIDT, Klaus. *High Availability and Disaster Recovery : Concepts, Design, Implementation*. 1st edition. Berlin : Springer, 2006. 410 p. ISBN 978-3-540-24460-8.

[18.] SVATÁ, Vlasta. *Projektové řízení v podmínkách ERP systémů*. 1. vyd. Praha : Vysoká škola ekonomická, 2002. 116 s. ISBN 80-245-0266-6.

[19.] *Svetstorage.info* [online]. c2010 [cit. 2010-06-22]. Spolehlivost, dostupnost a obslužnost (RAS). Dostupné z WWW: <http://www.svetstorage.info/spolehlivost-dostupnost-obsluznost.php?p=23>.

[20.] ŠIMONOVÁ, Stanislava. *Modelování procesů a dat pro zvýšení kvality*. 1. vyd. Pardubice : Univerzita Pardubice, Fakulta ekonomicko-správní, 2009. 192 s. ISBN 978-80-7395-205-1.

[21.] TRUPL, Jan; ZEMAN, Jan. *Trask : Odborné články* [online]. 14.06.2006 [cit. 2010-06-21]. Business Continuity Planning aneb jak správným plánováním minimalizovat rizika. Dostupné z WWW: <http://www.trask.cz/DeliverLive/Odborne_clanky-14.6.06_-_Pl%C3%A1nov%C3%A1n%C3%AD_kontinuity_%C4%8Dinnost%C3%AD~79~1~746>.

[22.] UČEŇ, Pavel. *Systems Integration Conference Archive* [online]. 2003 [cit. 2010-06-22]. Metriky jako nástroj řízení efektivity IS/IT. Dostupné z WWW: <http://si.vse.cz/archive/proceedings/2003/dimenzovani-informatiky-jako-podpurneho-procesu.pdf>.

[23.] VACULÍK, Josef, et al. *Marketing : pro kombinovanou formu studia. 1. díl*. 1. vyd. Pardubice : Univerzita Pardubice, 2005. 108 s. ISBN 80-7194-812-8.

[24.] VARGAS, Enrique. *Blueprints - wikis.sun.com* [online]. 2000 [cit. 2010-06-22]. High Availability Fundamentals. Dostupné z WWW: <http://www.sun.com/blueprints/1100/HAFund.pdf>.

[25.] VEBER, Jaromír, et al. *Řízení jakosti a ochrana spotřebitele*. 2. aktualiz. vyd. Praha : Grada, 2007. 201 s. ISBN 978-80-247-1782-1.

[26.] VODRÁK, Ivo. *Metody byznys modelování : pro kombinované a distanční studium*. Ostrava : VŠB – Technická univerzita Ostrava, 2004. 91 s. Dostupné z WWW: <http://vondrak.cs.vsb.cz/download/Metody_byznys_modelovani.pdf>.

10. Přílohy

Příloha A – Kompletní seznam ověřených monitorů IS podle kategorií

Tabulka 39: Kompletní seznam ověřených monitorů IS podle kategorií (zdroj: vlastní)

Kategorie - Systém				
Monitor	**Pravidlo**	**Interval**	**Hlášení**	**závažnosti**
Souborový systém /zpone/data	obsazenost 90% a více	5 minut	1	chyba
Souborový systém /zpone/idx	obsazenost 90% a více	5 minut	1	chyba
Souborový systém /zpone/ai	obsazenost 90% a více	5 minut	1	chyba
Souborový systém /zpone/bi	obsazenost 90% a více	5 minut	1	chyba
Souborový systém /zpone/apl	obsazenost 90% a více	5 minut	1	chyba
Souborový systém /zpone/pscwrk	obsazenost 90% a více	5 minut	1	chyba
Disková aktivita	vytížení na 90% a více	5 minut	2	varování
Využití virtuální a systémové paměti	systémová paměť na 100%; virtuální na 80% a více	5 minut	2	varování
CPU aktivita	vytížení CPU na 80% a více	5 minut	2	varování

