Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Metoda monitorování IS/ICT

Disertační práce

Autor: Ing. Radek Brázda

Školitel: Doc. PhDr. Ivana Švarcová, CSc.

2010

Metoda monitorování IS/ICT

Method of IS/ICT monitoring

Poděkování

Rád bych poděkoval všem, kteří mi při této práci pomohli.

Zvláště děkuji své školitelce, Doc. PhDr. Ivaně Švarcové, CSc., za odbornou pomoc, ochotu a cenné připomínky k obsahu práce. Dále děkuji všem kolegům z katedry informačních technologií PEF ČZU za poskytnuté rady a postřehy. Dále bych na tomto místě rád poděkoval svým bývalým a současným kolegům, kteří mi předali mnoho svých zkušeností a znalostí, které pro mne byly inspirací při zpracování této disertační práce. Zvláště bych chtěl poděkovat: Ing. Petru Kramosilovi, Ing. Michalu Charvátovi, Ing. Pavlu Pokornému (všichni konzultanti společnosti NextiraOne Czech, s.r.o.) a Ing. Patriku Maninovi (obchodní manažer společnosti Rockwell Automation, s.r.o.). Mé poděkování patří také mé matce Aleně Brázdové za jazykové a stylistické korektury.

Abstrakt

Disertační práce se zabývá monitorováním služeb ICT a informačních technologií, na nichž jsou tyto provozovány. Monitorování je řešeno v rámci podpory při řízení provozu služeb ICT a infrastruktury IS/ICT v podniku na taktické a operativní úrovni. Na základě současných přístupů k řízení provozu IS/ICT je vhodné pro zavedení monitorování použít standardní a rozšiřitelnou metodu, která tyto základní činnosti a postupy popisuje. Metoda je určena informačním manažerům podniku, servisním manažerům, vlastníkům služeb a především konzultačním společnostem zabývajícími se nasazováním monitorování informačních technologií, aplikací, systémů a celých služeb na nich provozovaných. Vzhledem k široké předmětné oblasti je metoda zaměřena na monitorování služeb a jejich technologií dle následujících hledisek:

- stavu služby - stavové monitorování,
- pohled koncového uživatele - E2E monitorování,
- transakcí - transakční monitorování.

Metoda definuje proces, který popisuje nasazení monitorování z hlediska jeho základních aktivit, rozhodovacích prvků, vstupů, výstupů, nástrojů a odpovědností. Hlavní proces je členěn na dva dílčí procesy: proces stavového monitorování a proces transakčního monitorování a monitorování z pohledu koncového uživatele. Transakční monitorování a monitorování z pohledu koncového uživatele je vzhledem k podobné povaze získávaných dat popsáno v rámci jednoho dílčího procesu. Informačním základem, na němž je metoda založena, je metodický rámec ITIL, a proto jsou popsané procesy metody s metodickým rámcem v souladu. Integrace metody do metodického rámce je provedena na základě popisu vazeb mezi výstupy metody a vstupy jednotlivých procesů ITIL.

Práce je rozdělena do tří základních částí. První část práce je věnována vymezení současných oblastí, přístupů a trendů v řízení provozu IS/ICT. Pro lepší orientaci v této oblasti je součástí první části práce i popis a analýza trhu s produkty z oblasti řízení a provozu informačních technologií (ITOM). Ve druhé stěžejní části je navržena metoda monitorování služeb IS/ICT. Poslední část je věnována případové studii nasazení monitorování služeb dle definované metody. Mezi hlavní teoretický přínos práce patří definice dosud nevytvořené metody monitorování služeb IS/ICT. Jako hlavní přínosy práce pro praxi lze shledat v použití metody

při nasazování monitorování pomocí takto standardizovaných postupů, které vedou k časově a nákladově efektivnějším výsledkům nasazení a provozu monitorování. Metoda byla použita při nasazení monitorování služeb IS/ICT v prostředí významného mobilního operátora v České republice.

Klíčová slova: IS/ICT, metoda, metodický rámec, ITIL, SLA, infrastruktura ICT, služba ICT, aplikace, systém, podnik, architektura monitorování, výpadek, výkonnost, E2E, transakce

Abstract

The dissertation thesis deals with the monitoring of ICT services and related information and communication technologies. Monitoring is implemented within the ICT services and IS/ICT infrastructure operational support on the tactical and operational level of management. On the basis of current approaches to IS/ICT operations management, it is convenient to use a standard and extensible method which describes techniques and actions to be taken in order to implement and operate IS/ICT monitoring. The method is designed for enterprise information managers, service managers, services business owners and especially for the consulting companies dealing with IT, applications, system and whole IT services monitoring. With regard to a wide problematic area, the method is focused on the monitoring according to the following points of views:

- service state - state monitoring,
- end user experience - E2E monitoring,
- transactions - transactional monitoring.

The method defines a process, which is describing an implementation of monitoring in terms of its basic activities, decisions, inputs, outputs, tools and responsibilities. The main process consists of two particular processes: process of state monitoring and process of monitoring from the transactional and end user point of view. Transactional monitoring and end user monitoring is described in one detailed process, because of the similar monitoring data character. The method has been developed upon the selected methodology framework ITIL servant as an informational basis and therefore the method's processes must be compliant with this framework. The method integration into the methodology framework has been performed on the basis of the relations between method outputs and particular framework processes inputs.

The thesis is divided into three main parts. The first part of the thesis is dedicated to a specification of a problematic area, current approaches and trends in management of IS/ICT operation. This part of the work also describes and analyses the IT operation management (ITOM) software market in order to achieve a better orientation in the area. The method for IS/ICT monitoring is designed in the second main part of the work. The last part is dedicated to a case study of implementation and deployment of IS/ICT services monitoring using a defined

method. The theoretical contributions of the thesis include a definition of a method which has not been defined yet. The main contribution to a practice can be seen in using of the method when implementing and deploying monitoring by performing formal and standard procedures defined in the method. This leads to a time and cost effective implementation, deployment and future monitoring operation. The method has been used and therefore demonstrated during an implementation of IS/ICT services monitoring in the environment of the Czech mobile operator.

Key words: IS/ICT, method, methodology framework, ITIL, SLA, ICT infrastructure, ICT service, application, system, enterprise, monitoring architecture, outage, performance, E2E, transaction

Obsah

Seznam Obrázků

Seznam Tabulek

1 Úvod

Dynamický rozvoj moderních informačních a komunikačních technologií (ICT) znamená od konce 20. století až do současnosti významný posun prakticky ve všech odvětvích lidské činnosti. Tyto technologie se stávají běžnou součástí života široké skupině obyvatelstva i firemním subjektům, ze kterých je většina využívá k rozvoji svého podnikání. Hlavní přínosy těchto technologií jsou ve zcela nových prvcích komunikace, řízení, organizace prodeje výrobků a služeb, marketingu, organizace podnikových procesů apod.

Kvalitní a spolehlivá infrastruktura IS/ICT je v dnešní „síťové ekonomice“ jedním z předpokladů prosperity a konkurenceschopnosti podniků. Spolu s exponenciálním rozvojem internetu, intranetu, GSM, UMTS a dalších typů sítí dochází u většiny podniků k potřebě řízení provozu podnikových sítí a s nimi spojených prvků ICT a tyto procesy následně automatizovat za účelem dosažení vyšší efektivity. Poskytovatelé služeb založených na využívání ICT stojí před otázkou, jakým způsobem zajistit a garantovat jejich dostupnost a spolehlivost svým zákazníkům? Jiné podniky využívají ICT nikoliv přímo za účelem poskytnutí služeb koncovým klientům, avšak ICT zde vystupuje jako podpůrný prostředek při výrobě a prodeji finálních produktů či poskytování jiných typů služeb. Z výše uvedeného vyplývá, že s rostoucí složitostí a komplexností dnešních ICT tedy narůstá i potřeba jejich efektivního řízení. Řízení podnikových ICT vychází z řízení podniku jako celku. Řízení ICT lze obecně rozdělit do několika úrovní: strategické, taktické a operativní. Na těchto úrovních jsou používány různé nástroje pro zabezpečení klíčových požadavků na provoz ICT. Jedním z nástrojů používaných na taktické a operativní úrovni je monitorování IS/ICT. Někdo by mohl namítat, že monitoringu sítí a dalších částí podnikového IS/ICT není třeba přikládat velký význam, protože se jedná o technologie, které „pouze“ podporují jejich provoz, avšak opak je pravdou. Bez potřebných informací, které zpravidla vycházejí z monitorování, nemohou podniky garantovat svým zákazníkům požadovanou kvalitu poskytované služby založené na využití ICT, protože jim jednoduše není známa. Následně pak nemohou identifikovat slabá místa ve své infrastruktuře IS/ICT, které je třeba zlepšit.

Disertační práce se zabývá zásadními principy návrhu a metody zavádění technologií monitorování jako podpůrného nástroje pro efektivní řízení a správu prostředků IS/ICT na taktické a operativní úrovni.

2 Cíle

Disertační práce si klade následující cíle:

- hlavním cílem je vytvořit metodu pro zavádění monitorování aplikací, služeb, business procesů a s nimi spojených technologií z hlediska monitorování jejich stavů, transakcí, výkonnosti a pohledu koncového uživatele, a tím řešit zavedení nástrojů pro podporu řízení IS/ICT na taktické a operativní úrovni v oblastech řízení výpadků a výkonnosti,
- dílčím cílem je metodu následně aplikovat a ověřit na případové studii projektu zavedení monitorování služeb IS/ICT pro vybranou telekomunikační společnost.

3 Metodika zpracování disertační práce

Disertační práce je rozdělena do tří základních částí.

První část práce (Výchozí situace) popisuje úvod do problematiky řízení a správy IS/ICT a východiska pro tvorbu metody monitorování. Tato část disertační práce je nejprve zaměřena na dostupné a nejvíce používané technologie pro správu a řízení IS/ICT. V rámci této části je dále vymezen pojem služba ICT a popsán ekonomický význam zavádění monitoringu služeb a aplikací ICT. Nedílnou součástí první části práce je popis a analýza vybraných metodik pro řízení IS/ICT a poskytování služeb ICT. Z výčtu metodických rámců bude vybrán jeden, na jehož principech bude nově vzniklá metoda vytvořena.

Druhá část práce (Metoda monitorování IS/ICT) je věnována vytvoření metody pro zavádění monitorování IS/ICT. Ještě před definováním metody jsou nejprve popsány hlavní motivační kroky pro tvorbu metody monitorování IS/ICT, které lze shrnout následovně:

- dostupnost popř. výkonnost dílčích aplikací zpravidla sleduje příslušné IT oddělení,
- pro řadu komplexních systémů a služeb IS/ICT je potřebné mít informace o jejich stavu a výkonu neustále k dispozici,
- výstupy z monitoringu podporují rozhodování o řízení IS/ICT (jak na operativní, tak i na taktické úrovni řízení),
- na trhu existuje mnoho produktů z oblasti monitoringu, avšak téměř žádné postupy a metody, jak monitoring nasazovat, což často vede k neefektivním implementacím, které se v důsledku mohou projevit následujícími nežádoucími účinky:
    - časově a zdrojově neefektivní nasazení,
    - zahlcování monitorovacího systému nepotřebnými informacemi,
    - vysoká míra falešných alarmů,
    - nesprávně spočítané hodnoty, které jsou použity v dohodě SLA.

Metoda monitorování je tvořena v několika krocích. Nejprve je prostřednictvím analýzy dostupných informačních zdrojů vybrán metodický rámec, který je pro potřebu tvorby metody nejvhodnější. Metoda monitorování vychází z principů vybraného metodického rámce. V dalším kroku tvorby metody jsou vybrány

konkrétní oblasti metodického rámce, které metoda rozšiřuje a doplňuje. Samotný návrh architektury metody plně respektuje vybraný metodický rámec, tedy například i to, že je metoda procesně orientovaná. V rámci návrhu architektury jsou definovány základní prvky procesu (vstupy, výstupy, nástroje a techniky, uživatelské role, odpovědnosti) a vybrán nástroj pro modelování metody. Nedílnou součástí je slovní popis instancí prvků metody. V závěrečném kroku je metoda začleněna do metodického rámce prostřednictvím mapování výstupů metody na vstupy procesů metodického rámce a naopak výstupů některých procesů metodického rámce na vstupy metody.

Třetí část práce je zaměřena na aplikaci navržené metody v rámci případové studie nasazení monitorování vybraných služeb ICT, aplikací, datových toků a business procesů v prostředí mobilního operátora. V rámci studie je nejdříve popsán a zhodnocen stávající stav monitorování z hlediska jeho architektury, funkcionalit a jednotlivých komponent. Ve druhé části případové studie je navrženo řešení v podobě rozšíření stávajícího stavu o doplňující monitoring, jehož nasazení vychází z nově definované metody monitorování.

Pro zpracování disertační práce bylo použito standardních vědeckovýzkumných přístupů, deduktivních metod, metody analýzy informačních zdrojů a jejich syntézy.

4 Výchozí situace

4.1 Hlavní technologie správy IS/ICT

V současnosti je na trhu mnoho technologií, které pomáhají vykonávat správu a řízení IS/ICT. V této kapitole jsou popsány vybrané technologie, které jsou nejčastěji používány pro správu IS/ICT.

4.1.1 SNMP

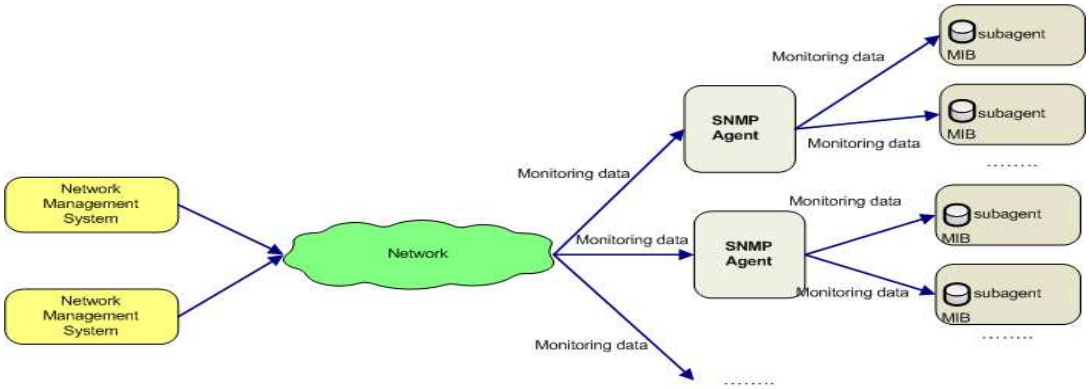
Simple Network Management Protokol (SNMP) je součástí aplikační vrstvy soustavy protokolů TCP/IP a slouží potřebám správy sítí. SNMP vystavuje informace o systému či jeho části, kterou může být prakticky jakýkoliv síťový či jiný prvek IS/ICT podporující komunikaci přes SNMP (router, server, ale např. i UPS), ve formě proměnných (např. volná paměť, počet běžících procesů, uptime apod.), které obsahují data o jeho konfiguraci a stavu. Prostřednictvím SNMP jsou posbírané monitorovací informace přenášeny sítí do centrálního úložiště monitorovacího systému, kde jsou následně zpracovány a prezentovány.

Při typickém použití SNMP je definováno více systémů, které jsou spravovány a monitorovány jedním nebo více monitorujícími systémy. Na koncových zařízeních tedy běží softwarová komponenta označovaná zpravidla jako agent, která má za úkol poskytovat informace o stavu zařízení přes SNMP do monitorovacích systémů (manažerům). Monitorovací systém může tyto informace získat aktivním způsobem sám, a tak se pomocí definovaných operací agenta doptat na požadované informace nebo agent odešle informace sám bez potřeby doptání. SNMP je tedy založen na architektuře klient-server. Server je označován jako agent a klient jako manažer.

4.1.1.1 Architektura SNMP

Architektura SNMP se skládá ze tří základních komponent spravovaných zařízení, agentů a manažerů. Agent je software, který poskytuje rozhraní ke spravovaným prvkům, kterými mohou být například routery, HUBy, servery, brány atd. Tyto prvky následně obsahují objekty monitorování, kterými mohou být například hardware, konfigurační parametry, statistiky výkonnosti apod. Tyto objekty jsou organizovány a uloženy ve virtuální bázi informací známé jako

Management Information Base (*4.1.1.3*). Manažer představuje stanici s běžícím management softwarem, který skrze toto rozhraní získává požadované informace, které jsou následně zpracovávány a prezentovány.



Obr. 4-1 - Architektura SNMP

Jeden agent může obsahovat více subagentů, kteří obsahují různé MIB v závislosti na tom, které objekty monitorují.

Typické funkce agenta: [9]

- implementuje SNMP protokol,
- ukládá a získává data z MIB (operacemi get, getNext, getBulk),
- může asynchronně zaslat událost manažerovi,
- může sloužit jako proxy agent pro zařízení, které nepodporují SNMP.

Typické funkce manažera:

- implementuje SNMP protokol,
- poskytuje funkce network management station,
- může se doptat agenta na data, získat odpovědi od agenta, nastavovat proměnné agenta, potvrdit zaslanou asynchronní událost z agenta.

4.1.1.2 Výhody a nevýhody používání SNMP

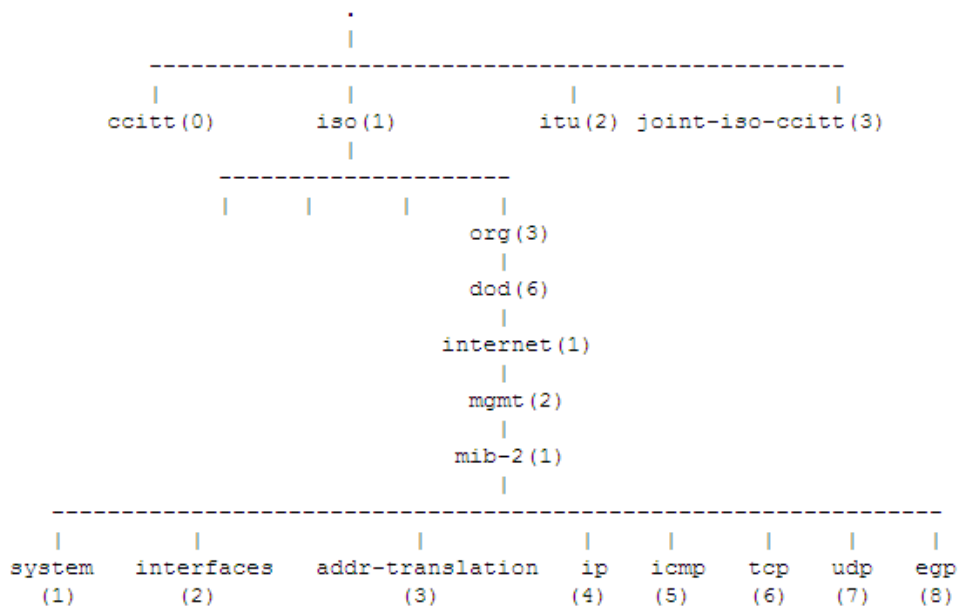
Mezi hlavní výhodu SNMP patří, že je velmi jednoduchý a snadno implementovatelný. Jednoduchý návrh umožňuje uživatelům snadno a rychle přidávat a modifikovat proměnné, které chtějí monitorovat. Další nespornou výhodou je jeho rozšiřitelnost v případě budoucích potřeb. SNMP je nyní standardem pro správu sítí, a proto jej výrobci síťových prvků hojně implementují do svých zařízení.

Největší nevýhodou SNMP byla od počátku vždy jeho bezpečnost. Bezpečnostní problémy jsou řešeny postupně v SNMP verzi 2 a 3. Ve verzi 2 na úrovni autentizace a řízení přístupů k agentům. Ve verzi 3 jsou data přenášena

po tomto protokolu šifrována tak, aby nemohla být zneužita nežádoucími osobami či systémy.

4.1.1.3 Management Information Base

Management Information Base (MIB) je datová struktura, která je využívána agenty k uložení informací o monitorovaném zařízení. Jedná se o standard definující jaká data agent uchovává a jaké operace jsou nad těmito daty povoleny. Struktura MIB má podobu stromu a data jsou uložena v jeho listech. Všechny uzly ve stromu mají své označení, a to jak slovní tak číselné. Na každý uzel ve stromu je možné se odkázat pomocí cesty od kořenu, kterou je pozice uzlu ve stromu vždy jednoznačně určena, neboť označení (slovní i číselné) každého uzlu je v rámci jeho bratrů unikátní.



Obr. 4-2 - Část stromu MIB

4.1.2 Syslog

Syslog se od svého vzniku a rychlým vývojem stal dnes standardem pro logování a zasílání zpráv z logu koncových zařízení po IP sítích. Syslog je v současné době technologií hojně využívanou ke správě infrastruktury IS/ICT. Protokol syslog je typu klient/server, kde klient vystupuje v roli odesílače textových zpráv obsahující systémové informace provozního charakteru kratších než 1KB a server v roli přijímače, často nazýván jako syslog démon. Standardizovaná syslog zpráva obsahuje:

- typ zařízení, které vygenerovalo zprávu (operační systém, aplikace, služba apod.),
- úroveň severity zprávy[1],
- datum a čas, kdy byla zpráva odeslána,
- jméno uzlu nebo adresa IP síťového zařízení nebo serveru, který odeslal zprávu,
- text zprávy obsahující popis události.

Operační systémy, aplikace a služby pak zasílají tento typ zpráv na centralizované syslogové servery, kde jsou tyto zprávy následně zpracovávány. V závislosti na možnostech konkrétních syslog serverů mohou být zprávy tříděny, potlačovány, přesměrovány na základě zdroje zpráv, jejich obsahu, severity atd. K integraci se systémy pro event management jsou pak zpravidla použity speciální programy často nazývané syslogové sondy, které umějí přijímat zprávy ze syslogových serverů a tyto dále zpracovat a doručovat dle souboru pravidel do centrálního dohledového systému.

4.1.3 Správa založená na webovém rozhraní

S velkým rozvojem webu a přidružených technologií jsou tyto stále více integrovány do systémů pro správu sítí a prvků IS/ICT. Různé přístupy v rámci webového pojetí řízení podporují různé architektury modelů, ze kterých vychází *4.2.7.1 Kategorizace dle architektury*. Následující podkapitoly popisují základní vybrané přístupy:

- HTTP - správa založená na HTTP implementuje centralizovaný model správy,
- JRMI - správa založená na vzdáleném volání metod na objektech implementuje silně distribuovaný hierarchický model,
- WBEM - Web Based Enterprise Management - implementuje slabě distribuovaný hierarchický model.

[1] Syslog zpráva může mít až 8 úrovní severity od nejméně závažné (8 - debug - ladící) po nejzávažnější (0 - Emergency - systém mimo provoz).

4.1.3.1 Správa založená na HTTP

Tento typ správy používá narozdíl od protokolu SNMP k přenosu monitorovacích informací od agentů k manažerům protokol HTTP. V rámci tohoto přístupu mají agenti v sobě zapouzdřený HTTP server a na stanici manažera běží webový prohlížeč. Informace pro správu jsou předávány v podobě HTML stránek od agenta směrem k manažeru. Jiným způsobem přenosu může být běh Java appletu ve webovém prohlížeči popř. Java aplikace na stanici manažeru a využití HTTP protokolu ke komunikaci mezi agentem a manažerem. Data mohou být doptána manažerem nebo zaslána agentem.

4.1.3.2 Správa založená na Java RMI

Java RMI podporuje volání Java metod na vzdálených objektech a tím umožňuje vytvářet distribuované objektově orientované aplikace správy IS/ICT. Společně s vývojem JMAPI (Java Management API), které představuje soustavu nástrojů a metod k vytváření appletů správy podporující Java RMI, tak je možné mapovat spravované objekty v SNMP, MIB a MIB II na objekty Java. JMAPI je na konci 90. let nahrazeno JMX (Java Management eXtensions), které slouží jako framework pro objektově orientovanou správu založenou na webových technologiích. Správa založená na Javě umožňuje nyní velmi efektivně vytvářet výkonné silně distribuované aplikace pro správu a řízení IS/ICT. Podmínkou však je, že všichni agenti a manažeři musí podporovat Javu.

4.1.3.3 Správa založená na WBEM

Web-Based Management Enterprise System reprezentuje sadu technologií pro správu IS/ICT, které sjednocují správu distribuovaných výpočetních prostředí [11]. Cílem konsorcia vedeným společností Microsoft bylo integrovat správu všech typů sítí a systémových zařízení, jakými jsou např. servery, stanice, routery, přepínače, tiskárny atd. Vývoj přístupu přešel pod záštitu organizace DMTF (Desktop Management Task Force) a v rámci jeho dalšího rozvoje došlo k definování nového objektově orientovaného informačního modelu (CIM).
Mezi hlavní charakteristiky správy založené na WBEM patří: [11]

- vzdálená správa aplikací,
- správa více instancí jedné aplikace jako samostatné jednotky,
- standardizované rozhraní pro vzdálenou správu různých aplikací,

- odpojení klienta od správy aplikací,
- publikace klíčových informací jiným aplikacím o spravované aplikaci.

4.1.4 Inteligentní agenti

Z hlediska kategorizace produktů dle podporovaných architektur modelů popsaných v *4.2.7.1 Kategorizace dle architektury* patří inteligentní agenti do silně distribuovaného kooperativního modelu. Agenti pro správu sítě představují typ software, který vykonává aktivity správy nad sledovanými objekty a reportuje výsledky manažerům. Inteligencí se zde rozumí řada charakteristik, které samy o sobě nedeterminují agenty jako inteligentní, avšak pokud fungují společně, mohou prezentovat relativně inteligentní chování [10]:

- nezávislost - agenti nevyžadují instrukce, vědí, co mají učinit v jakých situacích,
- spolupráce - agenti spolupracují s ostatními agenty za účelem dosažení jejich cílů,
- komunikace - schopnost výměny informací s ostatními agenty,
- delegování - jeden agent může požádat jiného agenta o službu v podobě vykonání některých akcí,
- důmyslnost - schopnost agenta jednat na základě jeho znalostí,
- učení - agenti získávají a používají nové znalosti,
- pohyblivost - agent se může přemístit ze systému na jiný a pokračovat ve svých aktivitách správy,
- plánování - agent umí organizovat své aktivity na základě priorit a časového hlediska,
- proaktivita - agenti rozumějí příčině obdržené informace a umějí předpokládat, co nastane,
- reaktivita - agenti odpovídají na události obdržené ze spravované infrastruktuře.

Koordinací agentů v rámci celého systému správy lze docílit chování, které se jeví jako inteligentní. Na základě výše uvedených charakteristik lze inteligentní agenty rozdělit na:

- důmyslné - založeni na znalostech spravovaného prostředí a logickém programování,

- reaktivní - založeni na sadě předdefinovaných akcí, které je třeba učinit v případě obdržení události,
- hybridní - složeni z obou výše uvedených vrstev: důmyslné a reaktivní.

4.2 Hlavní oblasti řízení provozu ICT

4.2.1 Vymezení problémové oblasti

V dnešním světě se hlavní činnosti podniku definované podnikovými business procesy prakticky neobejdou bez využívání podpůrných IS/ICT. Tento trend má za následek stále více těsnější závislost businessu na ICT, a proto je důležité zabezpečit řízení a správu těchto technologií, kde monitoring slouží jako jeden z nástrojů. Nově vznikající metoda se zabývá monitoringem základních oblastí IS/ICT podniku. Mezi tyto oblasti patří technologická infrastruktura, procesy ICT, služby ICT a business procesy na nich provozované.

Definice služby ICT dle [ITIL 2007] je následující: „*Služba poskytovaná jednomu nebo více zákazníkům poskytovatelem služby ICT. Služba ICT je založena na využívání IT a podporuje zákazníkovy business procesy. Služba ICT je pak tvořena prostřednictvím lidí, procesů a technologií. Služba ICT je definována v rámci dohody o poskytování služby (SLA).*“ Výše uvedená definice není jediná, protože více autorů ve svých pracích píše o službách informatiky, informatických službách, službách ICT nebo službách IS/ICT. Výše uvedené pojmy definují často odlišnými způsoby. Autoři Jelínek, Šild a Voříšek ve svém článku [28] sjednocují definici služby ICT na základě jejího vztahu k modelu řízení informatiky SPSPR následovně: „*ICT služba jsou koherentní aktivity a/nebo informace dodávané poskytovatelem ICT služby příjemci služby. ICT služba je vytvářena ICT procesy, které při svém průběhu konzumují ICT zdroje (hardware, software, data, lidé atd.). Služba se realizuje na základě dohodnutých obchodních a technických podmínek.*“ Pro účely disertační práce bude použita tato definice [28] pro všechny výše uváděné pojmy. Pro zjednodušení se v dalším textu disertační práce může vyskytovat pouze pojem „služba“, kterým bude chápána služba ICT, pokud nebude označena jiným způsobem např. „neinformatická služba“.

V současnosti existuje celá řada modelů řízení IS/ICT. V návaznosti na vymezení pojmů bylo v definici služby dle [28] odkázáno na model SPSPR. Model SPSPR pohlíží na řízení IS/ICT v pěti vzájemně provázaných vrstvách [47]:

- S - Strategie - vrcholové vedení podniku stanoví hlavní cíle (týkající se prodeje výrobků a služeb, provozu, zdrojů apod.) a prostředky, kterými jich chce podnik dosáhnout,
- P - Procesy podniku - primární business procesy podniku jsou soustavy strukturovaných aktivit, které jsou definovány procesními manažery tak, aby produkovaly požadované výrobky či služby v optimálním čase a nákladech,
- S - Služby ICT - služby založené na ICT, které podporují hlavní business procesy podniku. Služby ICT mohou být provozovány buď interně tj. vlastními prostředky podniku, externě (outsourcing) nebo kombinací obou způsobů,
- P - Procesy ICT - procesy ICT produkují služby ICT. Příkladem procesů ICT jsou procesy metodického rámce ITIL, kterými může být řízen provoz služeb ICT,
- R - Resources ICT - zdroje spotřebovávány procesy ICT, které produkují a zabezpečují služby ICT. Mezi ICT zdroje patří technologická infrastruktura (HW, O.S., síť a její prvky atd.), aplikace, databáze, IT personál, režijní zdroje (prostory, elektřina atd.).

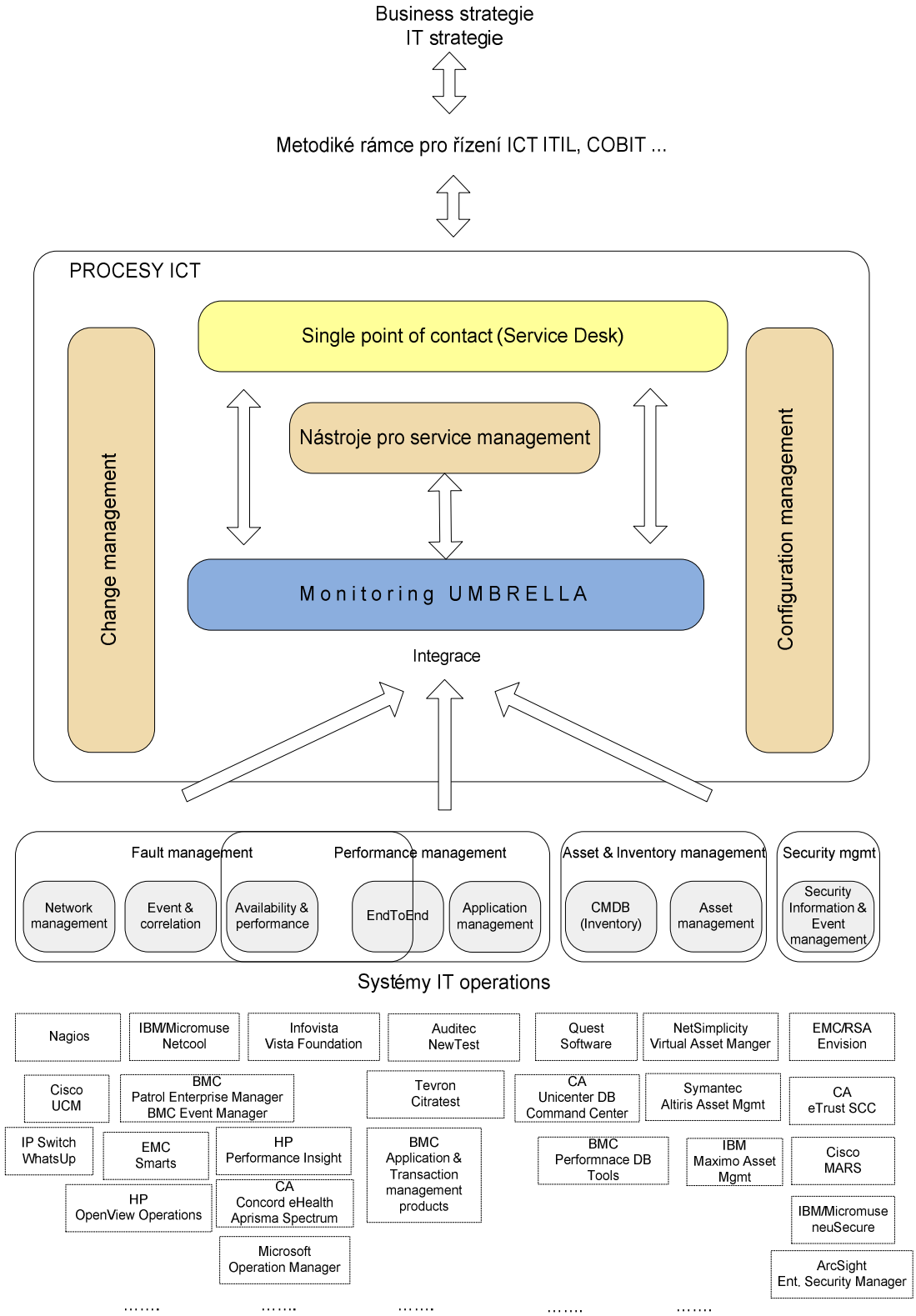
Výše uvedené rozdělení řízení podnikových IS/ICT do pěti úrovní umožňuje formulovat vazby mezi požadavky primárních business procesů a podnikových IS/ICT. Toto členění dále pomáhá definovat odpovědnosti vedoucích pracovníků na jednotlivých úrovních řízení a metriky efektivnosti jednotlivých procesů. Oblast metody monitorování lze najít postupně na následujících vrstvách modelu SPSPR postupně od nejnižší úrovně:

- R - na nejnižší úrovni zdrojů ICT je metoda zaměřena na nasazení monitorování technologických zdrojů ICT, mezi které patří HW, O.S., aplikace, databáze, síťová infrastruktura apod. Monitoring lidských ICT zdrojů pro dosažení správného fungování ICT procesů je možný aplikovat za předpokladu, že existují datové záznamy o aktivitách těchto zdrojů,
- P - metoda umožňuje nasazení monitorování procesů ICT za předpokladu, že existují data vypovídající o průběhu procesu. Příkladem výstupu takového monitoringu může být počet vyřešených incidentů a průměrná délka řešení incidentu v rámci procesu Incident Managementu nebo poměr počtu zavěšených hovorů na Service Desku vůči obslouženým apod. Monitorování poskytuje výstupy pro procesy ICT,

- S - metoda popisuje nasazení monitorování služeb ICT, které jsou provozovány za účelem podpory primárních business procesů. Mezi služby ICT, které lze implicitně monitorovat metodou, patří: služby informační, aplikační a infrastrukturní - rozdělení dle předmětu služby na základě kategorizace v [28]. Služby vývojové, podpůrné lze monitorovat za předpokladu, že mají svůj datový obraz použitelný pro monitoring,
- P - metoda popisuje nasazení monitorování primárních business procesů, které lze na základě jejich charakteru monitorovat prostřednictvím dostupných technologií. Nutnou podmínkou monitoringu business procesu je možnost definice měřících bodů a existence datových struktur, ze kterých lze informace o průběhu business procesu získat. Příkladem může být business proces vyřízení objednávky. Bude-li existovat datový zdroj, ze kterého lze získat informace o stavech a atributech objednávky, bude možné nasadit monitoring jejího průběhu,
- S - Strategie - metoda není primárně zaměřena na nasazení monitorování strategického řízení, avšak výstupy monitorování mohou sloužit jako vstupy pro strategické rozhodování.

Výše uvedené znamená, že monitoring je možné nasadit a uplatnit vertikálně skrze jednotlivé vrstvy modelu. K vymezení oblasti monitoringu je záměrně přistoupeno v obráceném pořadí, protože i k nasazování monitorování je třeba provést od nejnižší vrstvy tj. od zdrojů ICT a teprve rozšířit na vyšší úrovně modelu. Metodu monitorování lze obecně použít v takové oblasti řízení, která má nějaký datový základ, tzn. že i monitoring netechnologických částí business procesů lze nasadit za předpokladu, že bude existovat datový zdroj, odkud lze tyto business informace získat.

Na základě studia předmětné oblasti je na Obr. 4-3 autorem práce definováno schéma řízení IS/ICT z pohledu jejich provozu, technologií a procesů, které tento provoz pomáhají zabezpečit.



Obr. 4-3 - Hlavní oblasti řízení provozu IS/ICT

Obr. 4-3 představuje výchozí situaci v hlavních oblastech správy a řízení provozu IS/ICT včetně ukázek společností a jejich produktů, které poskytují pro vybrané oblasti softwarové zabezpečení. Graficky znázorněná kategorizace produktů z oblasti ITSM je pouze orientační, protože ve skutečnosti některé produkty splňují charakteristiky pro zařazení do více oblastí, popř. hranice mezi oblastmi nejsou striktně vymezeny. Jednotlivé oblasti správy a řízení IS/ICT z hlediska operativního a taktického lze integrovat do tzv. „umbrelly“ a uchovávat tak důležité provozní informace na jednom místě. Takováto integrace má následující výhody:

- pomáhá snižovat náklady na provoz operátorských center,
- umožňuje vybudovat strom služeb (service-tree) a tím přejít od sledování stavu části infrastruktury IS/ICT ke sledování služeb ICT na nich provozovaných,
- usnadňuje měření hodnot dostupnosti služeb pro účely definice SLA.

Informace z platformy jsou následně použity v service-desku, jednotném místě kontaktu zákazníků a uživatelů služeb s jejich podporou. Veškeré procesní a softwarové zabezpečení je pak v souladu s podnikovou strategií, ze které pak vyplývají i použité přístupy k řízení informatických služeb (ITIL, COBIT apod.). Metoda monitorování se zabývá dvěma stěžejními oblastmi nezbytnými pro řízení provozu podnikových IS/ICT, kterými jsou řízení výpadků a řízení výkonnosti.

4.2.2 Řízení výpadků (Fault management)

V dnešním podnikovém prostředí stále více vzniká potřeba řešení výpadků počítačových a telekomunikačních sítí a elementů rozsáhlých infrastruktur IS/ICT. V dnešních komplexní sítích, systémech, aplikacích a celých službách vzniká velké množství událostí, a proto se jejich správa a provoz stává náročnějším úkolem, který je bezpochyby potřeba automatizovat. Postupně se tedy odstupuje od manuálního řešení vzniklých problémů, a tak se stává automatizace procesu řízení a správy informačních technologií nezbytnou. Fault management je jednou z disciplín v rámci řízení IS/ICT představující rozsáhlou skupinu automatizovaných funkcí, které mají za úkol odhalit, izolovat a opravit výpadky či defekty v sítích a všech ostatních prvcích, jakými jsou např. routery, servery, systémy, aplikace apod. Jedním z nástrojů podporující fault management je stavový monitoring.

4.2.3 Řízení výkonnosti (Performance management)

Performance management představuje soustavu nástrojů a procesů monitorující výkonnost sítě a jejích prvků, aplikací, systémů, serverů a následně i služeb na nich provozovaných. Hlavními nástroji podporující řízení výkonnosti jsou monitorování výkonnosti, E2E monitorování a transakční monitorování. Hlavním rozdílem mezi monitorováním výkonnosti a stavovým monitorováním lze nalézt primárně ve způsobu získávání monitorovacích dat a následně i v jejich prezentaci. Zatímco v případě stavového monitorování jsou generovány a následně zpracovány události, které představují výpadky jednotlivých částí infrastruktury IS/ICT, které jsou následně prezentovány ve formě alarmů v rámci dohledového systému, při monitorování výkonnosti jsou monitorovací data sbírána v pravidelných intervalech, ukládána do performance management databáze a následně vyhodnocována. Nástroje performance management tak poskytují svým uživatelům spojitý pohled na získaná data a tím i spojitý pohled na výkonnost technologií, sítí, aplikací a služeb. Díky těmto datům jsou podniky schopné určit výkonnost v rámci dlouhých časových intervalů např. za období jednoho čtvrtletí, pololetí či roku.

4.2.4 Řízení bezpečnosti (Security management)

V každém podniku hrají klíčovou roli pro obchodní rozhodování jeho informační aktiva. Informační aktiva jsou jakékoliv části informace, které jsou uloženy způsobem, který je využitelný a hodnotný pro organizaci. Informační aktiva je vhodné v podniku klasifikovat za účelem udržování jejich přiměřené ochrany. Příkladem klasifikace informací je následující výčet:

- veřejné - určeny pro veřejné použití, k nahlédnutí komukoliv v rámci podniku i mimo něj (např. tiskové zprávy, marketingové informace apod.),
- interní - určeny pouze pro zaměstnance podniku a nikoliv pro veřejné použití (organizační směrnice, šablony dokumentů, telefonní seznam apod.),
- citlivé - sděleny pouze na zvláštní povolení, poskytnutí tohoto typu informací třetím osobám může vážně poškodit podnik či jeho obchodní partnery (nabídky, projektová dokumentace, obchodní smlouvy apod.),
- mimořádně citlivé - sdělení tohoto typu informací nežádoucím osobám může ohrozit významnou část společnosti (platové výměry, hesla do IS, strategické plány organizace apod.).

Security management z hlediska informačních technologií popisuje aktivity nezbytné k ochraně informačních aktiv podniku proti riziku jejich ztráty, poškození nebo neoprávněnému zneužití. Rizika ohrožující informační aktiva podniku, ať už z hlediska důvěrnosti, integrity nebo jejich včasné dostupnosti, pak přímo ohrožují obchodní výkonnost podniku jako celku. Rizika lze stanovit analýzou následujících oblastí:

- potencionální ohrožení podnikových aktiv - události, které mohou zapříčinit náhodnou či úmyslnou ztrátu, poškození či zneužití informačních aktiv,
- zranitelnost a napadnutelnost - identifikace míry napadnutelnosti podnikových aktiv útoky zvenčí či zevnitř organizace,
- potencionální dopad - identifikace závažnosti dopadu (finanční dopad, ztráta důvěryhodnosti apod.) při ztrátě, poškození či zneužití informačních aktiv na podnik.

V oblasti bezpečnosti informací je velmi důležitá norma ISO 27001 z roku 2005, kterou se mohou nechat organizace certifikovat. Jedná se o mezinárodní standard definující požadavky na systém managementu bezpečnosti informací [14]. Systém managementu bezpečnosti informací představuje systematický přístup k řízení bezpečnosti důvěrných informací zahrnující zaměstnance, procesy, informační technologie a strategii podniku.

Systém informační bezpečnosti podniku má za úkol navrhnout, implementovat a spravovat procesy a systémy efektivního řízení přístupu k informačním aktivům a zajištění jejich důvěrnosti, integrity a včasné dostupnosti. Jedním z nástrojů podporující mimo jiné výše uvedené je bezpečnostní monitorování. Obecně lze rozdělit bezpečnostní systémy na systémy prevence nebo eliminace bezpečnostních hrozeb a systémy monitorování bezpečnostních hrozeb tak, jak uvádí ve svém článku Kramosil [30]. Systémy prevence a eliminace bezpečnostních hrozeb jsou nástroje určené k přímému zabránění napadení vlastního informačního systému. Mezi takové systémy patří hraniční systémy síťové infrastruktury, jako jsou např. zařízení firewall, autorizační a autentifikační systémy, systémy antivirové a antispyware ochrany atd. Systémy monitoringu bezpečnostních hrozeb monitorují informační systémy a infrastrukturu IS/ICT a v případě výskytu bezpečnostního incidentu prezentují incident v reálném čase, archivují incidenty pro pozdější analýzy a notifikují o výskytech závažných incidentů. Monitorovací systémy pouze sledují a prezentují vzniklá nebo potenciální nebezpečí. Jejich součástí není funkcionalita

umožňující zabránit vlastním bezpečnostním rizikům. Oba systémy mohou být vzájemně provázány. Monitorovací systém přijímá informace o bezpečnostních hrozbách nejenom z vlastních napadených zařízení a aplikací, nýbrž také z bezpečnostních systémů. Na druhé straně může být monitorovací systém nakonfigurován tak, aby v případě výskytu bezpečnostního incidentu požádal bezpečnostní systém o vykonání určité předdefinované nápravné akce, například zakázání komunikace na firewallu apod.

4.2.5 Řízení a správa majetku (Asset Inventory Management)

Asset Inventory Management představuje soustavu systematických procesů řešících potřeby přesné, včasné a aktuální evidence veškerých aktiv podniku. Tyto procesy zabezpečené informačními technologiemi a systémy jsou klíčové pro efektivní plánování kapacit a upřednostňování oblastí kritických potřeb podniku prostřednictvím identifikace nevyužitých aktiv. Systémy pro správu aktiv umožňují zaznamenávat změny v jejich evidenci. Taková správa majetku sledující jeho životní cyklus od pořízení, přes změny až do vyřazení zvyšuje návrat do jeho investice (např. redukováním nákladu na pořízení nepotřebného vybavení apod.). Využití systémů na správu majetku spolu přináší další výhody z používání technologií, jakými jsou např. čárové kódy, sledování mobilních aktiv prostřednictvím check-in/check-out systému atd. Systémy správy majetku mají často vazbu na podnikové účetnictví a ERP systémy, a tak je možné sledovat pořizovací náklady, data pořízení, nákladové účty, odpisy atd.

4.2.6 Řízení sítí a prvků IS/ICT

Současným trendem je nasazování integrovaných řešení pokrývající veškeré potřeby managementu sítí, serverů, klientských stanic, síťových prvků a podnikových aplikací. Tato řešení umožňují proaktivně sledovat a monitorovat systém jako celek, včas detekovat aktuální nebo vznikající problémy a následně na ně reagovat.

Společnými rysy těchto řešení jsou [28]:

- SNMP síťová konzole pro monitorování síťových zařízení,
- síťový a systémový agent pro monitorování aplikací,
- sondy fungující jako pasivní kolektory síťových událostí,
- nástroje pro konfigurování a monitorování síťových klientů,

- management a administrativní nástroje pro správu lokálních a vzdálených serverů,
- nástroje pro inventarizaci zdrojů a reportování.

4.2.7 Kategorizace produktů z oblasti monitorování

Na současném lokálním i světovém trhu existuje mnoho různorodých řešení využívaných k řízení, provozu a monitoringu IS/ICT, proto je můžeme rozdělit dle vybraných charakteristik za účelem lepšího pochopení těchto technologií. Existuje mnoho kategorizací těchto systémů, a proto je někdy velmi složité provést jasné rozlišení mezi některými typy systémů, což je způsobeno nejednoznačností a nejednotností charakteristik. Některé monitorovací systémy mohou spadat do více kategorií, protože splňují některé jejich charakteristiky. Na druhé straně jiné řešení splňuje pouze část charakteristik pro zařazení do určité skupiny, zbylé však nikoliv. V následujícím textu budou monitorovací řešení rozdělena na základě několika různých úhlů pohledu tak, aby byly vystiženy podstatné aspekty těchto produktů.

4.2.7.1 Kategorizace dle architektury modelu monitorování

Management systémy a modely lze rozdělit podle míry distribuce, rozvržení jednotlivých řídících komponent a míry flexibility přiřazení řízených objektů k jednotlivým řídícím komponentám. Tato flexibilita je určena stupněm decentralizace řídících komponent. Komponenty sběru dat, vyhodnocení dat, řídící a monitorovací funkce systému mohou být distribuované. Na základě tohoto organizačního pojetí lze rozlišit základní dva typy architektur management systémů *centralizovaný a distribuovaný*: [7]

- centralizovaný model koncentruje zpracování a řízení do jednoho uzlu zvaného manažer, který využívá agenty k získání monitorovacích dat. Agenti zde vystupují pouze v roli poskytovatele dat a neimplementují žádnou vnitřní logiku. Tato implementace je relativně jednoduchá, avšak skýtá určité nedostatky. Slabým místem je například chápáno to, že stanice manažeru v této architektuře vytváří „single point of failure“. V případě výpadku části infrastruktury, která je odpojena od manažeru, zůstává tato bez dohledu,
- silně distribuovaný řídící systém je charakteristický tím, že řídící úlohy již nenáleží pouze manažerům, avšak oba dva typy komponent jsou zapojeny jak manažeři tak plně i agenti. Mezi další charakteristiky patří ztráta robustnosti,

kdy definice úkolů agenta zůstávají statické bez možnosti flexibilně je měnit. Manažeři mohou delegovat úkoly vertikálním (na agenty na nižší úroveň) nebo horizontálním (mezi sebou na stejné úrovni) způsobem,

- v distribuovaném typu architektury jsou jednotlivé komponenty rozmístěny na více uzlů. Podle role agentů lze rozlišit další dvě kategorie architektury management systémů: slabě a silně distribuované,
- slabě distribuovaný model řeší nedostatek centralizovaného modelu jeho škálovatelností. Řízení a zpracování v této architektuře je koncentrováno do několika málo uzlů. Typicky je síť rozdělena na různě řízené domény s jedním manažerem na doménu a mnoha agenty poskytující monitorovací data bez další implementované logiky, rozhodování či kooperace nebo je naopak implementován jeden manažer a několik málo agentů, kteří jsou „chytřejší“ než ostatní a implementují monitorovací logiku,
- silně distribuované technologie lze rozdělit na tři skupiny: mobilní kódy, distribuované objekty a inteligentní agenty. První dvě implementují vertikální delegaci a představují tzv. silně distribuovaný hierarchický model. Distribuované objekty implementují horizontální delegaci a komunikaci mezi manažery, tím představují silně distribuovaný kooperativní model. Kooperativní typ architektury je zaměřen na cíl, kde inteligentní agenti dostávají od manažera pouze seznam úkolů a agent odvodí, jakým způsobem je vykonat.

Na základě odvozených architektur lze kategorizovat jejich typy následovně:

- centralizovaný model,
- slabě distribuovaný hierarchický model,
- silně distribuovaný hierarchický model,
- silně distribuovaný kooperativní model.

4.2.7.2 Kategorizace dle povahy získaných dat

Management systémy lze dále kategorizovat na základě charakteru dat, která jsou prostřednictvím systému získána, zpracována, analyzována a následně prezentována.

IT event correlation & analysis systems (systémy zpracování, analýzy a korelace událostí) - jedná se o takový druh produktů, jejichž hlavním cílem je zpracování nespojitých dat, jejich analýza, korelace a následná prezentace. Monitorovací data

získávaná prostřednictvím tohoto typu software mají informativní charakter o výpadcích a defektech v infrastruktuře. Vzniku alarmu zpravidla předchází nějaká událost např. výpadek napájení routeru, výpadek spojení routeru, výpadek serveru, zaplnění diskového svazku, pád kritického aplikačního procesu nebo databáze atd. Alarmy informující o těchto událostech jsou následně generovány jednotlivými prvky IS/ICT (routery, přepínače, servery, ale například i dohledovým systémem třetí strany pro určitou technologii atd.) a prostřednictvím různých cest (SNMP, syslog, propriteární protokoly atd.) doručovány do centrálního dohledového systému, kde jsou následně analyzovány, korelovány a prezentovány. Jednotlivé produkty se liší úrovní a možnostmi korelace a zpracování těchto událostí.

Mezi významné produkty této kategorie patří například platforma Netcool původně produkt společnosti Micromuse, která byla v roce 2006 akvizována společností IBM, dále HP OpenView Operations od společnosti HewletPackard, ConcordHealth, Unicenter NSM, Arisma Spectrum všechny v produktovém portfoliu společnosti Computer Associates. Microsoft má v této oblasti své zastoupení produktem Microsoft Operation Manager, který je však limitován prostředím operačního systému Windows.

Systémy řízení výkonnosti (Performance management systems) - tento typ software je určen ke sledování výkonnosti infrastruktury IS/ICT, aplikací, systémů i služeb. Performance management nástroje zpracovávají zpravidla informace spojitého charakteru. Informace o stavu prvků IS/ICT jsou získávány a ukládány do performance management databáze periodicky v předem definovaných intervalech. Narozdíl od předchozí skupiny produktů, zde dochází k ukládání i informací o tom, že je prvek, služba, server dostupný a tím pádem vzniká spojitost monitorovacích dat. Typickými příklady indikátorů výkonnosti jsou například zatížení CPU, využití paměti, datový přenos na rozhraní routeru, dostupnost služby ale také například počty úspěšně i neúspěšně zpracovaných transakcí na back-end systémech, délky trvaní transakcí apod.

Nejrozšířenější service-centric performance management software je bezesporu robustní platforma InfoVista od stejnojmenného dodavatele. HP OpenView Performance Insight společnosti Hewlet-Packard je další produkt, který poskytuje platformu pro monitorování výkonnosti systémů, sítí a na nich provozovaných aplikací.