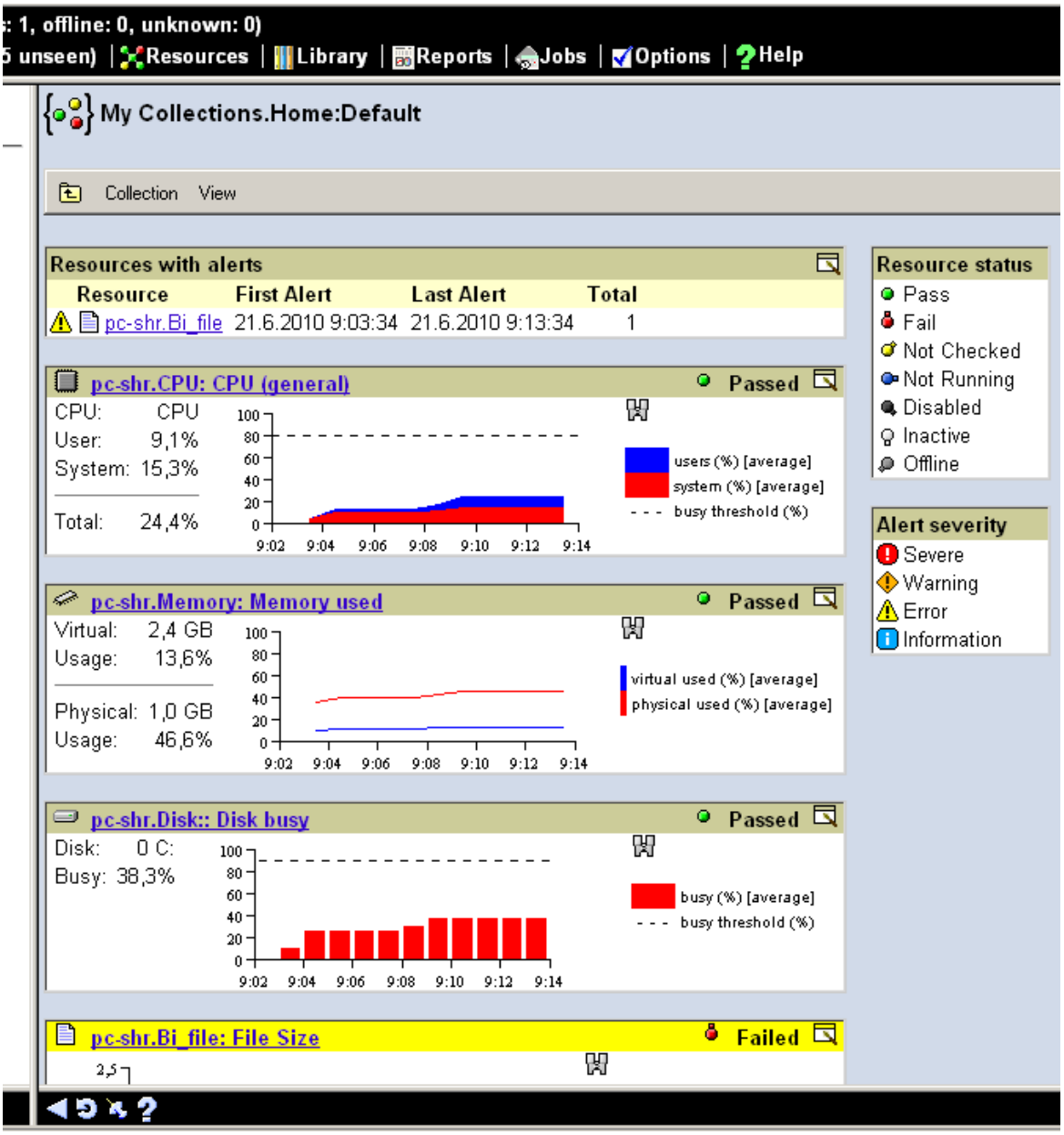
Kategorie - Síť				
Monitor	**Pravidlo**	**Interval**	**Hlášení**	**závažnosti**
SMPT_MAIL (TCP)	odpověď větší než 500ms nebo bez odpovědi 2000ms	2 minut	1	chyba
PING_cluster_node	odpověď větší než 500ms nebo bez odpovědi 2000ms	2 minut	1	chyba
Webová samoobsluha (TCP)	odpověď větší než 500ms nebo bez odpovědi 2000ms	2 minut	1	chyba

Kategorie - Soubor				
Monitor	**Pravidlo**	**Interval**	**Hlášení**	**závažnosti**
Velikost souboru /zpone/ai/zpone.a1	Kontrola velikosti AI souboru větší než 4 GB	5 minut	1	Informace
Velikost souboru /zpone/ai/zpone.a2	Kontrola velikosti AI souboru větší než 4 GB	5 minut	1	Informace
Velikost souboru /zpone/ai/zpone.a3	Kontrola velikosti AI souboru větší než 4 GB	5 minut	1	Informace
Velikost souboru /zpone/bi/zpone.b1	Kontrola velikosti BI souboru větší než 4 GB	5 minut	1	Informace
Kontrola zálohování databáze	Výskyt klíčového slova v logu zálohování	1 den	1	Varování
Kontrola dlouhých transakcí	Výskyt klíčového slova v logu transakcí	5 minut	1	Varování

Kategorie - Databáze				
Monitor	**Pravidlo**	**Interval**	**Hlášení**	**závažnosti**
Abnormální ukončení databáze	Výskyt klíčového slova v databázovém logu	5 minut	1	Závažné
Abnormální ukončení agenta	Výskyt klíčového slova v databázovém logu	5 minut	1	Varování

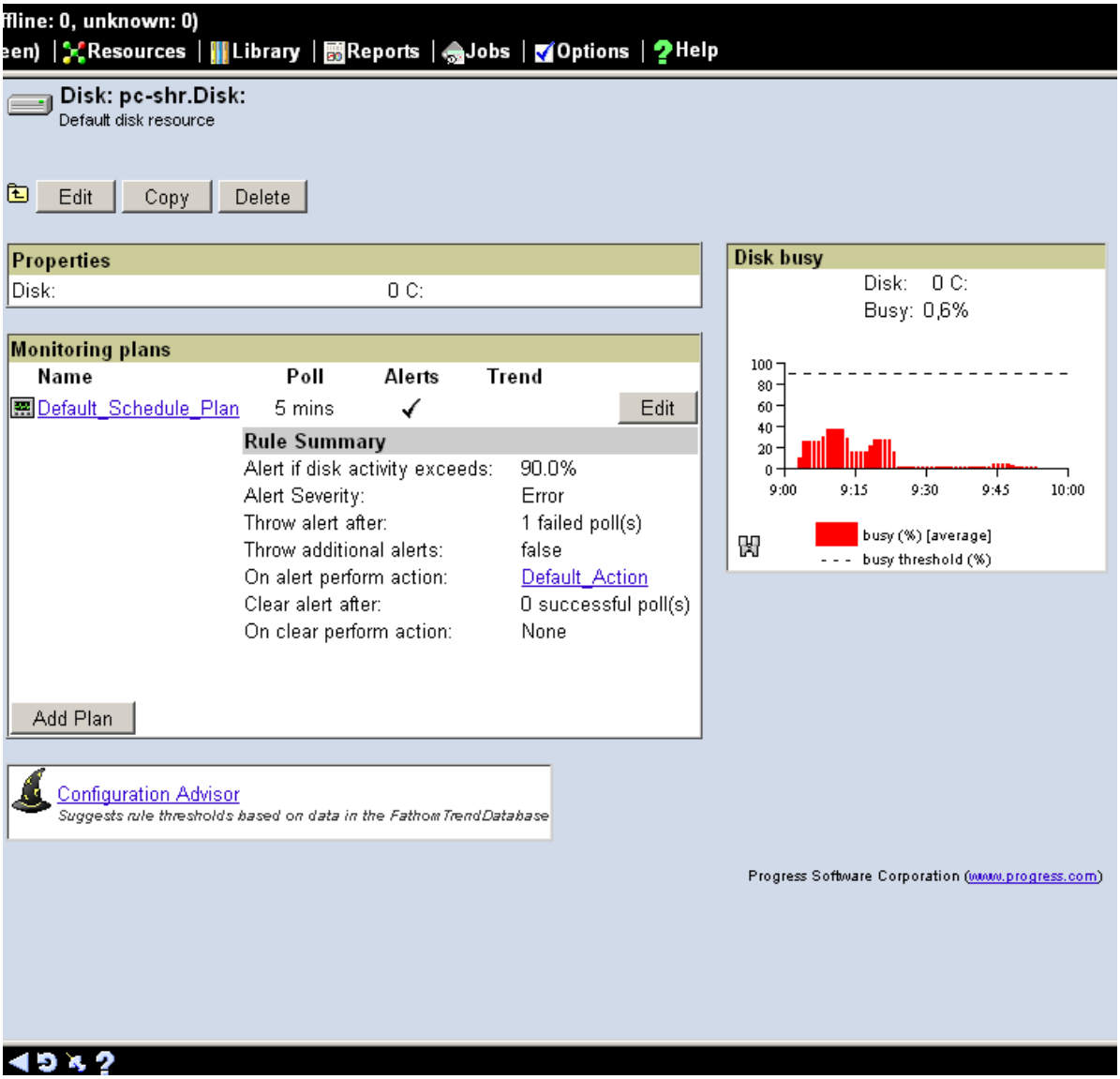
Kategorie - AppServer				
Monitor	**Pravidlo**	**Interval**	**Hlášení**	**závažnosti**
Abnormální ukončení appserveru	Výskyt klíčového slova v databázovém logu	5 minut	1	Chyba
Nedostupný nameserver	Výskyt klíčového slova v databázovém logu	5 minut	1	Chyba
Nedostupný appserver	Výskyt klíčového slova v databázovém logu	5 minut	1	Chyba