Systémy pro řízení bezpečnosti (Security management systems) - tento typ software je určen ke sledování a analýze bezpečnostních událostí. Na základě funkcionalit, které tyto systémy poskytují, je lze členit na:

1. **IDS (Intrusion Detection Systems)** - systémy detekce neoprávněného průniku rozumějí síťovým protokolům a tím umožňují rozpoznat určité signatury, které naznačují bezpečnostní útoky. Signatura je definována množinou podmínek, které když jsou splněny, naznačují pokus o neoprávněný průnik. Signatura tak obsahuje popis známých útoků a podezřelých aktivit. Tento typ zařízení je schopen detekovat bezpečnostní incidenty a zaznamenat je v logu, avšak již není určen k jejich aktivnímu řešení,
2. **IPS (Intrusion Prevention Systems)** - systémy zamezení narušení bezpečnosti jsou na rozdíl od detekčních systémů schopny i zabránit bezpečnostnímu incidentu tím, že jsou zapojeny do cesty síťového provozu mezi takovými části infrastruktury, kde je to žádoucí.

V poslední době je trendem integrovat skupiny produktů, do kterých patří IDS, IPS, firewally, antiviry, VPN brány apod., do jednoho univerzálního bezpečnostního softwarového nástroje. Tento typ komplexních řešení pak často bývá nazýván UTM (Unified Threat Management).

3. **SIEM (Security Information Event Management)** - tento typ software umožňuje získávat a analyzovat bezpečnostní události týkající se provozu IS/ICT z koncových zařízení. Hlavními úkoly SIEM systémů jsou:
    a. komplexní analýza bezpečnostních dat z různých zdrojů, které spolu na první pohled nemusí vždy úplně souviset,
    b. archivace bezpečnostních událostí, která je v určitých typech organizací, např. bankách, vyžadována normami a regulacemi,
    c. zajištění integrity bezpečnostních událostí,
    d. korelace událostí z různých typů síťových prvků,
    e. sledování privilegovaných uživatelů systému,
    f. zpracování auditních žurnálů (informace z logu systému),
    g. podpora provozu Security Operation Center (SOC) korelací, analýzou a prezentací bezpečnostních událostí.

Zpracování bezpečnostních událostí probíhá v těchto systémech zpravidla v několika fázích. V první fázi jsou přijímány informace z monitorovaných zařízení,

bezpečnostních systémů, sond a ostatních specializovaných komponent bezpečnostního monitorování. Mezi monitorovaná zařízení patří servery, pracovní stanice, síťové komponenty, informační systémy a další. Mezi bezpečností systémy patří například firewall, antivirový a antispyware software, analyzátory datových toků apod. Hlavním cílem této fáze je rychlý, spolehlivý, přesný a efektivní přenos těchto informací z ohroženého zařízení nebo bezpečnostního systému do monitorovacího systému. Způsoby přenosu informací mohou být různé a jejich výběr je závislý na typu monitorovaného systému a přenosových možnostech síťové infrastruktury. Mezi nejrozšířenější patří SNMP trapy a syslogové zprávy, které nemají vysoké nároky na síťový přenos, avšak na druhé straně nesplňují požadavek na spolehlivost doručení informací. V obou případech je přenos založen na nestavovém protokolu UDP, a proto standardně nedochází k potvrzení přijetí zprávy monitorovacím systémem. Dalším způsobem přenosu monitorovacích dat je zpracování auditních žurnálů, který je sice spolehlivý, avšak nedochází zde k předávání informací v reálném čase. [30]

Ve druhé fázi jsou posbírané informace v různých formách (SNMP trapy, syslog zprávy, auditní žurnály) dále zpracovány speciálními programy a následně předány do centrálního dohledového systému, kde jsou prezentovány v podobě alarmů informujících o bezpečnostních incidentech. Dále zde dochází k nastavení deduplikace a korelace nad příchozími alarmy. Deduplikace představuje nahrazení opakovaného výskytu alarmu jedním alarmem spolu s uvedením počtu jeho výskytů. Korelace umožňuje další analýzu a akce (např. zvýšení závažnosti při opakovaných výskytech alarmu, párování alarmů a následné snížení závažnosti apod.) nad doručenými bezpečnostními alarmy v dohledovém systému. Například alarmy upozorňující na tři neúspěšné přihlášení uživatele do určitého systému budou korelovány s alarmem upozorňující na uzamčení účtu stejného uživatele v daném systému. Na závěr druhé fáze jsou nastaveny notifikační a eskalační příznaky.

Ve třetí fázi dochází k notifikaci pověřených osob popřípadě vlastních uživatelů, kterými byl bezpečnostní incident vyvolán. Alarmy jsou po dobu jejich řešení uchovávány v databázi centrálního dohledového systém a následně pak archivovány do archivní databáze. Nad archivní databází jsou implementovány reportovací nástroje, které umožňují forenzní analýzu a zpracování těchto dat.

4.2.8 Ekonomické aspekty zavedení monitorování aplikací a služeb

4.2.8.1 Přínosy monitoringu

Společnosti mohou získat ze zavedení monitorování mnoho různých přínosů. Některé přínosy ze zavedení monitoringu jsou měřitelné (dosažení stanovených SLA, SLO, OLA), jiné jsou naopak měřitelné a kvantifikovatelné velmi těžko, popř. vůbec (např. změna způsobu práce zaměstnanců, kterých se monitorování přímo dotýká v důsledku inovace procesů v oblasti řízení problémů a incidentů vzniklých v infrastruktuře v podniku, kde implementace monitorování slouží jako podpora této změny nebo zkvalitnění služeb koncovým uživatelům). V současnosti jsou sledovány převážně měřitelné přínosy zavedení monitorování, které lze často kvantifikovat i v poměrně krátkém období po implementaci řešení. Následující text popisuje některé z klíčových přínosů:

1. získání podkladů ke stanovení, měření a dosahování dohod SLA,
2. schopnost srovnat business požadavky s výkonností systémů a aplikací - v některých případech, kdy systémy poskytují vyšší výkonnost a dostupnost, než je možné využít businessem, může paradoxně dojít k motivaci ke snížení SLA a tím i ke snížení nákladů na jeho dosažení,
3. pro-aktivním přístupem zlepšení kvality poskytovaných služeb koncovým (interním i externím) zákazníkům,
4. snížení počtu výpadků - studie ukazují, že jeden z klíčových faktorů ke zvýšení produktivity práce je snížení času, po který jsou klíčové aplikace, systémy a služby nedostupné,
5. zlepšení komunikace a spolupráce mezi pracovníky podpory IT - často uváděný přínos,
6. efektivnější správa IS/ICT a využití existujících informačních technologií - vede k efektivnějšímu a méně nákladnějšímu provozu IS/ICT a business aplikací,
7. snížení nákladů na:
    - provoz sítě a úložiště dat,
    - administraci business aplikací,
    - mzdové náklady spojené s provozem a správou aplikací a systémů;
8. zlepšení zákaznického servisu - nabídka služeb zákazníkům 24x7,
9. zvýšení ROI - Return On Investment.

4.2.9 Důležité faktory při zavádění monitorování business aplikací

4.2.9.1 Return on Investment

Jedním z nejdůležitějších faktorů, který je třeba uvažovat při zavádění systému monitorování v podniku, je ROI (Return On Investment) neboli vyčíslený návrat z investice. Samotný vzorec pro výpočet ROI zní: „Příjem z investice za stanovenou dobu vydělený finančním množstvím investice za stejnou dobu.“

ROI = kvantifikovatelné přínosy/ kvantifikovatelné náklady

Avšak i tato charakteristika má svá úskalí a někdy se může stát ne zcela vypovídající. Největším problémem je zpravidla složitost vyčíslení nákladů, protože zavedení nového systému IT spolu často přináší další dodatečné náklady, které jsou obtížněji kvantifikovatelné. Nejčastěji se jedná o náklady na síť a její provoz, na personál odpovědný za zavedení a podporu a v některých případech i na uživatele. Tak, jak bylo zmíněno v úvodu kapitoly, také přínosy mohou být v některých případech složitě kvantifikovatelné. Na druhé straně ROI je metrika, která je stanovena za určité předem dané období, a proto je třeba vytvořit určité srovnání stavu před a po zavedení. Další zajímavý poznatek spočívá v tom, že při jednom zavedení monitorování klíčových business aplikací, služeb či datových toků mají různé přínosy dopad na různé skupiny uživatelů. V závislosti na typu monitorování (fault monitoring, performance monitoring, E2E monitoring) jsou výstupy z monitorovacího systému doručovány různým skupinám uživatelů, jakými jsou operátoři dohlížející na provoz služeb, aplikací a IS/ICT infrastruktury jako celku, business vlastníci monitorovaných služeb či aplikací, servisní manažeři a neposledně i jejich systémoví administrátoři. Implementace monitoringu například nabídne business vlastníkům přínosy v podobě reportů měření dosažení SLA a naopak servisním manažerům a systémovým administrátorům přínosy v podobě informací o provozním stavu aplikace či služby 24 hodin denně. Tyto informace jsou následně využitelné v procesu zlepšování kvality poskytované služby koncovým zákazníkům.

4.2.9.2 Total Costs of Ownership

Podniky si při rozhodování o zavádění nových IS/ICT kladou velmi důležitou otázku: „Kolik to celkově bude stát?“. Dle Baileyho [1] je zpravidla jednoduché zkalkulovat transparentní náklady, jakými jsou pořizovací cena HW a cena licencí SW, avšak tím zdaleka náklady nekončí. Vedení podniků je kolikrát udiveno, že i v případě úspěšné implementace nového IS/ICT či jeho části dochází v průběhu provozu ke stále se zvyšujícím provozním nákladům a nákladům na údržbu nově implementovaného IS/ICT.

Total Costs of Ownership (TCO) je metodika určena ke stanovení celkových nákladů spojených s pořízením, vlastněním a provozem nových IS/ICT nebo jejich jednotlivých částí po dobu životního cyklu. I přesto, že metodika TCO byla původně používána na vyčíslení nákladů při nákupu a provozu desktopových počítačů a desktopového softwaru, díky rozšíření na sítě, client/server software, distribuované zpracování dat apod., je dnes aplikovatelná i v případě pořizování systému monitorování. TCO je navržena tak, aby zohlednila a zkalkulovala i skryté náklady na vlastnění technologie, které by nemusely být jinými metodami zaznamenány a tudíž ani zohledněny. Tato vlastnost TCO je velmi přínosná také u nákladů spojených s pořízením a nasazením systému monitorování.

TCO se skládá z přímých a nepřímých nákladů vzniklých v průběhu životního cyklu aktiva IT a zahrnuje náklady na jeho pořízení, implementaci či instalaci, provoz, podporu a vyřazení.

Rozdělení nákladů v rámci TCO:

Náklady přímé - obvykle pokrývají viditelnou část ICT a jejich podporu

1. HW a SW:
    - pořizovací náklady (nákupní cena HW či SW) nebo náklady na pronajímání HW či SW. V případě vydělení těchto nákladů dobou životního cyklu aktiva IT lze spočítat roční náklady,
    - náklady na související a přídavný HW (síťové prvky, kabeláž, úložiště dat apod.),
    - náklady na údržbu poskytovanou dodavatelem v případě uzavřené smlouvy,
    - náklady na náhradní díly, náhradní systémy, roční náklady všech dodávek dalších komponent a materiálu,

2. Provoz:
    - mzdové náklady na zaměstnance zajišťující provoz ICT, náklady na helpdesk,
    - náklady na provoz a správu sítě, uživatelských stanic,
    - provozní náklady zabezpečující projekt zavedení ICT (nákup nábytku, pronájem kanceláří),
3. Administrativa:
    - náklady na práci ostatních oddělení (personální oddělení, finanční oddělení, jiné administrativní síly) zapojených do projektu zavádění ICT,
    - náklady na plánování implementace ICT,
    - náklady na školení pracovníků ICT i běžných uživatelů.

Náklady nepřímé - zpravidla nebývají na první pohled viditelné a jsou rozptýlené v podnikových procesech uvnitř společnosti. Skládají se z:

1. práce koncových uživatelů - veškeré investice do nových ICT zpravidla vyžadují náklady na podporu koncových uživatelů. Tyto náklady jsou identifikovány a vyčísleny v rámci projektu zavedení ICT. Mnohdy se však objevují jiné méně evidentní náklady spojené s akcemi koncových uživatelů. Tyto náklady vznikají tehdy, když si koncoví uživatelé pomáhají řešit případné problémy s ICT sami tzv. „na vlastní pěst“ bez podpory specializovaného oddělení ICT. Do této skupiny nákladů patří i samostudium (resp. neformální školení) či vývoj vlastních aplikací koncovými uživateli, kteří tím neplánovaně spotřebovávají čas i podnikové zdroje. Pro přesnější vyčíslení TCO je třeba zachytit a vyčíslit i tyto náklady, což bývá zpravidla velmi obtížné,
2. výpadky systému - sem patří převážně náklady na ztrátu produktivity zaměstnanců v případě plánovaných či neplánovaných výpadků systému. Plánované výpadky jsou způsobovány údržbou IS/ICT (nutná aplikace patchů, či rekonfigurace částí IS/ICT) a neplánované výpadky vznikají náhodně v důsledku jiných vlivů (selhání části IS/ICT či selhání lidského faktoru).

4.2.9.3 Outsourcing

Další možností, jak se postavit k implementaci monitorování, je možnost outsorcingu celého řešení. V současné době se stává velmi populární model MSP (Monitoring Service Provider), který zajišťuje poskytování služeb monitorování IS/ICT a business aplikací prostřednictvím internetu.

Základní charakteristické rysy modelu MSP:

- MSP vlastní a provozuje softwarové aplikace, které monitorují infrastrukturu a aplikace zákazníka,
- MSP poskytuje svým zákazníkům přístup do instance monitorovací aplikace odkudkoliv ze sítě internet prostřednictvím webového prohlížeče či jiného tenkého klienta,
- MSP účtuje zákazníkům poplatky za používání monitorovacího systému.

Výhody modelu MSP:

- pro malé firmy nižší vstupní náklady na monitoring IS/ICT a rychlejší nastavení monitorování,
- nepotřebnost specializované infrastruktury IS/ICT pro běh monitoringu aplikací, která je přenesena na MSP,
- snížení nákladů na zajištění SLA,
- efektivnější plánování kapacit infrastruktury IS/ICT.

Při rozhodování o implementaci či volbě modelu MSP je vždy důležité brát v úvahu konkrétní podmínky daného podniku. V konkrétních podmínkách je třeba rozhodnout, zda se daná volba podniku vyplatí s ohledem na strategii IS/ICT do budoucna.

Základní faktory rozhodování o outsourcování monitorování:

- neexistence vlastní monitorovací infrastruktury IS/ICT,
- ekonomické faktory - rentabilita.

4.3 Trh s produkty IT operations management (ITOM)

Dynamicky, avšak nesourodě se rozvíjející trh s produkty řízení, správy a provozu IS/ICT (IT Operations Management Software - ITOM) prochází několika vývojovými stádii jak ve světě, tak i v České republice. Zatímco ve světě vzniká tento trh již v letech 2000 - 2001, v České republice vlivem některých faktorů,

které budou zmíněny v kapitole *4.3.2 Trh ITOM v ČR*, se rodí tento trh až v roce 2002. V prvním stádiu (2000-2001) dochází ve světě ke vzniku a postupnému rozvíjení trhu a posílení pozice firem specializujících se na některé oblasti z IT Operations Management. Ve druhém stádiu dochází ke vstupu velkých softwarových společností do této oblasti a posílení jejich pozic. Ve třetím stádiu (2005 – 2006) dochází k postupné konsolidaci tohoto trhu. V tomto období vznikají první akvizice společností za účelem snadnějšího vstupu na trh nebo zlepšení své stávající pozice na trhu.

V současnosti je situace odlišná jak ve světě, tak v ČR, kde je alespoň částečně možné zhodnotit nabídku a poptávku po produktech ITOM. Jelikož se oba trhy (český a světový) vyvíjejí v odlišných podmínkách, je kapitola rozdělena na popis a vývoj světového a českého trhu. Trh je popsán jak kvantitativně (objem trhu a jeho penetrace), tak kvalitativně - převážně z hlediska produktů a pozice jejich dodavatelů.

4.3.1 Trh ITOM ve světě

Dle společnosti Gartner's Group [18] dosáhl v roce 2005 celkový objem trhu 9,9 miliard USD, což představuje celkově 12,6 % nárůst oproti roku 2004. Objem trhu je metodicky měřen jako celkový výnos software, který zahrnuje výnosy z prodeje nových licencí, softwarových aktualizací, subskripcí a hostování, technické podpory a údržby. Do výpočtu nejsou zahrnuty výnosy z poskytování profesionálních služeb a prodeje hardware. Následující tabulka ukazuje srovnání podílů nejvýznamnějších dodavatelů na trhu ve letech 2004 a 2005.

Dodavatel	Výnosy 2005 (mil. USD)	Podíl na trhu 2005 (%)	Výnosy 2004 (mil. USD)	Podíl na trhu 2004 (%)	Meziroční nárůst příjmů (%)
IBM	2 398,1	24,2	2 182,0	24,8	9,9
CA	1 318,4	13,3	1 194,5	13,6	10,4
BMC	1 188,4	12,0	1 164,4	13,2	2,1
HP	724,9	7,3	576,8	6,6	25,7
Quest SW	384,1	3,9	323,6	3,7	18,7
Ostatní	3 893,1	39,3	3 359,7	38,2	15,9
Celkem	**9 907,1**	**100,0**	**8 801,0**	**100,0**	**12,6**

Tabulka 4-1 - Celosvětový odhad tržeb dodavatelů ITOM
zdroj:Gartner's Dataquest (červen 2006)

Z tabulky je patrné, že předních pět dodavatelů si v těchto letech rozdělilo přibližně 60 % celosvětového trhu. Tento trend je dán zejména uskutečněním řady akvizic, které jsou pro toto období charakteristické. Například IBM kupuje Micromuse,

Computer Associates kupuje Concord Communications atd. Ze studie dále vyplývá, že Configuration management byl nejrychleji rostoucí oblastí s meziročním nárůstem o 25 %, což je převážně způsobeno stále zvyšujícími požadavky IT manažerů na IT Configuration management, který s konfigurací prvků IS/ICT přímo souvisí. Produkty používané pro řízení dostupnosti a výkonnosti (availability a performance management) získaly v roce 2005 nejvyšší podíl (25 %) na trhu. Toto je dlouhodobý trend, kdy společnosti zvyšují důraz a prioritu na investice do nástrojů podporující availability a performance management, které pomáhají integrovat následující oblasti: end-to-end service quality results, event management, end-to-end application transaction measurement, SLA monitoring & reporting a business service management. Společnost Gartners's Group dále uvedla v březnu 2007 studii [19], ve které kvantifikuje současný trh a uvádí predikci budoucího světového trhu s produkty z oblasti IT Operations Management. Z této studie vyplývá, že od počátku má trh rostoucí tendenci. Gratner's predikuje nárůst trhu z 11 miliard USD roce 2006 až na téměř 17 miliard USD v roce 2011, což představuje velmi významný růst investic v této oblasti IS/ICT. Studie kvantifikuje výnosy v následujících oblastech: application management, asset management, availability and performance, configuration management, database management, IT service desk and help desk, job scheduling, network management, a další IT operations management (output management) podle regionů. Tabulka 4-2 obsahuje predikci celosvětového vývoje objemu trhu v jednotlivých oblastech IT Operations Management.

IT Operations Management area	2005	2006	2007	2008	2009	2010	2011	CAGR (%) 2006-2011
Application Management	1 100,5	1 309,6	1 529,6	1 751,6	1 959,1	2 135,4	2 274,2	11,7%
Asset Management	307,9	355,7	409,0	469,6	533,0	593,3	643,8	12,6%
Availability and Performance	2 464,0	2 643,9	2 828,9	2 995,7	3 129,0	3 224,7	3 305,3	4,6%
Configuration Management	1 628,4	2 035,5	2 503,6	3 029,4	3 605,0	4 217,8	4 850,5	19,0%
DBMS Management	1 329,8	1 399,0	1 470,3	1 540,9	1 598,0	1 620,6	1 636,8	3,2%
IT Service Desk and Help Desk	757,9	860,2	959,1	1 044,6	1 122,8	1 179,3	1 228,8	7,4%
Job Scheduling	779,7	835,9	894,4	955,2	1 017,3	1 073,3	1 116,2	6,0%
Network Management	1 205,9	1 304,8	1 405,2	1 495,6	1 565,0	1 614,1	1 654,4	4,9%
Other ITOM	333,0	310,4	301,8	290,9	275,9	257,8	268,2	-2,9%
Total	**9 907,0**	**11 054,8**	**12 302,1**	**13 573,5**	**14 805,0**	**15 916,2**	**16 978,1**	**9,0%**

Tabulka 4-2 - Total ITOM Software Revenue by subsegment, 2006-2011 in millions $
zdroj: Gartner's Dataquest (January 2007)

Ze studie vyplývá, že průměrný meziroční nárůst v objemu trhu jako celku je 9 %. Nejvíce vzrůstají investice, tudíž i podíl na trhu v oblasti configuration managementu, nejméně naopak v řízení a dohledu databázových systémů. Studie

předvídá dokonce již v roce 2008 vyšší podíl segmentu configuration management než doposud stabilně největší podíly availability a performance managementu.

Tabulka 4-3 znázorňuje podíl na trhu rozdělen dle jednotlivých regionů. Největší podíl na trhu má Severní Amerika, kde se projevuje již tradičně velikost tohoto trhu a větší ochota firem investovat do inovací své ICT infrastruktury.

Region	2005	2006	2007	2008	2009	2010	2011	CAGR (%) 2006-2011
Asia/Pacific	523,9	641,3	779,6	926,8	1 078,6	1 235,2	1 400,6	16,9%
Europe	3 600,4	4 007,9	4 460,1	4 846,4	5 234,0	5 591,6	5 927,1	8,1%
Japan	447,6	483,3	534,5	581,4	625,4	664,9	700,0	7,7%
Latin America	230,0	263,5	300,7	336,8	372,6	406,2	439,8	10,8%
Middle East and Africa	151,6	180,9	209,1	243,4	277,8	309,5	342,5	13,6%
North America	4 953,6	5 477,9	6 018,1	6 638,7	7 216,7	7 709,0	8 168,1	8,3%
Total	**9 907,0**	**11 054,8**	**12 302,1**	**13 573,5**	**14 805,0**	**15 916,2**	**16 978,1**	**9,0%**

Tabulka 4-3 - Total ITOM Software Revenue by region, 2006 - 2011 in millions $
zdroj: Gartner's Dataquest (January 2007)

4.3.1.1 Souhrn poznatků o světovém trhu ITOM

- od jeho vzniku trh ITOM meziročně neustále roste,
- v letech 2007 - 2011 trh poroste meziročně přibližně stejně jako je průměrný meziroční růst trhu v IT odvětví obecně,
- tento růst trhu bude udržen tím, že tento druh technologií má zpravidla dobrý Return On Investments (ROI), protože obecně pomáhají optimalizovat využití již existujících informačních technologií a tím snižují náklady na provoz celkové IS/ICT infrastruktury, což implikuje i zlepšení kvality poskytovaných služeb a snížení rizik,
- vlivem mnoha akvizicí vzniká tendence rozdělení trhu mezi několik málo nadnárodních společností. Tento trend se bude i v příštích letech nadále prohlubovat,
- provoz IT (IT operations) se postupně stává oblastí vyššího zájmu v IT organizacích, protože je stále více zodpovědná za dosahování obchodních přínosů ve srovnání s jinými oblastmi podniku, jakými jsou např. marketing, prodej apod. Informační technologie přímo podporují ostatní oblasti, a proto jejich efektivní řízení a provoz je nezbytnou součástí získání konkurenční výhody na trhu. To motivuje dodavatele k vytváření inovativních řešení v oblasti IT operations,
- v posledních letech dochází ke změně postoje koncových uživatelů směrem k provozu IS/ICT tak, že spíše požadují dostupnost a výkonnost

provozovaných služeb, které jsou pro ně akceptovatelné z jejich pohledu než reporty o úrovni služeb, které vypovídají o jejich stavu z pohledu vnitřního fungování dané služby. Tento jev má za důsledek rozšíření používání monitorovacích nástrojů typu E2E k měření výkonnosti a dostupnosti dané služby z pohledu koncového uživatele. Implementace moderních technologií, jakými jsou např. webové služby nebo SOA, zvyšují komplexnost služeb, což otevírá prostor na trhu v oblasti řízení a monitorování aplikací (application management) a v oblasti produktů podporujících vizualizaci a mapování hierarchie komponent služeb (service management),

- poptávka po produktech z oblasti ITOM bude růst i na základě potřeby podniků dodržovat nové zákony a nařízení. Hlavním faktorem rozhodujícím pro pořizování produktů z oblasti ITOM bude bezesporu potřeba podniků vytvářet a provozovat spolehlivější a dostupnější služby. To je příležitostí pro firmy nabízející produkty ze segmentů Configuration management (řízení změn v IS/ICT) a Asset management (řízení správy veškerého majetku i majetku, který nemá povahu IS/ICT),
- trh bude v nejbližší době pozitivně ovlivněn taktéž faktem, že stále více stoupá obliba a ochota implementovat procesní koncepty, jakými jsou např. ITIL, COBIT apod.,
- z dlouhodobého hlediska působí pozitivně na růst trhu ITOM i fakt, že v podnicích dochází ke stále větší fragmentaci IT aplikací, ale i celkové ICT infrastruktury. Fragmentace IS/ICT, zavádění a používání moderních technologií (webové služby, SOA apod.) zvyšují náklady na řízení a správu IS/ICT. Na druhou stranu proti tomu působí fakt, že i tyto technologie pomáhají zavádět a integrovat systémy řízení a podpory provozu IS/ICT,
- dlouhodobě bude na růst trhu působit i fakt, že společnosti stále více investují do projektů následujících typů: dynamického poskytování a vytváření infrastruktury IS/ICT, optimálního využívání zdrojů IT ale i ostatních aktiv, řízení aplikací patchů na IT systémy, řízení a správa J2EE aplikací, řízení a správa sítí a následná korelace a zpracování generovaných událostí, správa a plánovaní rutinních úloh,
- stále větší důraz je firmami kladen na zabezpečení sítí, systémů a aplikací na nich provozovaných, a proto lze očekávat i nárůst v prodeji systémů SIEM

(Security Information & Event Management). Tento růst opět pozitivně působí na růst v celé oblasti ITOM,

- naopak negativně na růst trhu působí následující faktory. Z krátkodobého hlediska je to neporozumění dodavatelů zákaznickým potřebám či špatná definice zákaznických potřeb nebo nedostatečná kvalita podpory produktů. Nedostatek produktů pro malé a střední podniky působí negativně na růst trhu ITOM pro tento segment zákazníků. Mnoho akvizic v této oblasti v posledních letech nutí potencionální odběratele být obezřetnější při výběru konkrétních řešení. Vlivem stále větší konkurence na trhu dochází ke snižování cen produktů v méně aktuálních oblastech, což částečně negativně ovlivňuje velikost trhu. Z dlouhodobého hlediska se dodavatelé působící na trhu ITOM potýkají s následujícími problémy negativně ovlivňující tento trh:
    - včasné dodání produktů a jejich nasazení,
    - snížená kvalita produktů, která vychází z trendu, co nejdříve produkt dostat na trh a utržit za něj i za cenu následných patchů a oprav,
    - nedostatek efektivního marketingu pro tyto produkty,
    - nedostatečně funkční distribuční kanály apod.