Příloha B - Úvodní obrazovka monitorovacího nástroje OpenEdge Management



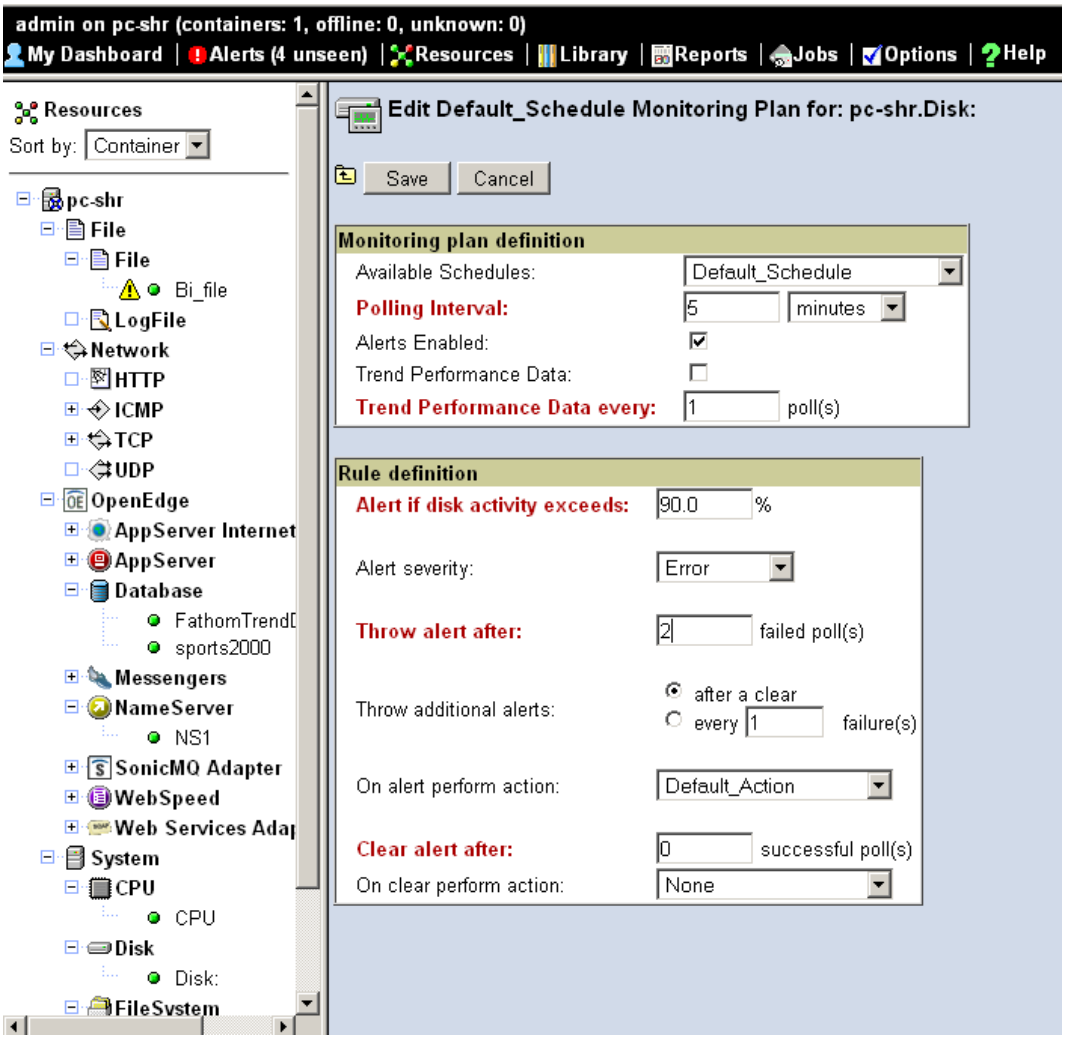
Obrázek 14: Úvodní obrazovka monitorovacího nástroje OpenEdge Management (zdroj: OEM)

Příloha C - Monitor diskové aktivity



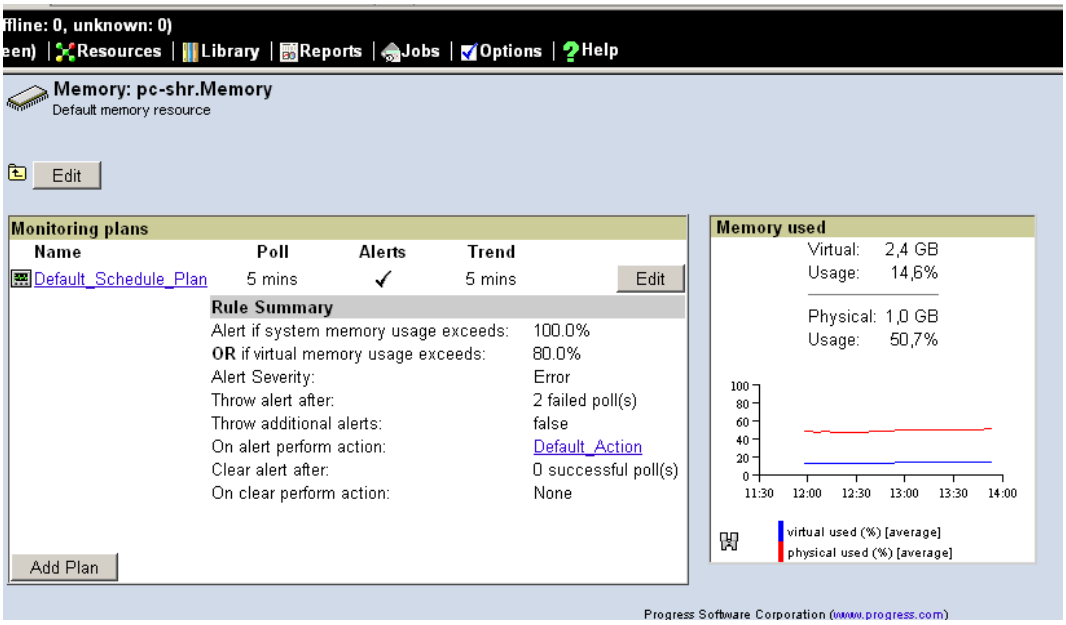
Obrázek 15: Monitor diskové aktivity (zdroj: OEM)