4.3.2 Trh ITOM v ČR

Vývoj trhu s produkty z široké oblasti IT Operations Management vychází částečně z trhu světového, avšak vlivem vnějších ekonomických a psychologických faktorů dochází ve vývoji k určitým odlišnostem, o kterých se zmiňuji v následujícím textu. V České republice dochází k rozvoji trhu s přibližně dvouletým zpožděním a v současnosti není ještě tento trh dostatečně vyzrálý v porovnání s trhem celosvětovým. V některých segmentech ITOM (např. fault management) je sice trh relativně nasycen a rozebrán velkými společnostmi IBM, HP, CA atd., avšak stále zbývá nevyužitý prostor pro zbylé segmenty z ITOM portfolia (configuration management, security management, asset management apod.).

V tuto chvíli se lze domnívat, že pomalejší rozvoj trhu v ČR je dán převážně charakteristickými podmínkami lokálního trhu, které lze shrnout následovně:

- na straně poptávky je menší kupní síla potencionálních kupců řešení v porovnání s americkými či západoevropskými společnostmi, které provádějí pravidelné a vyšší investice do rozvoje svých IS/ICT,

- světová úroveň cen licencí za produkty z oblasti ITOM je pro mnohé české podniky příliš vysoká,
- naopak obecná tendence většiny podniků v ČR je získat maximum z informační technologie bez větší ochoty reinvestovat finanční prostředky na zlepšení provozu či inovace,
- oblast potencionálních kupců se tedy zužuje na velké telekomunikační společnosti, poskytovatele datových a hlasových služeb a bankovní instituce, které zpravidla mají ve svých rozpočtech pravidelně plánované prostředky na rozvoj a provoz IS/ICT,
- nedostatek produktů pro malé a střední podniky negativně působí na rozvoj trhu,
- nedůvěra dodavatelů řešení ve schopnost svých partnerů prodat jejich produkty.

Do budoucna se na českém trhu prosadí společnosti dodávající svá řešení z oblasti ITOM pro menší a střední podniky (SME) za příznivější ceny. I přesto, že dodavatelé řešení přicházejí za klienty s „akčními nabídkami“ zavedení, je v současnosti poptávka po produktech ITOM stále limitována.

4.4 Vybrané metodické přístupy k řízení IS/ICT a poskytování služeb ICT

Tvorba metody monitorování IS/ICT vychází z existujícího metodického rámce řízení ICT a poskytování IT služeb, který vytvoří informační základnu pro její tvorbu. Finální metoda monitorování pak bude v souladu s tímto metodickým rámcem. Navržená metoda monitorování ICT může dokonce prohloubit a detailněji rozpracovat některé zobecněné principy obsažené ve zvoleném zastřešujícím metodickém rámci. V současném světě IT můžeme nalézt celou řadu takových metodických přístupů lišících se obsahem, dostupností, ale i jejich zaměřením. Pro výběr metodického rámce byly do užšího výběru vybrány metodické rámce splňující následující kritéria: všeobecná známost a přijetí, široká použitelnost v podnikové IT praxi, perspektivita z hlediska budoucího používání a dalšího rozvoje. Na základě výše uvedených kritérií byly vybrány následující:

- CMM (Capability Maturity Model),

- EUP (Enterprise Unified Process),
- COBIT (Control Objectives for Information and Related Technology),
- ITIL (Information Technology Infrastructure Library).

4.4.1 CMM

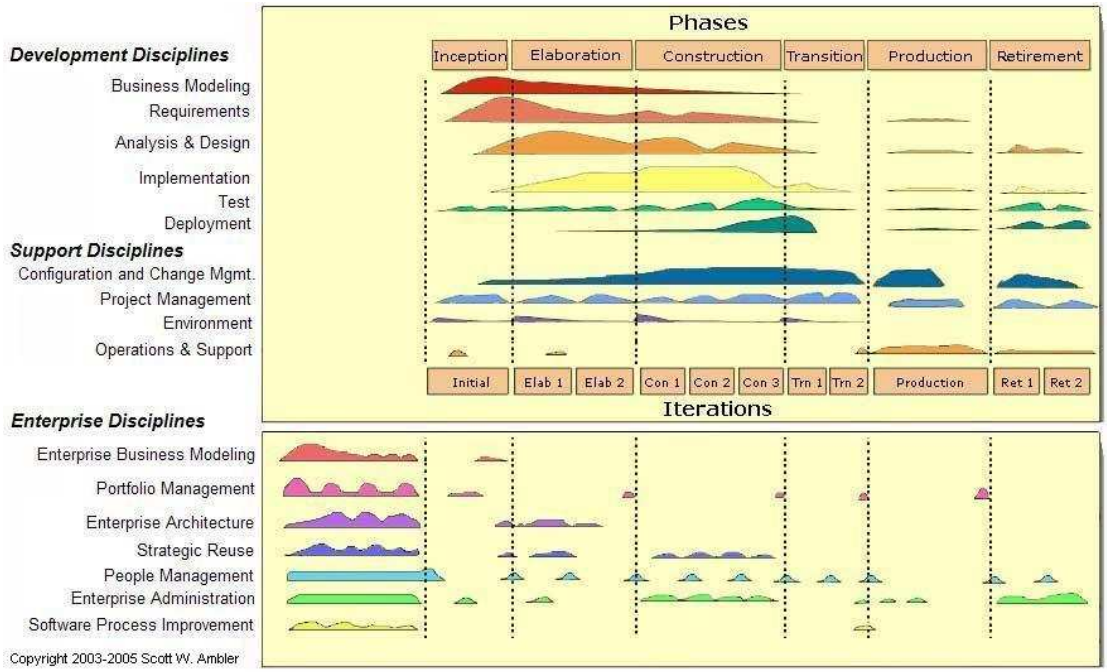
CMM je metodika, která se zabývá definicí, vývojem a zlepšováním procesů v organizaci. Poprvé byla popsána a použita v rámci řízení procesu vývoje software v knize Wattse Humpreyho Managing the Software Process. Metodika je založená na procesním modelu představující sadu praktik, které popisují základní charakteristiky efektivních procesů. Metoda CMM rozlišuje společnosti z hlediska fungování jejich procesů na vyspělé a nevyspělé. Každá společnost se nachází v jednom z pěti stádií vyspělosti Initial, Repeatable, Defined, Managed nebo Optimized od nejméně po nejvíce vyspělé. K dosažení jednotlivých stupňů procesu vývoje jsou definovány klíčové procesní oblasti (Key Process Areas), které musí být procesně zabezpečeny tak, aby společnost dosáhla příslušné hladiny vyspělosti. Posun mezi jednotlivými hladinami lze analogicky ukázat např. na stavbě domu. Stavba domu je také rozdělena do několika fází od budování základů přes stavbu nosných zdí až po zastřešení. Podobně je tomu u metody CMM, kde pro přechod do vyšší hladiny je třeba procesně zabezpečit všechny oblasti z nižší úrovně. Následující podkapitoly popisují jednotlivé stupně vyspělosti a procesy klíčových oblastí tak, aby bylo stupně dosaženo v rámci vývoje a nasazení softwarových produktů.

Jelikož metodika definuje, co by měl podnik udělat za účelem dosažení vyšší úrovně zralosti, avšak již nedefinuje, jakým způsobem toho dosáhnout, nejde o metodiku v pravém slova smyslu, ale jedná se spíše o metodický rámec.

4.4.2 EUP

EUP je metodika, která rozšiřuje RUP (Rational Unified Process) a je zaměřena na řízení vývoje, provozu a podpory informačních systémů podniku. Do původní RUP metodiky, která nepostihovala procesy a disciplíny potřebné pro provoz a podporu (Operations and Support) výsledných systémů, byly tyto postupným vývojem přidány. EUP pohlíží na vývoj a nasazení informačního systému z pohledu životního cyklu projektu, který je rozdělen do několika fází. Každou fázi je třeba zajistit potřebnými disciplínami z oblasti ICT. Metodika prošla od svého

vzniku podstatným vývojem a její současnou podobu je možné vidět na Obr. 4-4, kde je barevnými částmi znázorněna potřeba zdrojů v rámci jednotlivých disciplín v průběhu životního cyklu vývoje, nasazení a provozu informačního systému.



Obr. 4-4 - Životní cyklus EUP[43]

Současná podoba životního cyklu EUP zahrnuje i fázi vyřazení systému z provozu (Retirement), která v předchozích verzích nebyla uvažována. Se zakomponováním této fáze je nutné uvažovat i potřebné IT disciplíny a zajistit je příslušnými zdroji. V EUP jsou nyní disciplíny rozděleny do třech kategorií: vývojové, podpory a celopodnikové (Development, Support a Enterprise). Ve srovnání s ostatními metodikami je EUP zaměřena primárně na aktivity spojené s vývojem a provozem IS, avšak nepokrývá veškeré procesy potřebné k řízení IS/ICT.

4.4.3 COBIT

COBIT byl vyvinut nezávislou výzkumnou institucí ITGI (IT Governance Institute). Metodika COBIT primárně pohlíží na řízení IS/ICT z hlediska strategického řízení podniku. Jejím hlavním cílem je vytvořit rámec pro řídící a kontrolní systém fungující nad prostředím IT, který bude nastaven ve shodě s ostatními řídícími a kontrolními systémy podniku. [44] Tento rámec zajišťuje v organizaci následující dílčí požadavky [26]:

- IT je postaveno rovnocenně s businessem,
- IT plně podporuje business,
- IT zdroje jsou zodpovědně využívány,
- IT rizika jsou adekvátně řízena.

Metodika je zaměřená obchodně, a proto není určena pouze uživatelům, auditorům, poskytovatelům IT služeb, ale především vlastníkům obchodních a řídících procesů podniku. Hlavní principy metodického rámce jsou shrnuty v následujících bodech:

1. podnik potřebuje získat podnikové informace, které odpovídají business požadavkům tak, aby dosáhl svých business cílů,
2. business požadavky podniku vyžadují investice do zdrojů IT,
3. zdroje IT jsou následně využity procesy IT,
4. procesy IT poskytují podnikové informace, které odpovídají na business požadavky.

Výstupy procesů ICT musí splňovat následující podmínky, které jsou označovány za tzv. informační kritéria:

- efektivita (effectiveness) - informace musí být potřebné, relevantní a poskytnuté včasným, konzistentním a použitelným způsobem,
- účinnost (efficiency) - potřebné informace musí být poskytovány s optimálním využitím zdrojů,
- důvěrnost (confidentiality) - poskytované citlivé informace musí být zabezpečeny proti neoprávněnému zneužití,
- integrita (integrity) - informace musí být kompletní, přesné a validní ve vztahu k obchodním očekáváním,
- dostupnost (availability) - informace musí být k dispozici business procesům nyní i v budoucnu v závislosti na potřebách podniku,
- shoda (compliance) - informace musí být ve shodě se zákony, předpisy a obchodními smlouvami, jejichž je business proces předmětem,
- spolehlivost (reliability) - na základě poskytnutých informací musí být management podniku schopen spolehlivě rozhodovat.

V metodice jsou definovány následující informační zdroje, které jsou využívány procesy IT:

- aplikace - uživatelské systémy i manuální procedury zpracovávající informace,
- informace - data ve všech formách používaná business procesy,
- infrastruktura - veškeré technologie a zařízení využívaná aplikacemi (HW, SW, O.S., SŘBD, síťové prvky atd.),
- lidé - všichni ti, kdo se podílejí na aktivitách spojených s plánováním, organizováním, nákupem, podporou, provozem, monitorováním a hodnocením IS/ICT bez ohledu na to, zda jsou interními zaměstnanci nebo externími pracovníky.

Procesy IT, které využívají výše uvedené zdroje musí být efektivně řízeny. Procesy IT jsou rozděleny do čtyřech oblastí představující životní cyklus IS/ICT. Tyto oblasti jsou následující:

- plánování a organizování - aktivity poskytující stavební kameny pro nákup, implementaci IS/ICT, poskytování služeb IT a jejich podporu,
- nákup a implementace - poskytují řešení a formují je do služeb,
- poskytování služeb IT a jejich podpora - kroky vedoucí k poskytnutí služby koncovým uživatelům,
- monitorování a hodnocení - monitoring a hodnocení procesů za účelem zajištění provozu služeb.

V rámci výše uvedených čtyřech oblastí je definováno celkem 34 procesů IT, které jsou následně měřeny. Tak, aby mohly být tyto procesy efektivně měřeny definuje COBIT následující metriky a způsoby měření:

- MM (Maturity Models) - podobně jako v metodice CMM je definováno 5 úrovní vyspělosti procesu (0 - neexistující, 1 - ad-hoc, 2 - intuitivní a opakující, 3 - definovaný, 4 - řízený a měřený, 5 - optimalizovaný),
- OM (Outcome Measures)[2] - měří, zda byly dosaženy business cíle. Jedná se o tzv. „lag indicators“, protože mohou být získány pouze na základě uskutečnění a dokončení předmětu měření,

[2] Nahrazují KGI (Key Goal Indicators) z předchozích verzí COBITu. Poslední verzí COBIT je 4.1.

- PI (Performance indicators) - dříve nazývány KPI (Key performance Indicators) umožňují sledovat průběh výkonnosti procesu IT. Měří průběžně, zda funkce a procesy IT jsou dostatečně výkonné na to, aby bylo dosaženo stanovených cílů, tzn. vypovídají o pravděpodobném výsledku dříve, než je znám.

COBIT zasahuje následující skupiny uživatelů:

- výkonné vedení podniku - získává hodnotu a ziskovost investic do IS/ICT, získává podkladové informace k řízení rizik v oblasti IS/ICT,
- obchodní vedení podniku - získává záruky nad řízením služeb IT poskytovaných interním oddělením IT nebo externími firmami,
- IT vedení podniku - poskytují řízené služby IT, které obchodní vedení podniku vyžaduje na základě své business strategie,
- audit - získává podklady o efektivnosti řízení IT.

COBIT je vhodným podpůrným nástrojem pro strategická rozhodnutí o IS/ICT. Tím však, že říká CO by mělo být dosaženo, avšak nikoliv JAK by toho mělo být dosaženo, doporučuje jeho použití v kombinaci s dalšími standardy, popřípadě dalšími nejlepšími praktikami.

4.4.4 ITIL

Metodika ITIL je zkratkou pro „Information Technology Infrastructure Library“ a má původ v 80. letech ve Velké Británii, kde byla navržena vládní institucí UK Office Government Commerce (OGC) primárně k použití ve státní správě pro zefektivnění procesů při poskytování služeb IT. Záhy se však rozšiřuje i do komerční sféry. Vznikla jako sada knižních publikací popisujících způsob řízení služeb IT a IS/ICT infrastruktury, která je dostatečně obecná a univerzální[3], použitelná v organizacích všech velikostí. ITIL je na rozdíl od COBITu zaměřen specifičtěji na služby IT z hlediska taktického a operativního řízení. Podobně jako COBIT definuje procesy a činnosti, které je třeba zabezpečit, avšak konkrétní realizace je ponechána na rozhodnutí podniku samotného.

Mezi základní charakteristické rysy ITILu patří:

[3] ITIL lze použít dokonce i k návrhu procesů a procesnímu řízení firem mimo oblast ICT, tj. v jakékoliv firmě působící ve službách

- procesní řízení - používá na rozdíl od funkcionálního procesně orientovaný způsob řízení služeb IT. Procesy jsou definovány, řízeny, monitorovány, měřeny a vyhodnocovány a neustále zlepšovány, což je zpravidla odpovědností vlastníka daných procesů,
- zákaznicky orientovaný přístup - procesy jsou navrhovány primárně s ohledem na zákazníka, tzn., že každá aktivita v rámci procesu musí přinášet přidanou hodnotu pro zákazníka a pokud tomu tak není, je v procesu zbytečná,
- nezávislost na platformě - řízení procesů z oblasti ITSM dle ITIL je nezávislé na platformě.

Procesní řízení je založeno na modelu, který může být využit jako rámec pro zlepšování procesů následovně:
V rámci každého procesu definuje ITIL následující:

- rozpad na jednotlivé úkoly,
- pro každý úkol jsou definovány vstupy a výstupy (v přesné terminologii ITIL se jedná o RWO - objekty reálného světa, které mohou mít fyzický charakter např. faktura na papíře nebo mohou být v elektronické formě),
- každý úkol je vykonáván nějakou rolí, kde role je definována jako skupina odpovědností, aktivit a oprávnění,
- vykonávání role se řídí soustavou pravidel,
- každý proces musí mít svého vlastníka, který je zodpovědný za jeho definici,
- musí obsahovat metriky pro hodnocení (KPI).

4.4.4.1 Service Support

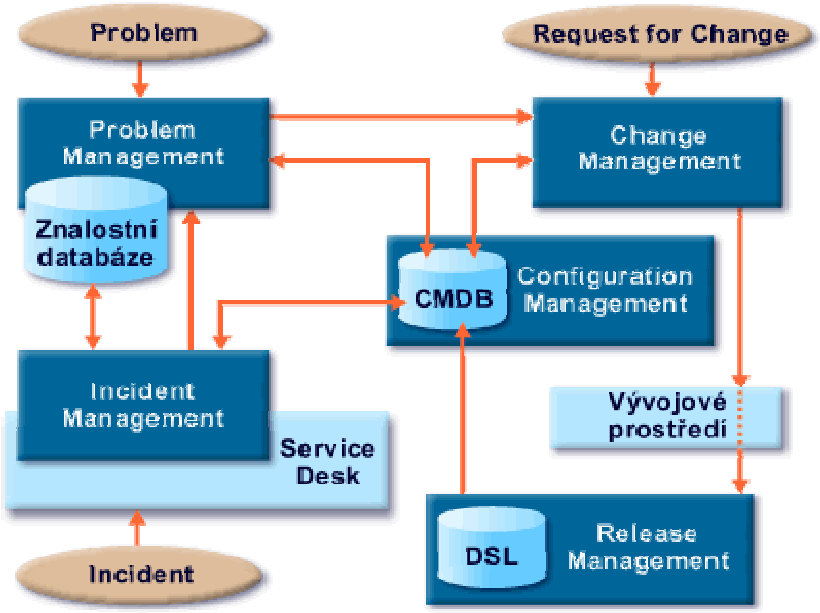
Na úrovni operativního řízení převládají procesy charakteru každodenního provozu, které jsou definovány v publikaci Service Support. Jednotným cílem těchto procesů je poskytování každodenní podpory uživatelům služeb IS/ICT. Výčet procesů je následující:

- Service Desk - poskytuje jednotné kontaktní místo mezi zákazníky služby, uživateli služby, podporou poskytovatele služby a podporami třetích stran. Proces popisuje, jak efektivně vytvořit kontaktní místo,
- Configuration Management - poskytuje logický model infrastruktury IS/ICT a na ní provozovaných služeb. Model je zajišťován identifikací, řízením

a správou verzí konfiguračních položek a jejich vzájemných vztahů mezi nimi. Hlavním nástrojem správy je konfigurační databáze (CMDB),

- Incident Management - incidentem se v terminologii ITIL rozumí událost, která není součástí standardního provozu služby a způsobuje nebo může způsobit přerušení nebo snížení kvality poskytované služby. Posláním procesu je co nejrychlejší obnovení normálního provozu dané služby tak, aby byly minimalizovány důsledky výpadků, přerušení dodávky či zhoršení kvality služby na její provoz; tedy v konečném důsledku na zákazníky a uživatele. Normálním provozem služby se rozumí provoz v rámci definované dohody SLA,
- Problem Management - problémem se v terminologii ITIL rozumí neznámá základní příčina jednoho či více incidentů. Proces se pak zabývá zjišťováním původních příčin incidentů. Hlavním úkolem procesu je minimalizovat nepříznivý dopad incidentů a problémů vznikajících v infrastruktuře IS/ICT na provoz business služeb, tedy na zákazníky a následně zajistit prevenci vzniku těchto chyb a s nimi spojených incidentů a problémů,
- Change Management - změny v rámci podnikové infrastruktury IS/ICT přicházejí buď jako výsledky řešení vzniklých problémů nebo jako proaktivní hledání obchodních přínosů v podobě zlepšování kvality poskytovaných služeb, popř. snižování nákladů na jejich provoz. Úkolem procesu je časově a nákladově efektivní aplikace schválených změn v podnikové infrastruktuře s minimalizací vzniku incidentů a jejich dopadů na provoz služeb (tedy dopadů na koncové uživatele a zákazníky),
- Release Management - release představuje v terminologii ITIL sadu schválených změn, které jsou aplikovány na služby IS/ICT. Proces se zabývá řízením nasazování nových verzí hardware a software do produkčního prostředí.

Zajímavé jsou vazby mezi jednotlivými procesy servisní podpory, které jsou znázorněné na Obr. 4-5.



Obr. 4-5 - Vazby mezi procesy operativního řízení

1. Incidenty, které vznikají v infrastruktuře, řeší proces Incident Managementu.
2. Incidenty jsou oznamovány na Service Desk - Service Desk je funkce (organizační jednotka), která ale zároveň plní roli 1. úrovně podpory v procesu Incident Managementu.
3. Incident Management potřebuje znalostní databázi, kterou řídí proces Problem Managementu, a konfigurační databázi (CMDB), kterou poskytuje proces Configuration Managementu.
4. Proces Incident Managementu použije informace z obou databází k vyřešení incidentu, ale proč incident nastal, se stále neví - zjistit příčinu incidentu je úkol pro Problem Management.
5. Incident Management není jediným zdrojem problémů - prakticky každý proces včetně procesů taktických může iniciovat vznik problému.
6. Problem Management použije informace z konfigurační databáze (CMDB), zjistí základní příčinu původního incidentu nebo problému a zahájí kroky vedoucí k odstranění této příčiny, tzn. iniciuje *Request for Change* (RfC), jímž se dále zabývá proces Change Managementu.
7. Problem Management není jediným zdrojem RfC - i některé další procesy mohou RfC iniciovat.

8. Change Management opět potřebuje informace z CMDB, aby mohl naplánovat realizaci změny co nejefektivněji, tzn. s co nejmenším dopadem na provoz služeb a s optimálními náklady.
9. O samotné nasazení změny do infrastruktury se pak stará proces Release Managementu, ale až po té, co je změna připravena a otestována ve vývojovém prostředí – povolení k implementaci dává Change Management, průběh implementace pak řídí Release Management.
10. Při implementaci je nasazena příslušná verze softwaru z *Definitive Software Library* (DSL).
11. Po úspěšné implementaci změny je provedena aktualizace CMDB.

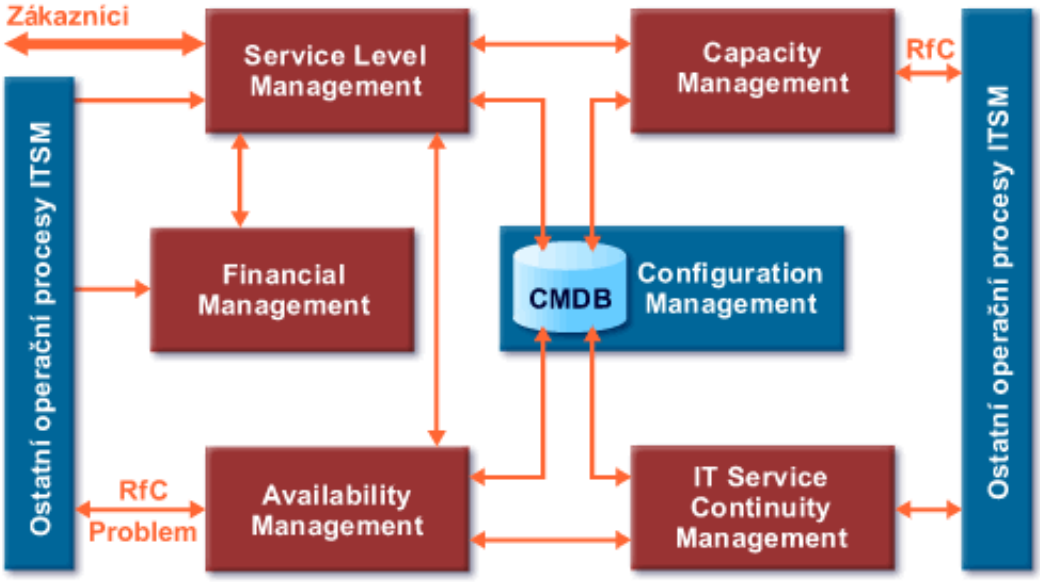
4.4.4.2 Service Delivery

Na úrovni taktického řízení převládají procesy charakteru dlouhodobějšího plánování. Hlavním cílem těchto procesů je vytváření vztahů se zákazníky a dosahování jejich dlouhodobé spokojenosti.

- Service Level Management - zabývá se plánováním, koordinací, navrhováním, uzavíráním, monitorováním a vyhodnocováním smluv o poskytování servisní podpory (SLA) se zákazníky a smluv se subdodavateli (OLA a UC). Cílem je řídit a zlepšovat jak kvalitu poskytovaných služeb, tak i vztah se zákazníky.
- Capacity Management - zodpovídá za zajištění trvale dostatečné kapacity infrastruktury tak, aby byly vždy uspokojeny všechny business požadavky, a to jak současné, tak i budoucí.
- Availability Management - proces optimalizuje schopnost infrastruktury IS/ICT, poskytovat takovou úroveň dostupnosti služeb na ní provozovaných, která splňuje definované business požadavky. Toho dociluje měřením a monitorováním dostupnosti IT služeb, porovnáváním těchto hodnot s business požadavky na jejich dostupnost a následně iniciováním kroků vedoucích k dosažení žádoucího stavu.
- IT Service Continuity Management - proces se zabývá způsobem zajištění poskytování business služeb a procesů, a to i za předpokladu, že dojde k negativním událostem v infrastruktuře IS/ICT (od selhání dílčí aplikace až po kompletní ztrátu předpokladů k obchodní činnosti).

- Financial Management for IT Services - proces podporuje plánování a plnění business cílů podniku s vazbou na jeho finanční zdroje; proces zodpovídá za evidenci nákladů na IT služby, vyhodnocování návratnosti investic do IT služeb a za všechny aspekty nákladů na znovu-obnovení provozu. Poskytuje podklady pro sestavování ICT rozpočtů a ceníků služeb.

Na Obr. 4-6 jsou znázorněny vazby mezi procesy taktického řízení z oblasti Service Delivery.



Obr. 4-6 - Vztahy mezi procesy taktického řízení

1. Service Level Management je proces jehož hlavním úkolem je vyjednat se zákazníkem druh a úroveň služeb, které mu budou poskytovány, tj. obsah dohody o úrovni poskytování služeb (Service Level Agreement - SLA).
2. Dostupnost těchto služeb je měřena a zjišťována prostřednictvím Availability Managementu. Service Level Management musí brát ohled na reálnou dostupnost služeb v okamžiku sjednávání SLA. Po uzavření SLA monitoruje Availability Management, zda je reálná dostupnost v mezích SLA.
3. Kapacitu (objem) služeb, které jsou k dispozici, měří Capacity Management, na což musí Service Level Management brát ohled již v okamžiku sjednávání SLA. Po uzavření SLA vyhodnocuje Capacity Management, zda je dohodnutá kapacita stále k dispozici.

4. Náklady na služby poskytované zákazníkům zjišťuje a eviduje Financial Management for IT Services. Pokud je uplatňována některá z forem zpoplatňování IT služeb, zajišťuje i účtování cen zákazníkům.
5. Obnovení kriticky důležitých služeb v případě globálního výpadku infrastruktury je starost IT Service Continuity Managementu, který úzce spolupracuje s Availability Managementem, zejména při analýze rizik a návrhu způsobu jejich eliminace.
6. Všechny aktivity taktických procesů však nejsou realizovatelné bez existence operačních procesů, zejména Configuration Managementu. Důvody pro úzkou provázanost jsou následující:

    - Service Level Management při sjednávání SLA musí vědět, které konfigurační položky se na dodávce sjednaných služeb budou podílet a jaký je jejich aktuální status. Po sjednání SLA je jejich obsah zanesen do CMDB (to má význam pro proces Incident Managementu, který v případě selhání některé konfigurační položky ihned zjistí, které služby pro které zákazníky jsou výpadkem zasaženy),
    - Aby Capacity Management mohl vyhodnocovat a plánovat kapacitu služeb, potřebuje vědět, které konfigurační položky se na dodávce služby podílejí,
    - Aby Availability Management mohl vyhodnocovat dostupnost služeb, potřebuje informace o souvisejících konfiguračních položkách, incidentech, problémech a změnách (všechny tyto informace jsou obsaženy v CMDB),
    - IT Service Continuity Management potřebuje CMDB mj. proto, aby mohl identifikovat kritická místa ICT infrastruktury. V případě zničení infrastruktury může podle záznamů v CMDB vybudovat tutéž infrastrukturu znovu.

7. Tím vazba taktických procesů na operační procesy nekončí:

    - Service Level Management potřebuje informace od Incident Managementu a Problem Managementu pro vyhodnocení míry plnění SLA,

- Financial Management for IT Services potřebuje informace od Change Managementu o změnách, aby je mohl vyhodnotit z hlediska nákladovosti,
- Pokud Availability Management zjistí, že reálná dostupnost služeb přestává být v mezích SLA, podniká příslušné kroky k nápravě (žádosti o změnu - Request for Change prostřednictvím Change Managementu nebo problému prostřednictvím Problem Managementu),
- Pokud Capacity Management zjistí, že kapacita služeb nepostačuje, podniká příslušné kroky k nápravě (inicializace Request for Change prostřednictvím Change Managementu). Současně Capacity Management vyhodnocuje každou navrhovanou změnu, zda nemá negativní dopad na kapacitu ostatních služeb,
- IT Service Continuity Management potřebuje údaje o minulých incidentech pro vyhodnocení rizik a rovněž používá proces Change Managementu pro realizaci změn v kontingenčních plánech.

4.4.5 Vztah ITIL a COBIT

V této podkapitole jsou shrnuty z několika zdrojů vztahy a rozdíly mezi metodickými rámci ITIL a COBIT. V zásadě jsou procesy ITIL kompatibilní s procesy COBIT, protože vývoj obou metodických přístupů probíhá ve vzájemné spolupráci zastřešujících institucí (ISACA, ITGI, OCG a itSMF), a proto existují i tabulky mapující navzájem procesy podle ITIL a COBIT.[4] Na druhé straně lze nalézt rozdíly v názvu některých procesů i definic, což je způsobeno tím, že oba dva přístupy mají jiný účel a primárně slouží jiným skupinám lidí. ITIL je zaměřen na řízení IS/ICT na různých úrovních, převážně však taktické a operativní, a vychází ze sady osvědčených postupů vzniklých v praxi. COBIT je více zaměřen na rozhodování o řízení IS/ICT na strategické úrovni a i proto je využíván skupinami lidí vně IT, jakými jsou vedení podniku, uživatelé IT a audit. ITIL neřeší všechny oblasti řízení IT, protože neobsahuje podpůrné procesy pro řízení lidských

[4] Mapováním procesů mezi ITIL a COBIT se podrobně zabývá publikace COBIT Mapping: Mapping of ITIL with COBIT 4.0 vydaná ITGI, která obsahuje mapování kontrolních cílů COBIT na příslušné procesy ITIL v2 [9]

zdrojů, majetku nebo projektů. COBIT oproti ITILu obsahuje propracovanější systém měření procesů ve vztahu k cílům a navíc i způsob zjišťování a měření vyspělosti procesů (maturity models). ITIL na druhé straně obsahuje velké množství nejlepších praktik sloužících k návrhu a řízení procesů (procesní schémata, vzory a šablony dokumentů apod.). Využití obou přístupů je dále dáno i velikostí organizace. Zatímco ITIL je použitelný v podnicích všech velikostí a typů, implementace procesů dle COBIT je doporučena velkým organizacím se složitou infrastrukturou. Vzhledem k tomu, že COBIT nevzešel z praxe, což je na jeho jazyku a srozumitelnosti znát, jeho implementace je oproti ITIL podstatně složitější. V malých organizacích by řízení dle COBIT přineslo pravděpodobně neúměrně vysoké náklady spojené s implementací, administrativou a provozem.

4.4.6 Další metodické přístupy

Vedle ITIL a COBIT existují další metodické přístupy k řízení IS/ICT, které řeší tuto problematiku jinými způsoby. Pro vývoj metody monitorování služeb IS/ICT nebyly použity z důvodu nesplnění kritérií pro užší výběr, které jsou popsány v úvodu kapitoly *4.4 Vybrané metodické přístupy k řízení IS/ICT a poskytování služeb*. Níže je uvedeno několik takovýchto přístupů pouze s odkazy do odborné literatury:

- EMF (Enhanced Management Framework) [15],
- eTOM (enhanced Telecom Operations Map) [16],
- Harris Kern’s Enterprise Computing Institute [20].

5 Metoda monitorování IS/ICT

Stěžejní kapitola disertační práce představuje definování metody pro zavádění monitorování.

5.1 Motivace pro tvorbu metody monitorování služeb IS/ICT

Řada pracovníků pracujících v provozu ICT, vlastníci služeb a vrcholové vedení si často kladou otázky související s dostupností a výkonností klíčových dílčích aplikací, systémů ale i komplexních procesů a celých služeb. Tyto otázky se zpravidla objevují, když se systémům nedaří včas zpracovávat požadavky od koncových uživatelů nebo jiných systémů. Dokáží tito lidé odpovědět na následující otázky:

- Jaké SLA hodnoty služba ve skutečném provozu splňuje?
- Jaká je aktuální výkonnost systému vyjádřená počtem obsloužených požadavků či transakcí za definovaný časový interval?
- Jak byl systém výkonný před týdnem, měsícem či za poslední rok?
- Jaká je aktuální dostupnost systému koncovým uživatelů či jiným systémům?
- Jaká je průměrná, minimální či maximální doba zpracování požadavků daného systému či služby?
- V jakých částech služby se nachází tzv. „úzké hrdlo“, které způsobuje problémy při zpracovávání požadavků a transakcí?
- V jakých částech dne je služba svými uživateli nejvíce využívána?
- Které typy služeb a přes které komunikační kanály si zákazníci nejvíce objednávali za poslední měsíc?

U jednoduchých aplikací či systémů zpravidla dokáže na tyto otázky jednorázově odpovědět příslušné IT oddělení, avšak jak získat tyto informace a mít je neustále k dispozici za komplexní systémy, procesy nebo celé služby? [23]. Tyto informace v ucelené podobě pak vytvářejí nástroj podporující rozhodování o klíčových otázkách na všech úrovních řízení IS/ICT. Z hlediska operativního řízení pomáhají identifikovat a řešit aktuální problémy v dostupnosti a výkonnosti služeb a aplikací na základě okamžitých informací. Statistické informace jako výstup monitorování charakterizují chování koncových uživatelů, např. v jakou dobu je služba nejvíce popř. nejméně využívána, a tím pomáhají s plánováním odstávek

technologií. Informace o využívání služeb koncovými zákazníky dále podporuje marketingové oddělení při plánování marketingových kampaní. Z hlediska taktického a strategického řízení pak slouží v delším časovém horizontu jako nástroj podpory rozhodování o změnách, rozvoji a plánování kapacit IS/ICT. Autor práce si je vědom, že na trhu ITOM existuje velká řada software podporující monitorování informačních technologií, avšak jejich nasazení a následné využití při monitorování služeb IS/ICT je zpravidla prováděno ad-hoc na základě zkušeností konzultačních firem a nikoliv dle předem definované obecné, otevřené a univerzální metody.

5.2 Cíl metody monitorování služeb IS/ICT

Hlavním cílem metody pro monitorování služeb IS/ICT je poskytnout obecný, univerzální a formalizovaný popis činností a postupů, které vedou k nasazení a provozu systému, který monitorování služeb IS/ICT zabezpečuje.

5.3 Postup tvorby metody monitorování služeb ICT

V této kapitole je popsán postup tvorby metody monitorování služeb podporovaných informačními technologiemi. Metoda je tvořena v několika následujících krocích:

1. na začátku je analýzou dostupných informačních zdrojů vybrán nejvhodnější metodický rámec, na jehož principech bude finální metoda založena,
2. ve druhém kroku jsou vybrány problémové oblasti z vybraného metodického rámce, které budou metodou hlouběji rozpracovány a doplněny,
3. v této fázi je vytvořena celková architektura metody a její hlavní principy. Budou definovány klíčové procesy a rozhodovací diagramy, kterými je řízeno nasazení monitorování technologií, služeb a procesů,
4. na závěr je metoda zakomponována do celkové koncepce vybraného metodického rámce definicí jejích výstupů na procesy metodického rámce.

5.4 Výběr metodického rámce

Výběr metodického rámce, který je proveden na základě studia vybraných rámců a jejich srovnání, je důležitým krokem, který ovlivní celkovou architekturu a použitelnost navrhované metody. Metodické rámce CMM a EUP jsou primárně orientované na vývoj a řízení informačního systému, a přestože se jedná o procesní

metodiky, tak v rámci předmětné oblasti nepokrývají veškeré procesy a oblasti pro řízení IS/ICT. V případě výběru jednoho z výše uvedených metodických rámců, by bylo potřeba definovat řadu nových pojmů a vazeb. Pro výběr metodického rámce je dále nezbytná orientace na koncept řízení a správy služeb IS/ICT, která je u těchto metodických rámců slabší.

Do užšího výběru byly tedy vybrány metodické rámce COBIT a ITIL. Tabulka 5-1 dle Matušky shrnuje kritéria použitelná pro porovnání obou dnes velmi hojně používaných přístupů k řízení a správě IS/ICT COBIT a ITIL. [31]

	COBIT	ITIL
Význam zkratky	Control Objectives for Information and Related Technology (Cíle řízení pro informační a související technologie)	Information Technology Infrastructure Library (Knihovna infrastruktury informačních technologií)
Vznik	90. léta, konzultační a auditorské společnosti	80. léta, vládní organizace CCTA ve Velké Británii
Označován jako	Soubor cílů a postupů pro řízení IT	Procesně orientovaný rámec osvědčených postupů, které pomáhají definovat procesy řízení služeb IT (ITSM)
Zaměření více na	Celkové řízení a hodnocení IT	Definici ICT procesů a procesů, praktické postupy
Zastřešující organizace	ISACA (Information System Audit and Control Association) ITGI (IT Governance Institute)	OGC (Office of Government Commerce) ITSMF (IT Service Management Forum)
Primární zdroje informací v Internetu	http://www.isaca.org/cobit (ang.)	http://www.itil.org (ang.) http://www.itsmf.com (ang.) http://www.itil.cz (česky)
Nejvhodnější použití	Ve velkých organizacích se složitou infrastrukturou IS/ICT	V organizacích všech velikostí a typů
Cílové skupiny	Vrcholové vedení podniku, audit, uživatelé IT	Vedení ICT
Úroveň řízení	Strategické	Taktická a operativní
Procesní záběr	Všechny aktivity a procesy, které souvisí s podnikovým IS/ICT	Jen přímé aktivity a služby IS/ICT
Mapování na druhý přístup	Možné (procesy m:n)	Možné (procesy m:n)
Náročnost implementace	Obtížnější z důvodu malé srozumitelnosti Procesy je nutné vymýšlet	Snadnější, přímočará implementace Procesy jsou definovány, ale jejich implementaci je ponechána volnost
Členění problémové oblasti	4 oblasti (plánování, implementace, provoz & podpora, monitoring 34 cílů řízení (odpovídají přibližně informatickým procesům) 318 detailních cílů Vše popsáno v 6 publikacích	2 oblasti řízení (operativní a taktická) 6 operativních procesů 5 taktických procesů Vše popsáno v 8 publikacích
Charakter návrhu	Neproprietární, nezávislý, volně dostupný tzv. public domain	Neproprietární, nezávislý, volně dostupný tzv. public domain
Dostupnost literatury	Většina dokumentace je ke stažení na Internetu zdarma	Ve specializovaných obchodech s IT literaturou (cena základní sady cca 9000 Kč)
Hlavní výhody	Definuje společnou informační základnu pro IT, vedení podniku a auditory, která umožní efektivně řídit a hodnotit služby IT ve vztahu na hlavní podnikové cíle a činnosti	Vychází z praxe ověřených postupů Je použitelný i na nižších úrovních řízení IT Zavádí jednotnou terminologii
Hlavní nevýhody	Je vzdálenější rutinně informatiky v pouhých identifikacích, vymezeních cílu IT.	Nepostihuje všechny oblasti řízení IT (např. lidské zdroje, majetek, projektové řízení)

Tabulka 5-1 - Kritéria porovnávání COBIT a ITIL

Hlavní kritéria pro výběr jednoho z metodických rámců byla zvolena následovně:

- rozsah a komplexnost pokrytí problematiky řízení IS/ICT jednotlivými oblastmi metodického rámce,
- obsah a srozumitelnost konkrétních postupů a procesů řízení IS/ICT.

Hlavním cílem a posláním ITILu je definice procesů umožňujících efektivní řízení IS/ICT na jednotlivých úrovních řízení organizace včetně taktické a operativní, přičemž k realizaci těchto cílů jsou použity osvědčené a konkrétní postupy z praxe (tzv. best practices), a tím je tento metodický rámec více přiblížen jednotlivým činnostem a postupům z oblasti řízení IS/ICT. Na rozdíl od ITILu COBIT na problematiku pohlíží spíše z úrovně strategického řízení podniku spojováním business cílů s cíly IT, a proto má ke konkrétním provozním činnostem dále. Jeden z rozhodujících faktorů je dále srozumitelnost metodiky. Po prostudování obou metodických rámců se jeví ITIL jako jasněji definovaný a pro potřeby řízení IS/ICT srozumitelnější než COBIT. Z výše uvedeného textu vyplývá, že pro potřeby tvorby metody monitorování je vhodnější použít metodický rámec ITIL než COBIT.

ITIL je vhodný rámec pro řízení služeb IS/ICT, avšak v jednotlivých procesech a oblastech abstrahuje od vyšší úrovně detailu, což je logické, protože jeho autoři se jej snažili vyvinout tak, aby byl dostatečně obecný a tím i všeobecně použitelný. V několika oblastech metodického rámce ITIL je monitoring klíčovou komponentou pro další navazující procesy tzn., že jeho výstupy slouží jako vstupy do dalších procesů. V metodickém rámci však není kvůli jeho obecnosti navržen konkrétní popis procesu monitorování. Nově vzniklá metoda monitorování služeb IS/ICT tak rozšíří a doplní stávající metodický rámec o procesy, postupy a šablony sloužící k efektivnímu nasazení monitorování aplikací, procesů, systémů a služeb.

5.5 Výběr oblastí metodického rámce

Metoda monitorování rozšiřuje procesy metodického rámce. V rámci definice metody je nezbytné identifikovat procesy tj. části metodického rámce, jejichž se metoda monitorování dotýká a vytváří s nimi vazby. Po prostudování rámce ITIL lze konstatovat, že budoucí metoda monitorování vytváří vztahy se všemi oblastmi a procesy ITIL. V některých případech výstupy metody tvoří vstupy do některých procesů ITIL, u ostatních naopak metoda potřebuje klíčové výstupy některých procesů ITIL. Nejvíce je metoda provázána s následujícími procesy metodického

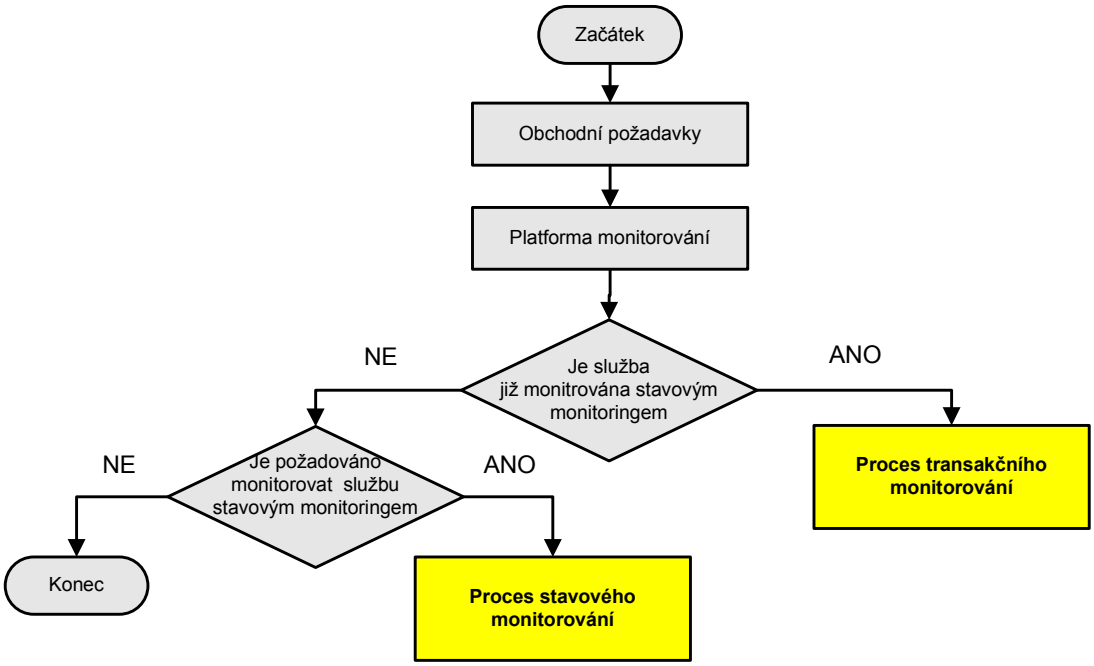
rámce ITIL: Service Level Management, Capacity Management, Incident Management, Problem Management, Change Management.

5.6 Návrh architektury metody

Návrh architektury metody vychází z vybraného metodického rámce, který je proveden v kapitole *5.4 Výběr metodického rámce*. Metoda je orientována procesně tak, aby splnila charakteristiky metodického rámce ITIL, který byl pro tyto účely vybrán. Metoda doplňuje knihy ITIL, které slouží jako informační základna pro definici procesů pro řízení služeb IS/ICT, o postupy a procesy z oblasti monitorování služeb IS/ICT.

5.6.1 Základní principy metody monitorování

Metoda monitorování služeb IS/ICT vychází z definice procesu obsahujícího jednotlivé aktivity nutné pro zavedení monitorování služeb IS/ICT. Jako nástroj pro vizuální znázornění procesu je použit vývojový diagram. Obr. 5-1 znázorňuje hlavní proces, jehož části jsou dekomponovány na dva dílčí procesy: proces stavového monitorování a proces transakčního monitorování dle typu business požadavku.



Obr. 5-1 - Hlavní proces metody monitorování služeb IS/ICT

5.6.2 Základní prvky procesu

Pro každou aktivitu jsou v rámci metody definovány následující prvky:

- vstupy,
- výstupy,
- nástroje, techniky,
- uživatelské role:
    - vlastník služby - osoba odpovědná za danou službu v rámci podniku,
    - administrátor služby - osoba technicky odpovědná za provoz služby, která je předmětem monitorování,
    - servisní manažer služby - osoba na řídící pozici zodpovědná za technický provoz služby,
    - operátor monitorování - osoba odpovědná za provoz monitorování,
    - analytik systémových a business procesů - osoba technicky zodpovědná za aplikace a systémy (nejčastěji middleware) integrující zúčastněné heterogenní sub-systémy,
    - konzultant pro monitoring - interní či externí osoba pracující na nasazení monitorování,
- odpovědnosti - úkoly přiřazené jednotlivým odpovědným osobám.

Výstupům aktivit jsou v metodě definovány šablony potřebných dokumentů.

5.6.3 Hlavní proces

Hlavní proces zavedení monitorování služeb IS/ICT popisuje aktivity, které souvisejí s nasazením platformy monitorování. Po nasazení této platformy jsou zařazovány jednotlivé služby a technologie do monitorování.

5.6.3.1 Business požadavky

Specifikace business požadavků je důležitou vstupní částí celého procesu. Detailně a korektně specifikované požadavky na nasazení softwarové platformy pro monitorování informačních technologií a služeb jsou předpokladem pro nasazení takové platformy, která odpovídá potřebám organizace.

Vstupy:

- strategie a cíle podniku.

Nástroje, techniky:

- analýza požadavků,

- specifikace cílů platformy monitorování,
- interview s dodavateli, work-shopy apod.

Role :

- vrcholové vedení,
- IT vedení podniku,
- operátor monitorování.

Odpovědnosti:

- vrcholové vedení podniku - předkládá obchodní podnikové cíle a celkovou strategii podniku,
- IT vedení podniku - mapuje strategické cíle podniku na cíle řízení služeb IS/ICT, ze kterých vyplývají dílčí cíle platformy monitorování,
- operátor monitorování - odpovědnost za koordinaci konzultací při specifikaci cílů a analýze požadavků.

5.6.3.2 Platforma monitorování

Výběr a implementace platformy pro monitorování služeb IS/ICT je klíčovou aktivitou v rámci celého procesu, která ovlivňuje výslednou podobu a funkčnost monitorování. Prostředkem ke splnění cíle výběru a implementace platformy monitorování je definice klíčových charakteristik platforem, které umožňují jejich komplexnější popis. Tyto charakteristiky lze rozdělit na obecné a specifické. Zatímco obecné charakteristiky jsou společné pro hodnocení všech platforem monitorování, specifické charakteristiky jsou hodnoceny pouze pro konkrétní typ platformy (např. platforma pro stavové monitorování, platforma pro monitorování výkonnosti, platforma pro transakční monitorování apod.). Dále jsou charakteristiky děleny na charakteristiky dodavatele a charakteristiky platformy. Přiřazením hodnot jednotlivým charakteristikám lze dosáhnout částečně objektivního hodnocení, které je však vždy vhodné doplnit subjektivním hodnocením a zvážením nasazení v konkrétním podnikovém prostředí. Tato aktivita si tedy neklade za cíl popsat nejvhodnější řešení pro všechny podmínky implementace, avšak poskytnout postup a sadu charakteristik, které je vhodné při výběru platformy zohlednit. Výběr a nasazení platformy musí být v souladu se specifikovanými business požadavky, které vycházejí z celkové strategie podniku.

Obecné charakteristiky dodavatele:

- velikost a spolehlivost dodavatele - cílem je zhodnotit, zda tady dodavatel bude s touto platformou i za několik let tak, aby byla platforma podporována a nedošlo ke koupi nestabilního a nestálého produktu. Mezi základní parametry této charakteristiky patří např.:
    - obrat dodavatele,
    - počet poboček,
    - celkový počet zákazníků,
- zaměření dodavatele v oboru ITSM - tato charakteristika napovídá o povaze a určení platformy. Dodavatelé jsou členěni podle typů oblastí ITSM řešených svými produkty tak, jak je popsáno v kapitole *4.2 Hlavní oblasti řízení provozu ICT*:
    - event & correlation management,
    - availability & performance management,
    - network management,
    - DBMS management,
    - SIEM (Security Information & Event Management),
    - E2E management,
- historie produktu a verze - popis historie a verzí produktu napovídá o vyspělosti dodavatele; pro tuto charakteristiku je potřeba zjistit následující informace:
    - seznam dosavadních verzí a jejich systém číslování vypovídající o skutečném počtu nově vydaných verzí,
- světová pozice dodavatele a jeho produktů - determinuje kvalitu platformy a podporu třetích stran. Tyto informace lze získat například zhodnocením významných konzultačních společností.

Obecné charakteristiky platformy:

- pozice platformy v celkové produktové mapě dodavatele - napovídá o zaměření produktu:
    - jaké jsou produkty dodavatele a jaký je přisuzován význam platformě; zda se jedná o dílčí monitorovací nástroj nebo zda se jedná o „umbrella“ řešení integrující více produktů z oblasti ITSM,

- ostatní produktové portfolio související s platformou - monitorovací platforma se podle typu řešení zpravidla skládá z více produktů nebo modulů, jakými jsou např. modul pro IT service management, modul korelační analýzy, modul root cause analýzy apod. Hlavním cílem této charakteristiky je zachytit celkové možnosti celé platformy:
    - seznamem produktů popř. modulů nabízených dodavatelem řešení v rámci platformy monitorování,
- základní schéma platformy - popisuje způsob fungování infrastruktury platformy monitorování a předurčuje některé její vlastnosti, které jsou dány celkovou její koncepcí,
- podporovaná grafická uživatelská rozhraní - popisují způsoby připojení uživatelů a práce s platformou:
    - tenký klient, tlustý klient apod.,
- možnosti a podpora databázových produktů - určuje, zda je možné platformu použít s různými druhy databázových software:
    - typy a verze podporovaných databází,
- možnosti a podpora operačních systémů - určuje zda je možné platformu použít s různými druhy operačních systémů:
    - typy a verze podporovaných operačních systémů,
- standardy a otevřenost - jedná se o velmi zásadní charakteristiku, která je často sledována při výběru dnes prakticky všech softwarových produktů; mezi hlavní sledované parametry v případě platforem pro monitorování patří:
    - protokolové standardy používané pro správu a řízení sítí a dalších prvků IS/ICT na úrovni TCP/IP: SNMP, syslog atd.,
    - standardní zprávy pro přenos monitorovacích informací: SNMP trapy,
    - standardy ukládání informací o monitorovaných zařízeních: MIB;
- cenová charakteristika - v rámci této charakteristiky je popsána cenová politika, cenová hladina a způsob licencování produktu.