Příloha D - Nastavení pravidel monitoru diskové aktivity



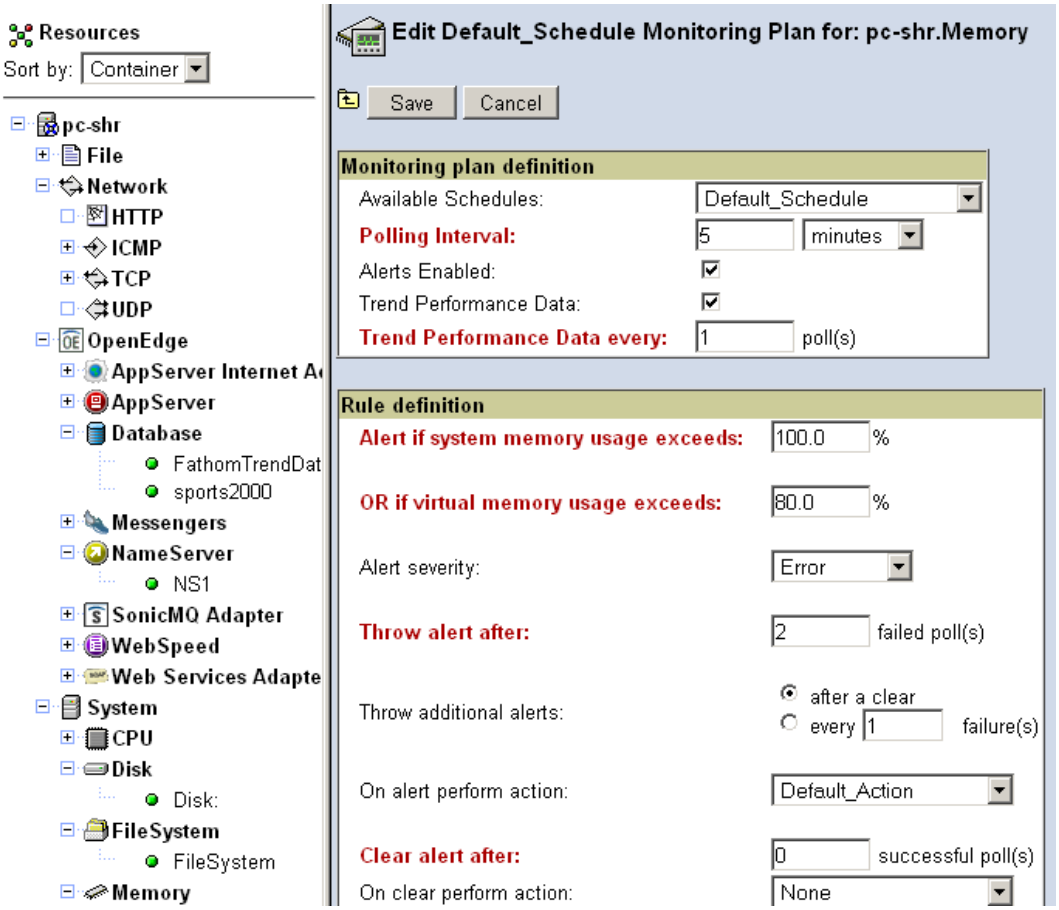
Obrázek 16: Nastavení pravidel monitoru diskové aktivity (zdroj: OEM)