Specifické charakteristiky platformy pro stavové monitorování:

- výkonnost a škálovatelnost:
    - podpora víceprocesorového popř. víceserverového prostředí,
    - možnosti nasazení failoveru,
    - výkonnost z hlediska rychlosti zpracování událostí,

    - maximální počty zpracovávaných událostí z infrastruktury IS/ICT,
- integrace - možnost zpracování událostí ze širokého spektra technologií a ostatních specifických produktů na řízení IS/ICT,
- korelace a deduplikace - podpora korelace určuje možnosti analýzy informací nad platformou monitorování (nad alarmy z infrastruktury doručenými do platformy); deduplikace umožňuje identifikovat alarmy ze stejné části infrastruktury IS/ICT, které jsou při výpadku či vzniku problému periodicky doručovány do platformy, a pak je následně uložit do databáze pouze v podobě jednoho záznamu, přičemž každý další výskyt stejného alarmu je deduplikován s původním záznamem (tím dochází k velké úspoře místa v databázi monitorovací platformy),
- podpora procesů významných metodických rámců - některé produkty z oblasti monitoringu IS/ICT jsou navrženy s podporou procesů některých metodických rámců řízení informačních technologií, jakým je např. ITIL,
- bezpečnostní standardy:
    - šifrování (až v SNMP v3),
    - ověření a autorizace uživatelů,
    - správa uživatelských profilů.

Specifické charakteristiky platformy pro monitorování výkonnosti:

- výkonnost a škálovatelnost:
    - podpora víceprocesorového popř. víceserverového prostředí,
    - možnosti nasazení failoveru,
    - výkonnost z hlediska počtu možných dotazů (tzv. polling) na monitorovaná zařízení za specifikovaný časový interval,
- otevřenost, standardy a interoperabilita:
    - možnosti zpracování nashromážděných monitorovacích dat jinou cestou než dotazováním na koncová zařízení (importem do platformy),
    - možnosti integrace se dalšími systémy EMS a OSS (event management, provisioning, service management apod.),
    - použití standardních SŘBD,
- úroveň analýzy dat v reálném čase:

- některé produkty umožňují analyzovat a prezentovat data již v rámci jejich sběru (před dalšími agregacemi),
- jiné zase umožňují dále porovnávat aktuální data (real-time) s historickými daty za účelem odhalení podmínek nestandardního chování systémů IS/ICT,

Kromě výše uvedených charakteristik je vhodné zhodnotit produkt i slovním popisem, kterým lze upozornit na jeho silné a slabé stránky, vhodnost použití pro konkrétní implementaci (popř. vymezit oblasti použití) a odhad budoucího vývoje. Z výše uvedeného textu vyplývá, že výběr a implementace platformy pro monitorování služeb je třeba provést na základě následujících informací:

- specifikované business požadavky,
- vyplněné charakteristiky s definovanými vahami,
- slovní subjektivní hodnocení s ohledem na konkrétní podmínky podniku.

Vstupy:

- specifikované business požadavky.

Nástroje, techniky:

- definice charakteristik platforem,
- definování vah kritérií a přiřazení hodnot,
- slovní popis platformy.

Role :

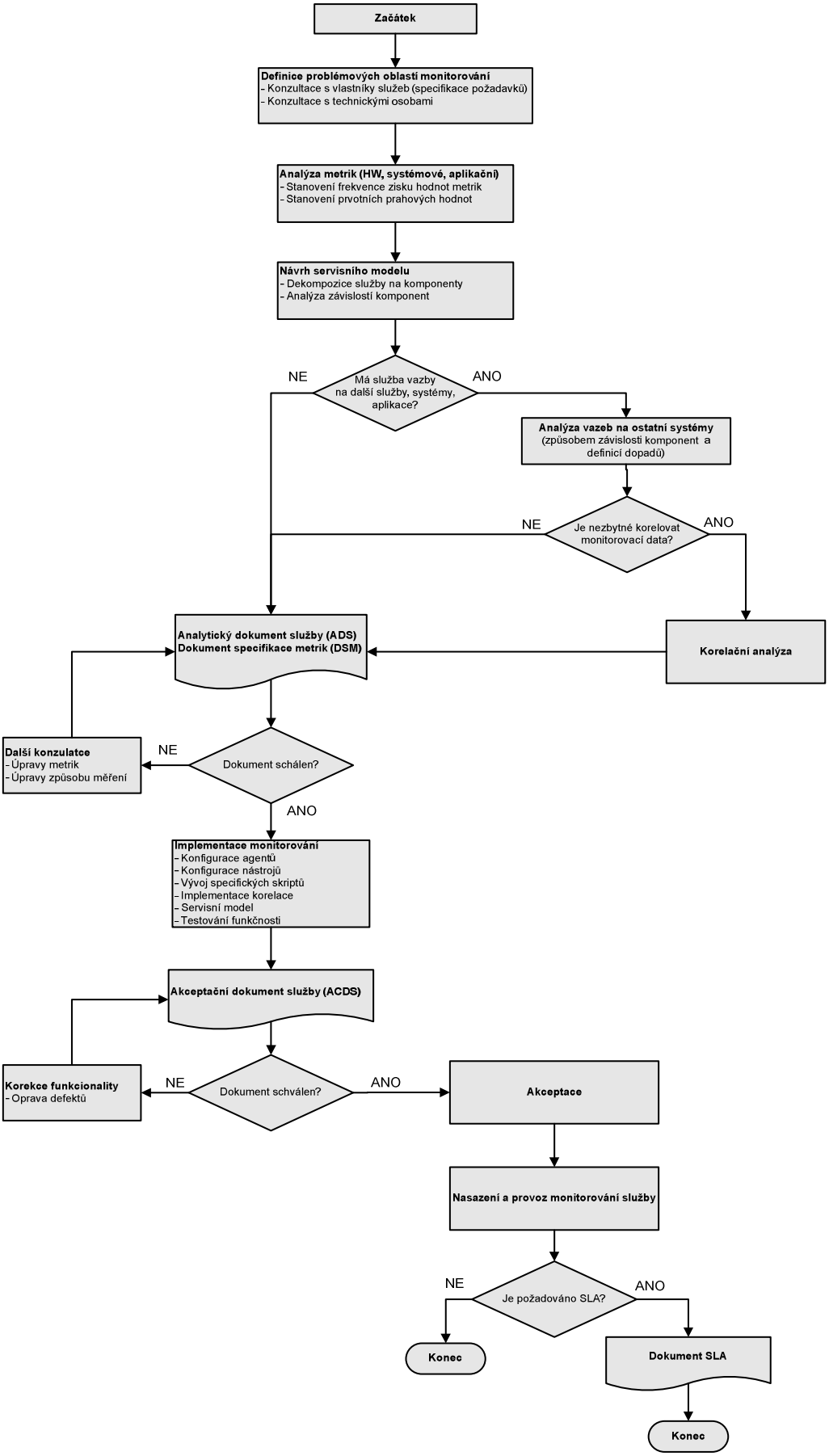
- operátor monitorování,
- IT vedení podniku.

Odpovědnosti:

- IT vedení podniku - finální rozhodnutí o výběru,
- operátor monitorování - informační podpora při výběru řešení a specifikace požadavků na zavedení.

5.6.4 Proces stavového monitorování

Obr. 5-2 představuje vývojový diagram sloužící k definování navrhovaného procesu nasazení stavového monitorování služeb IS/ICT. Následující podkapitoly pak popisují a definují jednotlivé části (aktivity, dokumenty, rozhodovací prvky) daného procesu.



Obr. 5-2 - Dekompozice procesu stavového monitorování

5.6.4.1 Definice problémových oblastí

Aktivita slouží k získání základních informací o službě, definování problémových oblastí služby a zjištění specifikace požadavků na monitorování. Tyto informace jsou doporučeny získat na základě informačních schůzek s vlastníky a administrátory služeb.

Vstupy:

- spuštění mechanismu (nasazení nové služby zákazníkům, změna ve službě apod.).

Nástroje, techniky:

- konzultace s vlastníky a administrátory služby.

Role :

- vlastník služby,
- administrátor služby,
- konzultant pro monitoring.

Odpovědnosti:

- vlastník služby - poskytnout základní informace o službě (typ, počet uživatelů, perspektivita do budoucna apod.),
- administrátor služby - poskytnout technické informace o problémových oblastech (HW, OS, aplikace),
- konzultant pro monitoring - získat a analyzovat dostupné informace.

Výstupy:

- seznam problémových oblastí,
- popis služby,
- technické složení služby.

5.6.4.2 Analýza metrik

Hlavním cílem této aktivity je definovat seznam metrik, které jsou předmětem monitorování, popsat technický návrh jejich implementace a navrhnout model služby. Metriky jsou dle modelu stavového monitorování rozděleny na následující typy.

- hardwarové - monitorování hardwarových komponent služby,
- systémové - metriky operačního systému,
- aplikační (databázové, generické a specifické).

Každé metrice je přidělen unikátní identifikátor, severita a vliv na komponentu modelu. Dalším krokem této aktivity je definice intervalu zjišťování hodnot definovaných metrik.

Vstupy:

- seznam problémových oblastí.

Nástroje, techniky:

- konzultace s administrátory služeb.

Role :

- administrátor služby,
- konzultant pro monitoring.

Odpovědnosti:

- administrátor služby - poskytnout technické informace o službě,
- konzultant pro monitoring - konzultovat s ostatními odpovědnými osobami, analyzovat získané informace a připravit analytický dokument a dokument specifikace metrik.

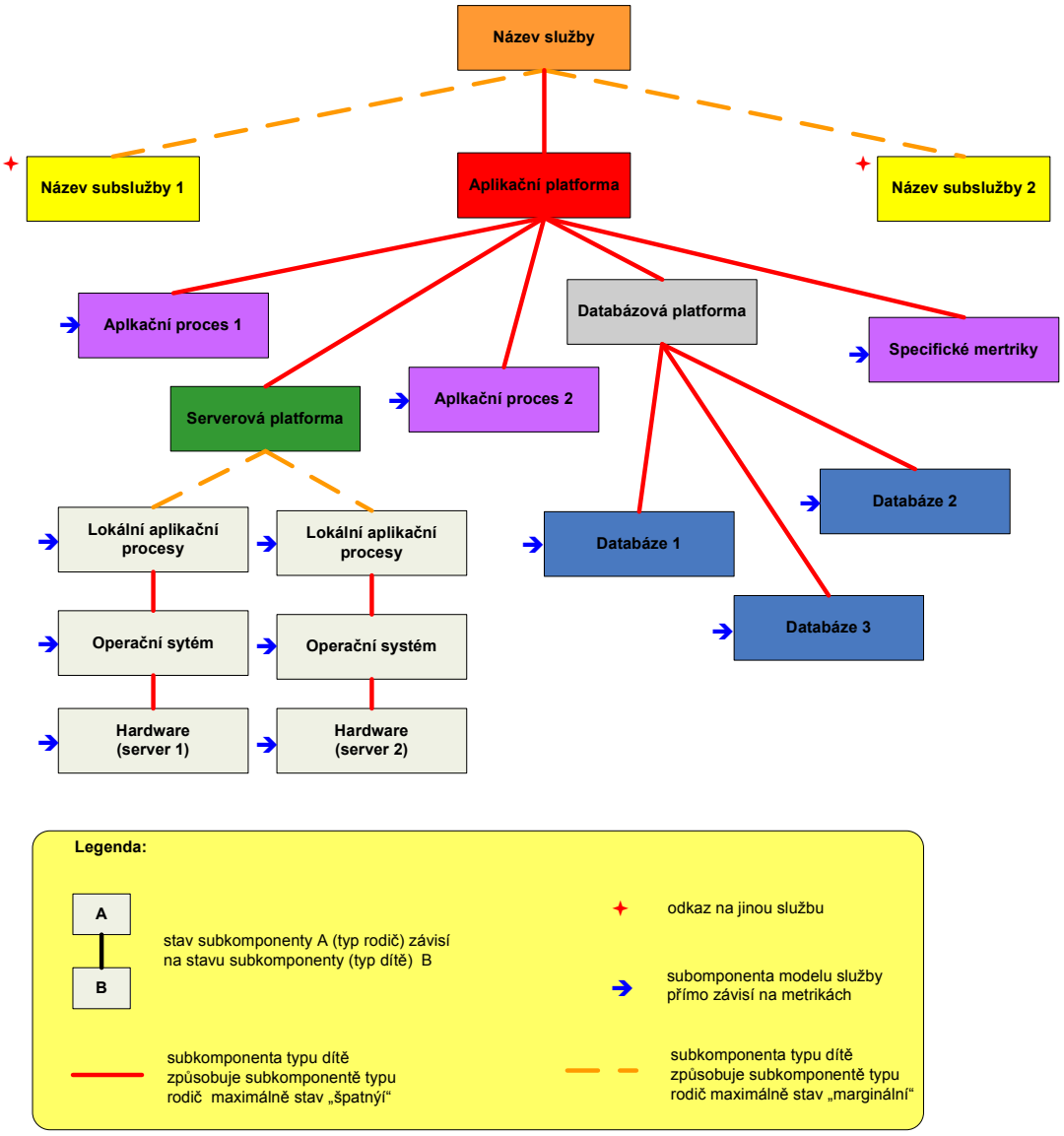
Výstupy:

- Analytický dokument služby,
- Dokument specifikace metrik.

5.6.4.3 Návrh servisního modelu

Servisní model představuje grafické znázornění služby rozdělené na jednotlivé komponenty dle modelu monitorování. Takové rozdělení umožňuje přiřazovat definované sady metrik k jednotlivým komponentám a tím v provozu monitorování určovat, která část služby je nefunkční, popř. má omezenou funkcionalitu. Mezi jednotlivými komponentami dané služby jsou definovány v rámci stavového monitorování vztahy. Vztahem mezi komponentami služby se rozumí fakt, že funkčnost jedné komponenty služby závisí na funkčnosti jedné nebo více jiných komponent. Tyto vazby pak vytvářejí vztahy rodič - dítě tak, že komponenta rodič přímo závisí na komponentě dítě, přičemž platí, že jedna komponenta může mít více rodičů. Vazby jsou dále řízeny pravidly závislostí, která na základě stavu komponenty dítě, definuje stav komponenty rodič. Následující stavy komponent služby jsou doporučeny zavést: dobrý, marginální a špatný. Komponenta služby, která je v dobrém stavu poskytuje plně svoji funkcionalitu tak, jako za běžného standardního provozu. Komponenta, která je v marginálním stavu

poskytuje omezenou funkcionalitu. Komponenta ve špatném stavu vůbec neposkytuje očekávanou funkcionalitu. Ukázka typického servisního modelu služby je na Obr. 5-3.



Obr. 5-3 - Servisní model služby (servis tree)

Vstupy:

- seznam metrik.

Nástroje, techniky:

- dekompozice služby na jednotlivé komponenty,
- vytvoření vazeb.

Role:

- administrátor služby,
- konzultant pro monitoring.

Odpovědnosti:

- administrátor služby - poskytne technické informace o vazbách na ostatní systémy,
- konzultant pro monitoring - na základě konzultací s administrátorem služby navrhnout a popsat servisní model.

Výstupy:

- servisní model.

5.6.4.4 Analýza vazeb na ostatní systémy

Tato aktivita je v procesu relevantní za předpokladu, že služba nebo některá její komponenta, má vazby na ostatní aplikace, systémy nebo další služby. Vazbou je v oblasti stavového monitorování chápán fakt, že funkčnost služby nebo její části závisí na komponentách jiné služby (popř. systému či aplikace). Naopak funkčnost služby, která je předmětem stavového monitorování může ovlivňovat funkcionality jiných aplikací, systémů nebo celých služeb. Vazby mezi službami vycházejí z analogie vazeb mezi jednotlivými komponentami, což nabízí převzít termíny rodič (pro službu, která závisí na jiné službě) a dítě (služba, která determinuje stav jiné služby). V rámci aktivity jsou definovány následující typy vazeb: marginální a špatná. Je-li mezi dvěma službami typu rodič a dítě definována marginální vazba, znamená to, že služba rodič nabude maximálně marginálního stavu na základě marginálního nebo špatného stavu služby dítě. Je-li mezi dvěma službami typu rodič a dítě definována vazba typu špatná, znamená to, že služba rodič nabude maximálně špatného stavu na základě špatného stavu služby dítě.

Vstupy:

- vyplněný dotazník služby,

Nástroje, techniky:

- maticový zápis závislostí:
    - typy vztahu: rodič - dítě (služba rodič závisí na službě dítě),
    - typy vazeb: marginální, špatný,
- konzultace s administrátory všech relevantních služeb.

Role:

- administrátor služby,
- konzultant pro monitoring,

Odpovědnosti:

- administrátor služby - poskytne technické informace o vazbách na ostatní systémy,
- konzultant pro monitoring - konzultovat s administrátory, vytvořit matici závislostí služeb a promítnout ji do servisního modelu.

Výstupy:

- navržená matice závislostí služeb,
- doplněný servisní model.

5.6.4.5 Korelační analýza

Za předpokladu, že je potřeba korelovat naměřené hodnoty definovaných metrik s jinými monitorovacími informacemi, slouží tato aktivita k návrhu takovéto korelace.

Vstupy:

- seznam metrik,
- servisní model.

Nástroje, techniky:

- servisní model.

Role:

- administrátor služby,
- konzultant pro monitoring.

Odpovědnosti:

- konzultant pro monitoring - navrhnout jaké výstupy monitorování a jakým způsobem budou korelovány,

Výstupy:

- analýza a návrh korelace.

5.6.4.6 Analytický dokument služby a dokument specifikace metrik

Analytický dokument služby je spolu s Dokumentem specifikace metrik základním dokumentem, který musí být schválen vlastníkem služby i administrátorem před tím, že může být monitorování služby implementováno. Analytický dokument služby obsahuje následující části:

- funkční analýza monitorování služby v jednotlivých vrstvách dle modelu monitorování,

- technický návrh realizace,
- popis akceptačních testů.

Ukázka šablony dokumentu je v příloze C.

Dokument specifikace metrik obsahuje seznam definovaných metrik s jednotlivými následujícími parametry:

- definice metriky,
- kategorie metriky,
- severita,
- služba,
- identifikátor metriky,
- interval zjišťování hodnot metriky,
- prahové hodnoty,
- způsob implementace.

Ukázka šablony dokumentu je v příloze D.

5.6.4.7 Další konzultace

Za předpokladu, že alespoň jeden z dokumentů nebyl schválen, je třeba učinit opravné kroky tak, aby se všechny zúčastněné strany dohodly na kompromisu o definici metrik a způsobu jejich implementace. Tato aktivita se může opakovat až do stavu schválení dokumentů.

Vstupy:

- připomínkovaný Analytický dokument služby,
- připomínkovaný Dokument specifikace metrik.

Nástroje, techniky:

- další konzultace s administrátory popř. vlastníky služeb.

Role :

- konzultant pro monitoring.

Odpovědnosti:

- konzultant pro monitoring - připravit na základě konzultací s administrátory popř. vlastníky služeb novou verzi dokumentů obsahující seznam definovaných metrik a způsoby získávání jejich hodnot.

Výstupy:

- nová verze Analytického dokumentu služby popř. Dokumentu specifikace metrik připravená ke schválení.

5.6.4.8 Implementace monitorování

Cílem této aktivity je implementačně zabezpečit monitorování tak, jak je popsané v dokumentech. Implementace monitorování je rozdělena na dvě základní části: implementaci definovaných metrik a implementaci servisního modelu. Implementace metrik probíhá v následujících dílčích fázích:

- implementace generických metrik - jedná se o soustavu metrik, jejichž implementace je použitelná ve více službách; implementace těchto metrik vychází z předem definovaných šablon; generické metriky lze rozdělit na následující skupiny:
    - metriky hardware,
    - metriky operačního systému,
    - metriky databázové,
    - metriky aplikační generické,
- implementace specifických metrik - jedná se o metriky, které jsou specifické pro danou službu, tyto metriky zpravidla vyžadují vyšší pracnost implementace,
    - metriky aplikační specifické.

Součástí implementace metrik je nastavení prahových hodnot metrik, při jejichž překročení dojde ke generování událostí, které jsou doručeny do platformy monitorování. V rámci implementace metrik je provedena korelace za předpokladu, že se během analýzy ukázalo, že je korelace nezbytná. Jsou definovány dva základní typy korelací:

- korelace na úrovni metrik - tato korelace je prováděna ještě předtím, než jsou monitorovací informace v podobě událostí odeslány do platformy monitorování,
- korelace na úrovni událostí - tato korelace je prováděna poté, co jsou informace odeslány do platformy monitorování (na úrovni generovaných událostí).

Jakmile jsou implementovány všechny požadované metriky, je možné přistoupit k vytvoření modelu služby. Model služby je vytvořen v nástroji pro modelování služeb dle návrhu modelu v Analytickém dokumentu služby. Jednotlivé komponenty se dostávají do jednoho z definovaných stavů (dobrý, marginální, špatný) na základě:

- metrik - metriky ovlivňují stav komponent,
- vazeb - závislost komponenty typu rodič na komponentě typu dítě,

- metrik i vazeb.

Vstupy:

- schválený Analytický dokument služby,
- schválený Dokument specifikace metrik.

Nástroje, techniky:

- konfigurace nástrojů monitorování (agenti, SNMP dotazování, prahové hodnoty),
- vývoj specializovaných monitorovacích skriptů pro specifické metriky,
- implementace modelu služby.

Role:

- konzultant pro monitoring.

Odpovědnosti:

- konzultant pro monitoring - implementovat a otestovat monitorování dle specifikace v analytickém dokumentu služby.

Výstupy:

- funkční a otestované monitorování,
- funkční a otestovaný model služby.

5.6.4.9 Korekce funkcionality

Za předpokladu, že nebyl schválen Akceptační dokument služby, je třeba učinit opravné kroky tak, aby byly odstraněny zjištěné defekty a datové nekonzistence v monitorování. Tato aktivita se může opakovat až do stavu schválení akceptačního dokument.

Vstupy:

- připomínkovaný Akceptační dokument služby,
- monitorování se zjištěnými defekty nebo jinými funkcionalitami, než jsou specifikované v Analytickém dokumentu služby a Dokumentu specifikace metrik.

Nástroje, techniky:

- analýza defektů, zjištění příčiny defektů, testování upravené funkcionality.

Role:

- konzultant pro monitoring.

Odpovědnosti:

- konzultant pro monitoring - upravit monitorování tak, aby byly splněny požadavky a specifikace na monitorování.

Výstupy:

- funkční a bezvadný monitoring služby.

5.6.4.10 Akceptace

Cílem této aktivity je demonstrovat splnění požadavků na implementaci monitorování specifikovaných v Akceptačním dokumentu služby.

Vstupy:

- specifikace akceptačních testů.

Role:

- konzultant pro monitoring,
- servisní manažer služby.

Odpovědnosti:

- konzultant pro monitoring - spustit monitorování v testovacím prostředí a demonstrovat funkčnosti,
- servisní manažer služby - zkontrolovat funkcionalitu monitorování a schválit či zamítnout akceptaci.

Výstupy:

- funkční monitorování v testovacím prostředí,
- podepsaný akceptační dokument služby oběma stranami,
    - akceptační dokument služby specifikuje seznam akceptačních testů, které jsou předmětem akceptace monitorování služby. Schválením dokumentu přechází monitorování dané služby do produkčního provozu.

5.6.4.11 Provoz monitorování

Cílem této aktivity je nasadit monitorování do produkčního provozu tak, aby bylo možné definovat a měřit hodnoty v rámci SLA. V rámci této aktivity dochází na základě konzultací a výsledků monitorování v produkčním provozu k úpravám prahových hodnot za účelem tvorby notifikací při jejich překročení. Dále jsou pak řízeny veškeré změnové požadavky na monitoring v souladu s procesy Change

Management metodického rámce ITIL. Výstupy z monitorování ve formě reportů dostupnosti služby slouží jako vstup do procesu definování a měření SLA.

Vstupy:

- akceptované monitorování služby potvrzené akceptačním protokolem.

Nástroje, techniky:

- analýza hodnot výstupů monitorování pro podporu tvorby SLA.

Role:

- konzultant pro monitoring,
- servisní manažer služby,
- operátor monitorování.

Odpovědnosti:

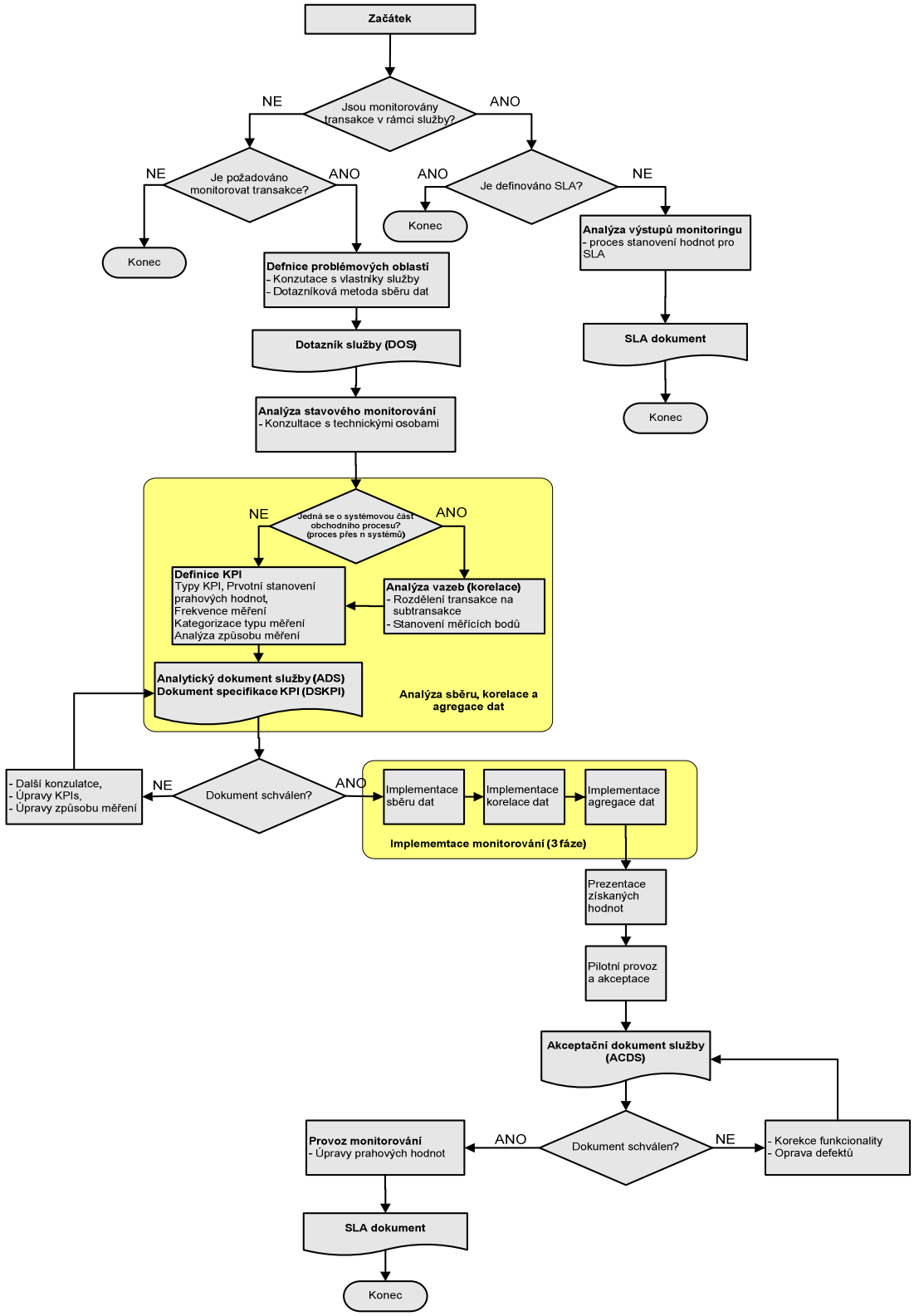
- konzultant pro monitoring - spustit monitorování v produkčním provozu,
- servisní manažer služby - konzultovat finální nastavení prahových hodnot,
- operátor monitorování - převzít monitorování služby do produkčního provozu.

Výstupy:

- funkční monitorování v produkčním provozu,
- reportování výpadků a defektů služby,
- měření SLA.

5.6.5 Proces transakčního monitorování

Obr. 5-4 předkládá v rámci metody monitorování schéma vývojového diagramu implementace navrhovaného procesu, který slouží k nasazení transakčního monitorování služeb IS/ICT. Následující podkapitoly popisují a definují jednotlivé části (aktivity, dokumenty, rozhodovací prvky) daného procesu.



Obr. 5-4 - Dekompozice procesu transakčního monitorování

5.6.5.1 Definice problémových oblastí

Tato aktivita slouží k získání základních informací o službě, k definování problémových oblastí služby a k vytvoření návrhu seznamu KPI. Tyto informace jsou doporučeny získat na základě informačních schůzek s vlastníky a administrátory služeb. Jako nástroj k získání potřebných informací o službě a jejich problémových oblastí je navržena a doporučena dotazníková metoda. Ze zkušenosti je doporučeno doplnit konzultační schůzky vyplněním dotazníku služby.

Vstupy:

- šablona dotazníku služby.

Nástroje, techniky:

- konzultace s vlastníky služeb,
- dotazníková metoda sběru podkladových informací.

Role :

- vlastník služby,
- administrátor služby,
- konzultant pro monitoring.

Odpovědnosti:

- vlastník služby - odpovědný za vyplnění první části dotazníku týkající se business požadavků a předběžné specifikace KPI,
- administrátor služby - odpovědný za vyplnění druhé části dotazníku týkající se technických detailů služby a způsobu získání hodnot KPI,
- konzultant pro monitoring - odpovědný za konzultace, ve kterých je vysvětlen záměr a obsah dotazníku, dále odpovědný za sběr a konsolidaci podkladových informací z dotazníkové metody.

Výstupy:

- dotazník s vyplněnými informacemi o službě.

5.6.5.2 Dotazník služby

Dotazník služby je dokument, který je součástí procesu Transakčního monitorování sloužící aktivitě *Definice problémových oblastí* ke strukturovanému zápisu získaných informací o službě. Dotazník služby je rozdělen na dvě základní části: *Business požadavky* a *Technické detaily služby*. Část *Business požadavky* vyplňuje business vlastník monitorované služby a obsahuje základní informace o službě, jakými jsou např.: název služby, funkcionality služby, počet a typy

uživatelů služby, finanční dopady na podnik v případě nedostupnosti služby apod. Důležitou součástí první části dotazníku je předběžný seznam KPI, které mají být monitorovány. Druhá část dotazníku *Technické detaily služby* je určena administrátorovi služby. V této části jsou podrobněji popsány technické detaily o službě, způsoby a návrhy, jakými lze získávat hodnoty KPI, které byly specifikovány vlastníkem služby. Ukázka šablony dotazníku služby je v příloze E.

Následující podkapitoly popisují aktivity a dokumenty, které tvoří samotnou analýzu sběru monitorovacích dat, jejich korelaci a následnou agregaci.

5.6.5.3 Analýza vazeb

Tato aktivita je v procesu relevantní za předpokladu, že služba, která je předmětem transakčního monitorování, má datové a systémově procesní vazby na ostatní systémy, procesy či další služby. Předmětem monitorování se v takovém případě stává systémová část business procesum, respektive její transakce, které začínají v jednom systému či aplikaci, a jsou zpracovávány napříč dalšími systémy. Hlavním úkolem této aktivity je na základě konzultací zjistit na jaké subtransakce se celková transakce rozpadá, jaké jsou požadované měřící body a jakým způsobem získat informace v jaké části (subtransakci) se transakce právě nachází.

Vstupy:

- vyplněný dotazník služby.

Nástroje, techniky:

- konzultace s vlastníky služeb,
- konzultace s administrátory všech zúčastněných sub-služeb, subsystémů,
- analytické metody, dedukce, transakční modelování, dekompozice transakce na části.

Role :

- vlastník služby,
- administrátor služby,
- analytik systémových a business procesů,
- konzultant pro monitoring.

Odpovědnosti:

- vlastník služby - poskytnout informace obchodního charakteru o vazbách na ostatní systémy,

- administrátor služby - poskytne technické informace o vazbách na ostatní systémy (potřebné datové vstupy a výstupy pro monitorovanou službu),
- analytik systémových a business procesů - navrhne způsob doručení informací týkající se měřících bodů mimo monitorovanou službu do předzpracovávajícího systému,
- konzultant pro monitoring - konzultovat s ostatními odpovědnými osobami za účelem dosažení cíle zisku výstupů aktivity.

Výstupy:

- detailní transakční model (hierarchie transakcí, transakční strom),
- seznam a popis měřících bodů.

5.6.5.4 Definice KPI

Hlavním cílem této aktivity je definovat konečný seznam KPI, které jsou předmětem monitorování a popsat technický návrh získávání dat potřebných pro realizaci monitorování. Tato data jsou získávána z primárních transakčních systémů nebo zároveň z dílčích transakčních sub-systémů. V rámci aktivity jsou definovány kategorie typů měření pro jednotlivá KPI.

Kategorie typů měření jsou následující:

- aktivní monitorování - spočívá v simulaci chování koncového uživatele služby (metodou takové simulace je nejčastěji E2E test),
- pasivní monitorování - spočívá ve sběru, korelaci a agregaci dat týkajících se transakcí ve zdrojovém systému,
- monitorování procesů - spočívá v dekompozici transakce systémového procesu na dílčí části, stanovení měřících bodů a sběru, korelaci a agregaci dat týkajících se transakcí a sub-transakcí napříč všemi zúčastněnými systémy.

Pro každé KPI jsou definovány jednotky měření, jakými jsou např. sekundy [s], milisekundy [ms], procenta [%], počet [count] atd.

U každého KPI je dále definován datový zdroj, ze kterého jsou potřebná monitorovací data získávána. Dalším krokem této aktivity je definice intervalu, ve kterém budou prováděna měření. Tento interval musí respektovat četnost vzniku transakcí ve zdrojovém systému. Např. vznikají-li data ve zdrojovém systému 1x za 24 h dávkovým zpracováním, nemá význam stanovit interval měření menší než 24h. U aktivních měření platí pravidlo, že čím je interval menší, tím vzniká větší

reprezentativní vzorek testů. Po stanovení výše uvedeného je třeba zvážit i určitá omezení monitorování. Jedním takovým omezením může být např. doba potřebná k uskutečnění měření a získání výsledků, která musí být vždy menší než je interval měření tak, aby nedocházelo ke spuštění více konkurenčních měření v rámci stanovené časové periody.

Vstupy:

- vyplněný dotazník služby.

Nástroje, techniky:

- konzultace s administrátory služeb,
- analýza vzorku zdrojových dat.

Role :

- administrátor služby,
- analytik systémových a business procesů,
- konzultant pro monitoring.

Odpovědnosti:

- administrátor služby - poskytnout technické informace o způsobu sběru dat, popř. navrhnout, jak tato data poskytnout,
- konzultant pro monitoring - konzultovat s ostatními odpovědnými osobami, analyzovat získané informace a připravit analytický dokument a dokument specifikace metrik.

Výstupy:

- Analytický dokument služby,
- Dokument specifikace metrik.

5.6.5.5 Analytický dokument služby a dokument specifikace KPI

Analytický dokument služby je spolu s Dokumentem specifikace metrik základním analytickým dokumentem, který musí být schválen vlastníkem služby i administrátorem před tím, že může být monitorování služby implementováno. Analytický dokument služby osahuje následující části:

- funkční analýza,
- technický návrh realizace,
- popis akceptačních testů.

Ukázka šablony Analytického dokumentu služby je v příloze F.

Dokument specifikace KPI obsahuje seznam definovaných KPI s následujícími parametry:

- název,
- zkratka,
- počet,
- subtyp,
- datový zdroj,
- jednotky,
- typ (časové, počítací a poměrové),
- perioda měření,
- detailní popis.

Ukázka šablony Dokumentu specifikace KPI je v příloze G.

5.6.5.6 Další konzultace

Za předpokladu, že alespoň jeden z dokumentů nebyl schválen, je třeba učinit opravné kroky tak, aby se všechny zúčastněné strany dohodly na kompromisu o definici KPI a způsobu jejich měření. Tato aktivita se může opakovat až do stavu schválení dokumentů.

Vstupy:

- připomínkovaný Analytický dokument služby,
- připomínkovaný Dokument specifikace KPI.

Nástroje, techniky:

- další konzultace s administrátory služeb.

Role :

- konzultant pro monitoring.

Odpovědnosti:

- konzultant pro monitoring - připravit na základě konzultací s administrátory služeb novou verzi dokumentů obsahující korektní seznam KPI a způsoby jejich měření.

Výstupy:

- nová verze Analytického dokumentu služby popř. Dokumentu specifikace KPI připravená ke schválení.

Podkapitoly *5.6.5.7* až *5.6.5.9* popisují implementaci monitorování služby ve třech fázích.

5.6.5.7 Implementace sběru dat

Cílem této aktivity je implementačně zabezpečit fázi sběru dat tím, že získaná data jsou uložena do struktur „raw“ vrstvy předzpracovávajícího systému.

Vstupy:

- schválený Analytický dokument služby,
- schválený Dokument specifikace metrik.

Nástroje, techniky:

- datové modelování,
- definice a vývoj scénáře pro simulační (E2E) testy,
- vývoj funkcí sběru dat.

Role:

- konzultant pro monitoring.

Odpovědnosti:

- konzultant pro monitoring - implementovat a otestovat fázi sběru dat.

Výstupy:

- funkční a otestovaný program pro sběr dat (implementovaný scénář E2E testu, program pro zisk dat z back-end systému, program provádějící specifické testy).

5.6.5.8 Implementace korelace dat

Cílem této aktivity je implementačně zabezpečit fázi korelace dat tím, že získaná data jsou uložena do struktur korelačních vrstvy předzpracovávajícího systému.

Vstupy:

- schválený Analytický dokument služby,
- schválený Dokument specifikace metrik.

Nástroje, techniky:

- datové modelování,
- definice a vývoj funkcí pro datovou korelaci.

Role:

- konzultant pro monitoring.

Odpovědnosti:

- konzultant pro monitoring - implementovat a otestovat fázi datové korelace,
- analytik systémových a business procesů - implementovat zasílání potřebných dat pro monitorování do předzpracovávajícího systému.

Výstupy:

- funkční a otestovaný program pro datovou korelaci,
- korelovaná data.

5.6.5.9 Implementace agregace dat

Cílem této aktivity je implementačně zabezpečit fázi agregace dat tím, že získaná a popřípadě korelovaná data jsou uložena do struktur agregační vrstvy předzpracovávajícího systému.

Vstupy:

- schválený Analytický dokument služby,
- schválený Dokument specifikace metrik.

Nástroje, techniky:

- datové modelování,
- definice a vývoj funkcí pro datovou agregaci.

Role:

- konzultant pro monitoring.

Odpovědnosti:

- konzultant pro monitoring - implementovat a otestovat fázi datové agregace.

Výstupy:

- funkční a otestovaný program pro datovou agregaci,
- agregovaná data.

5.6.5.10 Implementace prezentace dat

Cílem této aktivity je implementačně zabezpečit fázi prezentace získaných, korelovaných a agregovaných monitorovacích dat tím, že jsou získaná data exportována do systému pro prezentaci dat, kde jsou následně prezentována v různých grafických formách.

Vstupy:

- získaná, korelovaná a agregovaná data,
- implementované programy pro sběr, korelaci a agregaci dat.

Nástroje, techniky:

- definice a vývoj funkcí pro datový export,
- definice a tvorba reportů pro datovou prezentaci.

Role:

- konzultant pro monitoring.

Odpovědnosti:

- konzultant pro monitoring - implementovat a otestovat fázi datového exportu, implementovat a otestovat příslušné reporty, které slouží k prezentaci naměřených výsledků, příprava služby na akceptaci.

Výstupy:

- exportovaná data,
- reporty.

Následující podkapitoly popisují aktivity spojené s poimplementační fází monitorování.

5.6.5.11 Pilotní provoz a akceptace

Cílem této aktivity je nasadit monitorování do pilotního provozu tak, aby byly získány vzorky finálních dat, na kterých je možné demonstrovat funkčnost monitorování. Dílčím cílem je nastavit prahové hodnoty monitorování.

Vstupy:

- implementace monitoringu (funkce, programy, scénáře apod.).

Role:

- konzultant pro monitoring,
- servisní manažer služby.

Odpovědnosti:

- konzultant pro monitoring - spustit monitorování v pilotním provozu a nastavit specifikované prahové hodnoty,
- servisní manažer služby - konzultovat nastavení prahových hodnot.

Výstupy:

- funkční monitorování v pilotním provozu,
- akceptační dokument služby - specifikuje seznam akceptačních testů, které jsou předmětem akceptace monitorování služby. Schválením dokumentu přechází monitorování dané služby do produkčního provozu.

5.6.5.12 Korekce funkcionality

Za předpokladu, že nebyl schválen Akceptační dokument služby, je třeba učinit opravné kroky tak, aby byly odstraněny zjištěné defekty a datové nekonzistence v monitorování. Tato aktivita se může opakovat až do stavu schválení akceptačního dokument. Doporučená doba pilotního provozu je na základě nejlepších praktik 14 dní.

Vstupy:

- připomínkovaný Akceptační dokument služby,
- monitorování se zjištěnými defekty nebo jinými funkcionalitami, než jsou specifikované v Analytickém dokumentu služby a Dokumentu specifikace KPI.

Nástroje, techniky:

- analýza defektů, zjištění příčiny defektů, testování upravené funkcionality.

Role:

- konzultant pro monitoring.

Odpovědnosti:

- konzultant pro monitoring - upravit monitorování tak, aby byly splněny požadavky a specifikace na monitorování.

Výstupy:

- funkční a bezvadný monitoring služby.

5.6.5.13 Provoz monitorování

Cílem této aktivity je nasadit monitorování do produkčního provozu tak, aby bylo možné podpořit vytvoření SLA. V rámci této aktivity dochází na základě konzultací a výsledků monitorování v produkčním provozu k úpravám prahových hodnot za účelem tvorby notifikací při jejich překročení. Dále jsou pak řízeny veškeré změnové požadavky na monitoring v souladu s procesy Change Management metodického rámce ITIL. Výstupy z monitorování ve formě reportů slouží jako vstup do procesu definování SLA.

Vstupy:

- akceptované monitorování služby potvrzené akceptačním protokolem.

Nástroje, techniky:

- analýza výstupů monitorování.

Role:

- konzultant pro monitoring,
- servisní manažer služby,
- operátor monitorování.

Odpovědnosti:

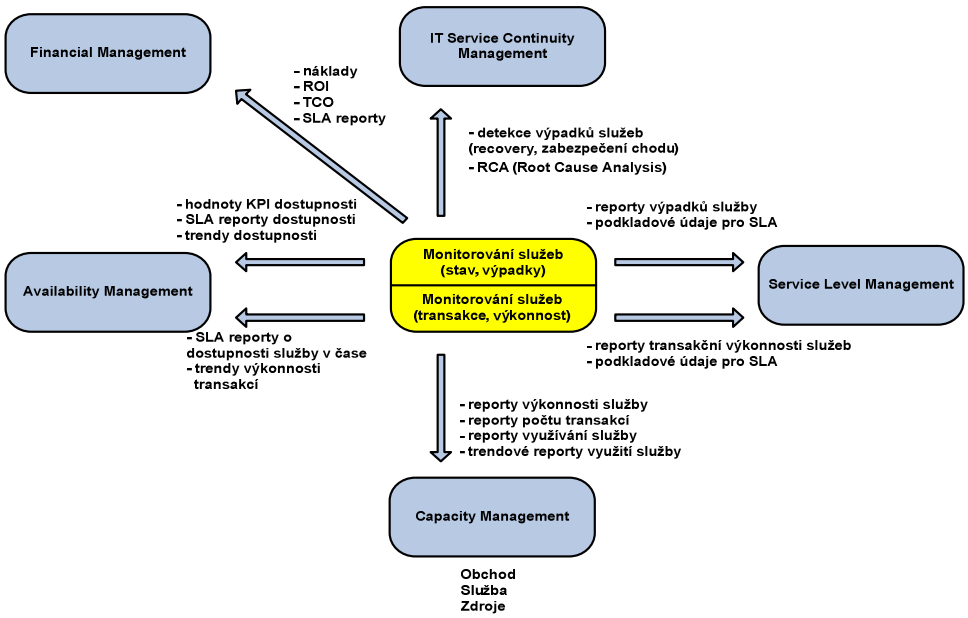
- konzultant pro monitoring - spustit monitorování v produkčním provozu a nastavit finální specifikované prahové hodnoty,
- servisní manažer služby - konzultovat finální nastavení prahových hodnot,
- operátor monitorování - převzít monitorování služby do produkčního provozu.

Výstupy:

- funkční monitorování v produkčním provozu,
- reportování naměřených hodnot.

5.7 Integrace metody do metodického rámce

Proces monitorování služeb IS/ICT poskytuje rozhraní v podobě výstupů s ostatními procesy metodického rámce ITIL, a to jak na taktické, tak i na operativní úrovni řízení ICT. Tato kapitola popisuje integraci metody monitorování do procesů rámce ITIL. Obr. 4-2 naznačuje vazby metody monitorování na procesy ITIL taktické úrovně řízení IS/ICT. Podkapitoly *5.7.1* až *5.7.5* nejprve popisují vstupy, výstupy, funkce, aktivity a cíle jednotlivého ITIL procesu. Závěrem každé podkapitoly jsou popsány vazby metody na konkrétní proces ITIL.



Obr. 5-5 - Vazba metody monitorování na procesy ITIL z oblasti taktického řízení

5.7.1 Vazby na SLM

Jakmile je definována, sepsána a podepsána dohoda o úrovni poskytování služeb, výstupy procesu monitorování slouží jako vstupy k určení, zda jsou definované hodnoty (např. dostupnosti) úrovně služby deklarované v dokumentu SLA, také dodrženy. Výstupy monitorování služeb slouží již procesu implementace SLM k měření dostupnosti a výkonnosti systémů a služeb tak, aby bylo možné definovat a uzavřít dohodu SLA mezi poskytovatelem služby a zákazníky. V rámci pokračujícího procesu SLM jsou požadovány reporty monitorování služeb. Výstupy stavového monitorování jsou reportovány v podobě výpadků jednotlivých komponent služby za předem definovanou periodu, například 1 měsíc. Implementací

modelu služby jsou zjištěny dopady těchto výpadků na službu jako celek. Délky výpadků služby jako celku jsou měřeny, ukládány, prezentovány v podobě naměřených hodnot SLA a následně porovnány s požadovanými hodnotami. Výstupy monitorování transakcí a výkonnosti služeb slouží k reportování naměřených hodnot v rámci procesu stanovení úrovně služby SLA. Výstupy z monitorování transakcí a výkonnosti služby mají odlišný charakter a představují stav služby z hlediska koncového uživatele popř. transakčního systému. Tyto výstupy jsou integrovány s výstupy ze stavového monitorování. SLA hodnoty dostupnosti popř. výkonnosti pak mohou být výsledkem buď kombinací z naměřených hodnot obou typů monitorování popř. prezentovány odděleně z hlediska stavu a výkonnosti.

5.7.2 Vazby na Availability Management

Vstupy procesu dle ITIL [[36], kap. 8.3.1]**:**

- business požadavky dostupnosti pro služby,
- stanovení dopadu na business,
- požadavky na dostupnost, spolehlivost a udržovatelnost komponent IT,
- informace o výpadcích a selháních služby,
- konfigurační a monitorovací data vztahující se k komponentám IT,
- dosažené úrovně služby definované v SLA.

Výstupy procesu dle ITIL [[36], kap. 8.3.2]:

- kritéria dostupnosti a zotavení služby,
- techniky zajišťující minimalizující dopad výpadku komponenty na celou službu (fail-over, recovery plan, RAC, load-balancing apod.),
- odsouhlasené cíle dostupnosti, spolehlivosti a udržovatelnosti,
- reportování dostupnosti, spolehlivosti a udržovatelnosti služeb,
- požadavky na monitorování komponent IT tak, aby bylo možné detekovat a reportovat nedostupnosti,
- plán dostupnosti - proaktivní zkvalitňování infrastruktury IS/ICT.

Vazby metody monitorování na dostupnost služeb:

Během provozování stavového monitorování vstupují do procesu Availability Managementu výstupy v podobě SLA reportů o dostupnosti služeb nebo jejich jednotlivých komponent, jakými jsou např. databázová platforma, aplikační platforma, síťová rozhraní apod. Dostupnost je počítána na základě přijatých událostí

z infrastruktury, jejich mapování do servisních modelů služeb a zjištění dopadu těchto událostí na komponenty služeb a služeb jako celku.

V rámci monitorování transakcí a výkonnosti služeb vstupují do procesu Availability Managementu reporty dostupnosti služeb z pohledu koncového uživatele. Tyto reporty mají charakter spojitých dat tzn., že dostupnost je periodicky, v předem definovaném časovém intervalu, měřena a zaznamenávána. Spojitost monitorovacích dat je umožňuje dále analyzovat např. do podoby trendových funkcí, pravděpodobností dostupnosti apod.

5.7.3 Vazby na Capacity Management

Vstupy procesu dle ITIL[[36], kap. 6.2]:

- nové technologie,
- SLR, SLA, katalog služeb,
- business strategie, plány a rozpočty,
- strategie IS/ICT, plány a rozpočty,
- incidenty a problémy jako výstupy ostatních procesů vztahující se k nižšímu výkonu služeb,
- změny a jejich plány jako výstupy ostatních procesů definované spolu s možným dopadem na kapacitu a dostupnost služby.

Dekompozice procesu na procesy dle ITIL [[36], kap. 6.2]:

- řízení kapacity businessu - trendy, plány, modely, rozsahy budoucích business požadavků,
- řízení kapacity služby - monitorování, analýza, ladění a reportování výkonnosti služeb; výkonnost služeb tak, jak je popsána v SLR a SLA, je monitorována a měřena a získaná data jsou dále analyzována a reportována,
- řízení kapacity zdrojů - řízení individuálních komponent IT s omezenými zdroji; měření a monitorování komponent a zdrojů; sběr, analýza a reportování monitorovacích dat.

Výstupy procesu jsou používány dle ITIL[[36], kap. 6.2]:

- v rámci dalších částí procesu - např. získaná monitorovací data jsou použita při řízení kapacity businessu - určení kdy a jaké hardwarové a softwarové vyšší verze budou potřeba k zajištění business požadavků,
- jinými procesy ITIL - např. procesy Capacity Managementu ověřují nové SLR a SLA; pomáhají procesu Financial Managementu určit finanční

prostředky, které budou potřeba k zajištění potřebných vyšších verzí hardware a software popř. k pořízení nových prostředků,

- jinými částmi podniku - např. oddělení provozu IS/ICT má za úkol implementovat změny, které navrhuje a doporučuje Capacity Management.

Vazby metody monitorování na řízení kapacit:

Do procesu Capacity Managementu vstupují v rámci monitorování výkonnosti následující informace:

- hodnoty výkonnosti služeb nebo jejich komponent,
- počty transakcí (otevřené, dokončené, úspěšné, neúspěšné apod.),
- hodnoty o využívání služby (počty operací a akcí provedené uživateli služby),
- trendové reporty (výkonnost, transakce, využití služby).

Typická KPI představuje následující výčet:

- využití CPU,
- využití paměti,
- délka fronty,
- počet transakcí,
- doba odezvy,
- délka běhu dávky.

5.7.4 Vazby na IT Service Continuity Management

Vstupy procesu dle ITIL [[36], kap. 7.1 - 7.3]:

- rizika,
- SLA, SLR,
- Business Impact Analysis (Analýza dopadu na business).

Výstupy procesu dle ITIL [[36], kap. 7.1 - 7.3]:

- řízení rizik,
- strategie obnovy systémů,
- strategie kontinuity.

Vazby metody monitorování na kontinuitu služeb IS/ICT:

V rámci zachování kontinuity business služeb slouží následující výstupy stavového monitorování jako vstupy pro tento proces:

- detekované aktuální výpadky služby nebo jejích komponent v podobě alarmů v systému pro řízení výpadků (fault management system),
- analýza příčiny (Root Cause Analysis).

5.7.5 Vazby na Financial Management for IT Services

Celkový proces finančního řízení IT je členěn na následující procesy [[36], kap. 5.1.2]:

- rozpočtování (budgeting) - předpovídající odhad finančních prostředků a stanovující čerpání finančních prostředků na projekty a provoz IT (periodický vyjednávací cyklus pro rozpočty); z hlediska provozu se dále zabývá monitorováním čerpání rozpočtu,
- účtování služeb ICT (accounting) - zabývá se účtováním položek čerpání rozpočtu; schopnost identifikovat, kategorizovat a evidovat náklady,
- účtování za služby ICT (charging) - zabývá se účtováním zákazníkům za poskytování služeb ICT.

Vstupy procesu dle ITIL[[36], kap. 5.1]:

- business požadavky na IT,
- úrovně služeb SLA,
- rozpočty.

Výstupy procesu dle ITIL[[36], kap. 5.1. - 5.2]:

- náklady a jejich kategorizace:
    - HW,
    - SW,
    - pracovní,
    - umístění prvků IS/ICT (budovy, serverové místnosti apod.),
    - externí služby,
    - transfer,
- náklady a jejich klasifikace:
    - kapitálové,
    - provozní,
    - přímé,
    - nepřímé,
- model účtování služeb,
- kalkulace nákladů na službu,
- ukazatele ROI, ROCE, TCO.