Příloha E - Monitor využití virtuální a systémové paměti



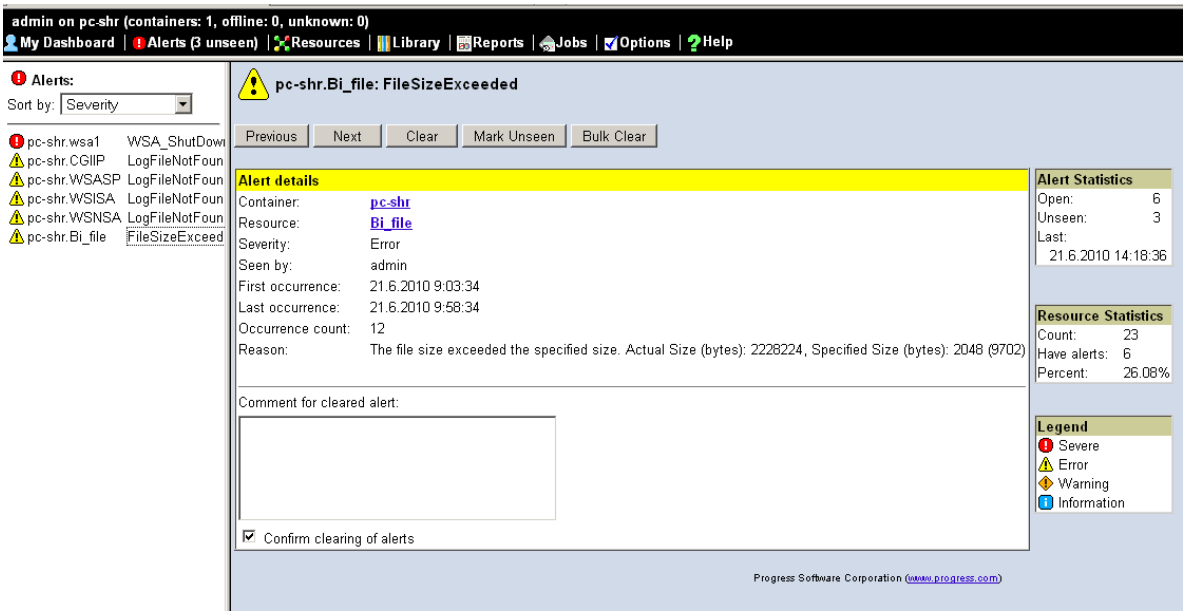
Obrázek 17: Monitor využití virtuální a systémové paměti (zdroj: OEM)

Příloha F - Nastavení pravidel monitoru využití virtuální a systémové paměti



Obrázek 18: Nastavení pravidel monitoru využití virtuální a systémové paměti (zdroj: OEM)

Příloha G - Obrazovka s přehledem nahlášených varovných zpráv



Obrázek 19: Obrazovka s přehledem nahlášených varovných zpráv (zdroj: OEM)

Příloha H - Emailové varovné hlášení monitoru CPU aktvity

OpenEdge Management Alert [7] Alert Name: CpuBusyThresholdExceeded Severity: Error Host: pc-shr Container: pc-shr Resource: CPU Occurred: 21.3.2010 21:41:03 Reason: CPU Busy Threshold Exceeded! Value: 100.0, Threshold 80.0 (9617) Occurrence Count: 2 Trigger value: 100.0 Link to OpenEdge Management: http://pc-shr:9090 Link to resource: http://pc-shr:9090/system/cpuconfig.jsp?key=localhost:resource.system.cpu.CPU Link to alert: http://pc-shr:9090/alert/alertdetail.jsp?key=7