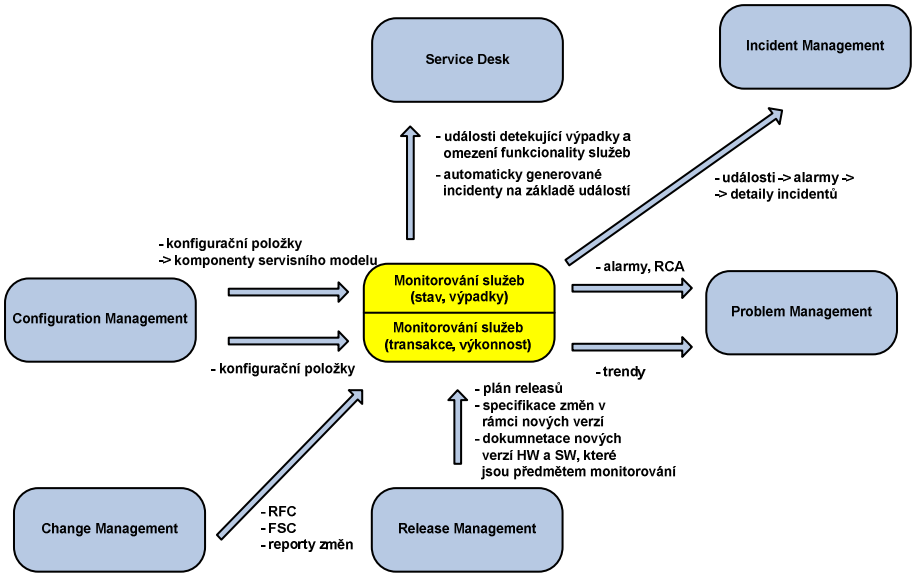
Vazby metody monitorování na finanční řízení služeb IT:

Monitorování služeb IS/ICT nepředstavuje z hlediska nasazení a provozu nic jiného než další službu ICT, se kterou jsou přirozeně spojené náklady, mezi které patří:

- náklady na pořízení a nasazení platformy pro stavové a transakční monitorování, které jsou dále členěné na:
  - kapitálové (pořízení serverů provozující platformu, pořízení softwarových licencí pro platformu),
  - provozní (údržba HW a SW, náklady na umístění platformy, personální náklady na roli operátora monitorování, strategii obnovení),
- náklady na implementaci monitorování konkrétní služby IS/ICT.

Na druhé straně výstupy monitorování služeb IS/ICT generují také výnosy, které jsou nárokovány na základě smluv SLA mezi poskytovatelem služby a jejím zákazníkem. Reporty dokazující porušení SLA hodnot s poskytovatelem služby nebo infrastruktury IT zpravidla vstupují jako podkladové údaje pro vyjednávání o zaplacení smluvní pokuty.

Následující text popisuje vazby metody na procesy ITIL z oblasti operativního řízení. Obr. 5-6 naznačuje vazby metody monitorování na procesy ITIL operativní úrovně řízení IS/ICT. Podkapitoly *5.7.6* až *5.7.11* korespondující s procesy ITIL popisují nejprve důležité vstupy, výstupy, funkce, cíle a aktivity každého ITIL procesu, ve druhé části každé podkapitoly jsou pak popsány vazby na metodu monitorování.



Obr. 5-6 - Vazba metody monitorování na procesy ITIL z oblasti operativního řízení

5.7.6 Vazby na Service Desk

Mezi hlavní funkcionality kontaktního místa patří [[37], kap. 4.4.1]:

- příjem hovorů a systémově generovaných incidentů,
- zaznamenání a sledování incidentů,
- informování klienta o stavu jeho požadavku,
- prvotní vyhodnocení a přidělení požadavku,
- monitorování incidentů, eskalační procedury vzhledem ke stanoveným SLA,
- řízení životního cyklu incidentu,
- komunikace o změnách úrovně služeb,
- koordinace podpory 2. úrovně a podpory od třetích stran,
- identifikace problémů,
- poskytování informací pro vedení podpory a doporučení na zlepšení poskytování podpory,
- zavírání incidentů a vyrozumění zákazníka.

Vstupy procesu dle ITIL [[37], kap. 4.1 - 4.7]:

- business požadavky na Service Desk,
- požadavky zákazníků,
- požadavky na metriky.

Výstupy procesu dle ITIL [[37], kap. 4.1. - 4.7]:

- manuály školení,
- seznam známých chyb a jejich řešení,
- knowledge base,
- procedury a postupy při poskytování podpory.

Vazby metody monitorování na Service Desk:

Z hlediska podpory služeb a Service Desku slouží výstupy monitorování v podobě alarmů informující o výpadcích služeb nebo jejich částí jako vstupy do systému podpory služeb. Integrace systému monitorování se Service Deskem zajišťuje proaktivní detekci problému, včasné vytvoření incidentu a jeho předání k řešení.

5.7.7 Vazby na Incident Management

Vstupy procesu dle ITIL [[37], kap. 5.2]:

- incidenty získané ze Service Desku:

    - vytvořené uživatelem,
    - automaticky vytvořené na základě alarmů v monitorovacím systému,
- konfigurační záznamy z konfigurační databáze,
- výsledky hledání problémů a známých chyb,
- detaily řešení incidentu,
- výsledky žádostí o změnu (RFC) - změnou se rozumí akce provedená na službě vedoucí k vyřešení incidentu.

Výstupy procesu dle ITIL [[37], kap. 5.2.]:

- žádosti o změnu (RFC),
- vyřešené a zavřené incidenty,
- komunikace se zákazníky a uživateli služeb,
- reporty pro management.

Hlavní aktivity Incident Managementu [[37], kap. 5.2.]:

- detekování incidentů a jejich evidence,
- klasifikace incidentů,
- diagnóza,
- nalezení řešení (možné i dočasné řešení - work-around),
- zavření incidentu po jeho vyřešení,
- vlastnictví, monitorování, sledování,
- komunikace:
    - směrem k zákazníkovi,
    - směrem k podpoře třetí strany.

Vazby metody monitorování na Incident Management:

Výstupy monitorování v podobě alarmů přijatých do systému stavového monitorování slouží jako vstupy do procesu Incident Managementu. Popis alarmu tvoří detail incidentu a poskytuje prvotní informaci, jak má být incident řešen. Řešení incidentu jsou zpravidla uložena ve scénářích řešení, které jsou na základě identifikátoru metriky svázány s konkrétními incidenty.

5.7.8 Vazby na Problem Management

Vstupy procesu dle ITIL[[37], kap. 6.2.]:

- detaily incidentů z Incident Managementu,
- konfigurační detaily položek z konfigurační databáze,
- definovaná dočasná řešení (workaround).

Výstupy procesu dle ITIL [[37], kap 6.2]:

- známé chyby,
- RFC,
- aktualizované záznamy problémů společně s jejich řešeními popř. dočasnými řešeními (work-around),
- vyřešené - zavřené problémy,
- odpovědi z Incident Managementu při hledání problémů a známých chyb,
- informace pro vedení a provoz IS/ICT.

Hlavní aktivity Problem Managementu [[37], kap. 6.2]:

- řízení problémů:
    - identifikace a zaznamenání problému,
    - klasifikace problému,
    - vyšetření problému a diagnóza,
- řízení známých chyb:
    - identifikace, zaznamenání a ohodnocení chyby,
    - zaznamenání řešení chyby (RFC),
    - uzavření chyby,
    - monitorování řešení chyb,
- proaktivní prevence problémů,
- identifikace trendů,
- získávání informací pro vedení.

Vazby metody monitorování na Problem Management:

Stavové monitorování poskytuje Problem Managementu klíčová data v podobě alarmů přijatých z infrastruktury IS/ICT a nad nimi aplikovanou analýzou příčiny problému (RCA - Root Cause Analysis). Na základě této analýzy příčiny je možné lépe stanovit řešení vzniklých problémů. Monitorování výkonnosti systémů, transakcí a aplikací z jeho povahy sběru, analýzy a uchování monitorovacích dat poskytuje tato tak, aby bylo možné stanovit trendy pomocí trendových funkcí. Na prezentační vrstvě vytvořené trendové reporty pomáhají identifikovat následující:

- trendy jako výskyt některých typů problémů na základě změn, které byly aplikované v infrastruktuře IS/ICT v minulosti,
- začínající výpadky u některých typů problémů,
- opakující se problémy určitého typu nebo na konkrétní komponentě či položce IT,

- potřeby školení pro zákazníky služby či zlepšení dokumentace.

5.7.9 Vazby na Configuration Management

Hlavní cíle Configuration managementu v rámci ITIL [[37], kap. 7.1]:

- evidence všech položek IS/ICT ve vztahu ke službám, které je využívají v rámci podniku,
- poskytovat přesné informace o konfiguracích a jejich dokumentace pro podporu ostatních ITIL procesů (Incident, Problem, Change a Release Management),
- ověřovat záznamy o konfiguračních položkách proti reálnému stavu infrastruktury a řešit nalezené nesrovnalosti.

Hlavní aktivity Configuration managementu v rámci ITIL [[37], kap. 7.2.]:

- plánování - definice cílů, rozsahu, procedur a postupů,
- identifikace - výběr a identifikace konfiguračních struktur a jejich vztahů, jejich dokumentace a záznam do CMDB,
- řízení - pouze akceptované a identifikované konfigurační položky jsou evidovány,
- evidence po celý životní cyklus konfigurační položky - umožňuje dohledat historické záznamy týkající se konfiguračních položek a jejich změn,
- ověření a audit - proces kontroly a ověřování CMDB proti skutečnému stavu infrastruktury.

Vazby metody monitorování na Configuration Management:

Záznamy o konfiguračních položkách jsou využívány při kompozici komponent servisních modelů monitorovaných služeb v rámci procesu stavového monitorování. Alarmy jsou mapovány na jednotlivé komponenty modelu a následně pak zjišťován dopad komponent na službu jako celek. Formální správnost celého modelu vycházejícího z položek CMDB zajišťuje korektní výpočet hodnot dostupností služby použitých v SLA. Konfigurační položky vstupují dále i do procesu monitorování transakcí a výkonnosti. Metoda ve své stávající podobě nepředpokládá datově systémovou integraci systémů monitorování a systémů pro Configuration Management, avšak změny v rámci procesu Change Managementu je třeba zabezpečit na procesní úrovni tak, aby byly v konfiguracích promítnuty i do systémů monitorování.

5.7.10 Vazby na Change Management

Vstupy procesu dle ITIL [[37], kap. 8.2.]:

- změnové požadavky (RFC),
- CMDB,
- plán budoucích změn (FSC).

Výstupy procesu dle ITIL [[37], kap. 8.2.]:

- aktualizované FSC,
- změnové požadavky (RFC),
- reporty provedených změn.

Hlavní aktivity Change managementu jsou následující [[37], kap. 8.2]:

- řízení vzniku, filtrování a evidence změn,
- zhodnocení dopadu, rizik, nákladů a výnosů změn,
- řízení oprávnění a schválení změn,
- řízení a koordinace implementace změn,
- monitorování a reportování,
- revize a zavírání změnových požadavků RFC,
- reportování vedení.

Vazby metody monitorování na Change Management:

Monitoring přímo závisí na vstupech z procesu Change Managementu, protože informace o prováděných a plánovaných změnách je třeba propagovat do systému monitorování. Typickým příklad může představovat přesun aplikace mezi hostujícími servery. Bez včasné informace o této plánované změně zůstává nastavení stavového monitorování např. aplikačních procesů na původním serveru, kde již však aplikace po dokončení změn více neběží. Dalším příkladem je změna databázové struktury ve zdrojovém back-end systému, ze kterého jsou získávána data pro účely transakčního monitorování. Hrubá vrstva zabezpečující zisk dat bez patřičných úprav přestane fungovat a monitorování se stává nefunkční. Z procesu Change Managementu jsou pro metodu monitorování relevantní následující informace:

- plán budoucích změn (FSC),
- aktuální stav změnových požadavků (RFC),
- reporty provedených změn.

5.7.11 Vazby Release Management

Hlavní cíle Release Managementu [[37], kap. 9.1]:

- plánovat a dohlížet na nasazování nových verzí HW a SW,
- navrhovat a implementovat efektivní postupy distribuce a instalace změn v systémech IT,
- zajistit sledování a možnost dohledání změn aplikovaných na systémech IT,
- zajistit, že pouze správné, ověřené a testované verze jsou instalovány do produkčního prostředí,
- řídit požadavky a očekávání zákazníků během plánování a nasazování nových verzí,
- domluvit přesný obsah a plán nasazení nových verzí na základě provázání s Change Managementem,
- implementace nasazení nových verzí do produkčního prostředí pouze prostřednictvím kontrolovaných procesů Configuration a Change Managementu,
- správa Definitive Software Library (DSL), která obsahuje veškeré hlavní kopie instalovaných verzí software a k nim související dokumentace,
- správa Definitive Hardware Store (DHS), který obsahuje náhradní HW součástky udržované na stejné úrovni jako jsou produkční pro případ nutnosti obnovení systémů,
- aktualizace CMDB skrze celý Release Management proces.

Výše uvedené cíle jsou zajišťovány prostřednictvím aktivit [[37], kap. 9.2]:

- navržení postupů a plánování nasazování nových verzí HW a SW,
- návrh, vytvoření, konfigurace a akceptace uvolnění nové verze,
- testování nových verzí dle akceptačních kritérií,
- schvalování implementací nasazení nových verzí,
- audit HW a SW před a po implementaci změn,
- instalace nového popř. aktualizovaného HW,
- uložení SW, který předmětem nasazení do produkčního prostředí,
- vydání, distribuce a následná instalace SW.

Vazby metody monitorování na Release Management:

Monitorování přímo závisí na vstupech z procesu Release Managementu, protože s nasazením nových verzí SW a HW mohou vznikat změny oproti předchozím verzím a tyto je třeba uvažovat v systému monitorování. Z procesu

Release Managementu jsou pro metodu monitorování relevantní následující informace:

- seznam plánovaných releasů,
- specifikace změn v plánovaných releasech s vazbou na systém monitorování,
- aktualizovaná dokumentace k nové verzi.

6 Případová studie

Případová studie ověřuje navrženou metodu monitorování prostřednictvím její aplikace v rámci projektu zavedení E2E a transakčního monitorování vybraných 45 služeb, aplikací, datových toků a business procesů v prostředí významného mobilního operátora T-Mobile Česká republika a.s. (dále jen TMCZ).

Cílem případové studie je ověřit navrhovanou metodu při rozšíření stávajícího dohledového systému zavedením E2E monitoringu a monitorování transakcí a výkonnosti vybraných systémů a služeb realizujících důležité business transakce v prostředí informační infrastruktury společnosti TMCZ.

6.1 Cíle počátečního výzkumu

Před realizací samotného projektu je proveden počáteční výzkum, jehož výstupy slouží jako vstupní data v analytické fázi realizace projektu a ve fázi rozhodování a realizaci projektu ze strany TMCZ.

Cíle počátečního výzkumu jsou následující:

- po konzultacích s odpovědnými pracovníky TMCZ a na základě informací ze stávajícího dohledového systému identifikovat kritické business služby,
- systémové části business procesů a aplikace, které budou projektem monitorovány. Finální rozhodnutí o výběru služeb je na straně TMCZ,
- identifikovat Key Performance Indicators KPI pro každou službu nebo proces zapojený do monitorování,
- poskytnout co nejpřesnější odhad pracnosti na realizaci projektu v jednotkách člověkoden (MD), který je zohledněn při výpočtu celkových nákladů na uskutečnění projektu,
- vytvoření prvotního návrhu systému specifikace hardwarových, softwarových a licenčních požadavků pro účely kalkulace celkových nákladů na realizaci budoucího projektu.

6.2 Výchozí situace

TMCZ používá k monitorování a řízení výpadků rozsáhlou implementaci fault management na platformě IBM/Micromuse Netcool. Platforma Netcool

na TMCZ obsahuje produkty z několika oblastí IT operations. Na TMCZ slouží tato platforma k příjmu, korelační analýze, zpracování a následné prezentaci alarmů generovaných na základě vzniku událostí v rozsáhlé infrastruktuře IS/ICT.

6.2.1 Komponenty řízení výpadků

V rámci výchozí situace jsou charakterizovány jednotlivé stavební prvky celého stávajícího dohledového řešení a jejich vzájemné vazby mezi nimi.

6.2.1.1 Netcool OMNIbus

Netcool OMNIbus představuje jádro celé platformy a slouží ke sběru a analýze alarmů generovaných z různorodých částí IS/ICT. Tyto informace jsou pak následně prezentovány ve zjednodušených pohledech a filtrech koncovým uživatelům, jakými jsou operátoři centrálního monitorovacího centra, systémoví administrátoři nebo servisní manažeři. Tato část celé platformy dále slouží ke konsolidaci monitorovacích informací z různých management systémů třetích stran. Na TMCZ je právě funkcionalita integrace s nativními dohlížecími systémy pro různé technologie, jakými jsou např. Motorola OMCR, Siemens, Alcatel, Ericsson PDH/HCC atd., využita. Mezi základní komponenty Netcool OMNIbus patří:

- objektový server (object server) - je databáze rezidující v operační paměti za účelem vyšší rychlosti a výkonnosti při zpracování velkého množství informací v krátkém časovém úseku. Do této databáze jsou monitorovací informace odesílány z externích programů, jakými jsou sondy, brány nebo také další objektové servery. Tyto informace jsou ukládány do databázových struktur a následně prezentovány uživatelům prostřednictvím listu událostí, pohledů a filtrů,
- sondy (probes) - sonda je program, který umí detekovat a získat data událostí ze zdrojového zařízení, které je předmětem monitorování. Sonda se buď aktivně připojí ke zdrojovému zařízení nebo pasivně naslouchá a přijímá informace o událostech na předem specifikovaném portu. Tyto informace jsou z „raw“ podoby transformovány prostřednictvím souboru pravidel do podoby události (alarmu), který je následně odeslán do objektového serveru,
- brány (gateways) - softwarová komponenta umožňující výměnu událostí mezi objektovými servery a systémy třetích stran např. help-desk systémem,

archivní databází událostí, systémem CRM atd. V prostředí TMCZ jsou brány použity k přenosu událostí mezi objektovými servery za účelem vytvoření architektury odolné vlastním výpadkům (fail over) a mezi objektovým serverem a archivní databází, kde jsou archivovány všechny příchozí události z IS/ICT infrastruktury,

- desktopové nástroje (desktop tools) - desktopové nástroje jsou součástí grafického uživatelského rozhraní a slouží k manipulaci s událostmi a ke konfiguraci prezentace událostí,
- administrační nástroje (admin tools) - slouží administrátorům k vykonávání rutinních úkolů správy a konfigurace systému.

Mezi nejdůležitější charakteristiky Netcool OMNIbus, které jsou podporovány patří vysoký stupeň možnosti automatizace, deduplikace a korelace událostí.

Automatizace je vlastnost podporovaná objektovým serverem umožňující detekovat změny ve stavu uložených alarmů a vyvolat automatické reakce na tyto změny bez nutnosti zásahu operátora, např. spárování a vymazání událostí typu *problém* a *vyřešení* tak, aby nezůstávaly v objektovém serveru a tím nezaplňovaly jeho databázi.

Deduplikace umožňuje více stejných alarmů pocházejících ze stejné konkrétní části IS/ICT (např. periodicky opakující se alarm o zaplnění svazku X na serveru Y dosáhlo 90% nebo výpadek spojení na routeru Z) redukovat na úrovni objektového serveru do jednoho alarmu s označením počtu takto akceptovaných alarmů a tím snížit zatížení a zaplnění objektového serveru.

Základní typ korelace událostí představuje označení událostí způsobujících výpadky či defekty v IS/ICT jako události typu „problem“ a událostí informující o odstranění problému a návratu ke standardnímu stavu jako „resolution“. Následné spárování těchto událostí podle toho, z jakého prvku či části IS/ICT pocházejí, je prováděno na úrovni sond v souborech pravidel. Informace o tom, zda se jedná o událost typu „problem“ nebo „resolution“, je poté propagována do objektového serveru.

6.2.1.2 Netcool Impact

Netcool Impact je další stavební prvek celé platformy, který funguje a zde vystupuje jako analytický a korelační modul rozšiřující komponentu Netcool

OMNIbus. Netcool Impact operuje nad databází událostí objektového serveru a prostřednictvím speciálních programů nazývaných „politiky“, které jsou naprogramovány implementačním týmem, provádí složitější datové korelace, obohacování událostí o informace uložených v externích systémech a databázích, které není vhodné mít v objektovém serveru a další složitější operace. V prostředí TMCZ je Netcool Impact používán k obohacování událostí objektového serveru o detaily alarmu a operátorské hlášky, které jsou uloženy v externí databázi. Operátorská hláška radí operátorovi, jak bezprostředně postupovat při hlášení a následném řešení problému. Každá událost, která je uložena a prezentována v objektovém serveru, je určena identifikátorem metriky, s níž je událost spojena. Na základě identifikátoru metriky a severity události jsou Impactem vybírány texty detailu a operátorské hlášky následně obohacující danou událost.

Netcool Impact je dále používán ke složitým korelačním analýzám příčiny vzniku mnoha událostí (Root Cause Analysis). Při rozsáhlejších výpadcích v IS/ICT se může stát, že dojde k vygenerování velkého množství alarmů, které jsou doručeny do objektového serveru, avšak pouze několik z nich nebo dokonce pouze jeden tvoří příčinu celého výpadku. Operátor není schopen zareagovat na stovky doručených alarmů, a proto je cílem korelační analýzy příčiny označit jednu či více událostí, jako událost příčinnou a jejím potomků, tedy událostem důsledkovým, snížit prioritu a následně je vymazat ze systému.

Příkladem může být například výpadek napětí na BSC (Base Station Controller) Y. V případě, že je více BTS zapojeno sériově a tedy závisí na dané BSC. Dojde k vygenerování více událostí typu „Power Outage“, avšak pouze událost „Power Outage on BSC Y“ je událostí příčinnou, ostatní události byly vygenerovány jako důsledek výpadku napájení na BSC Y a za normálních okolností by vygenerovány nebyly.

6.2.1.3 Netcool WebTop

Netcool WebTop je webová aplikace umožňující alternativní [5] rozšíření prezentace alarmů uložených v objektovém serveru a manipulaci s nimi. Webový server zprostředkovává data z jednoho či více objektových serverů a jeho uživatelé mohou k těmto informacím přistupovat prostřednictvím webového prohlížeče.

[5] K objektovému serveru se uživatelé primárně připojují prostřednictvím tlustého klienta

WebTopová mapa je grafickou vizualizací mapující alarmy objektového serveru. Mapu lze integrovat do sady webových stránek vytvořených administrátorem. V závislosti na typu licence mohou uživatelé manipulovat různými způsoby se zobrazenými alarmy.

6.2.1.4 Netcool RAD

Netcool RAD (Realtime Active Dashboards) je dalším prvkem monitorovací platformy implementovaným na TMCZ. RAD patří do oblasti service management. Prostřednictvím této aplikace je možné vytvářet grafické modely služeb a definovat závislosti mezi jednotlivými komponentami monitorované služby. RAD server je připojen k objektovému serveru, analyzuje příchozí události a následně je mapuje na základě definovaných příchozích pravidel do jednotlivých komponent servisního modelu dané služby.

V objektovém serveru je definováno šest severit příchozích událostí, kterým odpovídá šestičlenný barevný model. Těchto šest severit je mapováno pouze na tři možné dopady na komponenty dané služby. Způsob mapování severit je konfigurovatelný, konfigurace se provádí na základě analýzy dopadu jednotlivých typů událostí na dané komponenty. Tabulka níže znázorňuje možné výskyty severit události v objektovém serveru a RAD aplikaci.

Severita události v objektovém serveru		Možné dopady na službu v rámci servisního modelu	
0	Clear	1	Good
1	Indeterminate		
2	Warning	2	Marginal
3	Minor		
4	Major	3	Bad
5	Critical		
prázdné	Žádná událost	prázdné pole	Žádný dopad na službu

Tabulka 6-1 - Seznam možných severit objektového serveru a RAD aplikace

Prostřednictvím konfigurovatelných pravidel lze propagovat dopady komponent, které jsou v hierarchii služby na nižší úrovni na komponenty, které jsou v hierarchii celé služby o úroveň výše, postupně až na komponentu nejvyšší úrovně, která pak představuje stav celé služby.

6.2.1.5 Netcool SSM/ASM

Netcool SSM (Service System Monitors) je program, který umožňuje monitorovat dostupnost a výkonnost hostujících systémů a business aplikací na nich provozovaných. Aplikaci tvoří následující komponenty:

- hlavní agent (master),
- subagenti implementující MIB moduly sloužící k získávání monitorovacích dat pro sledování dostupnosti a výkonnosti,
- administrační nástroje sloužící ke konfiguraci a ovládání agenta[6].

Netcool ASM (Application Service Monitors) rozšiřuje funkcionalitu SSM ve formě dalšího subagenta tím, že umožňuje monitorovat dostupnost a výkonnost řady komerčních serverových a databázových produktů, jakými jsou např. SAP, SŘBD Oracle, IBM WebSphere server apod.

Z hlediska monitoringu výpadků business aplikací na TMCZ poskytují programy SSM/ASM společně s externími skripty vstupní monitorovací data pro další zpracování. Na TMCZ jsou prostřednictvím externích skriptů a SSM agentů monitorovány systémové, databázové a aplikační metriky.

6.2.2 Stávající architektura monitorování výpadků služeb na TMCZ

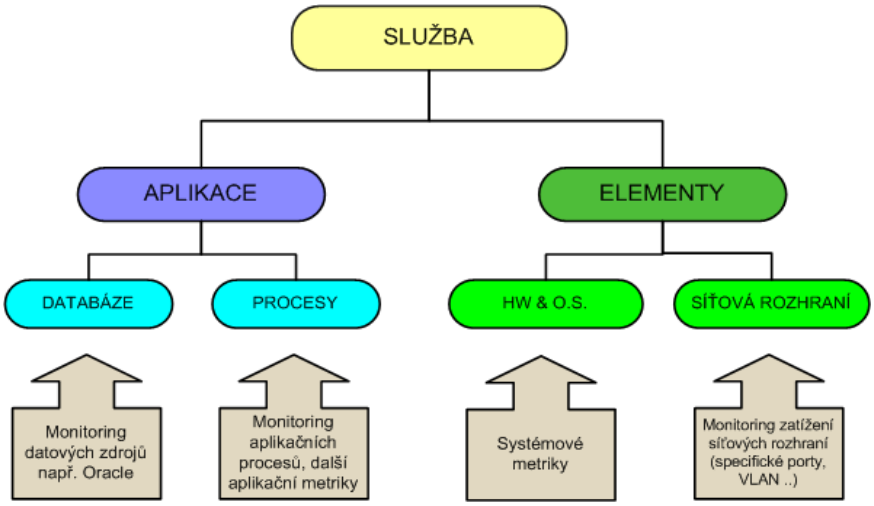
Monitorování business služeb na TMCZ je plně založeno na hierarchickém modelu, který je rozdělen do jednotlivých částí. Elementy jsou plně pokryty SSM agenty, kteří jsou nainstalováni na jednotlivých serverech. SSM agenti sledují podle jednotné konfigurace následující systémové a síťové metriky:

- počet běžících procesů v operačním systému,
- využití diskového prostoru na jednotlivých svazcích,
- využití fyzické paměti serveru,
- využití CPU,
- na síťových rozhraních: nefunkční síťové spojení, obnova spojení, smyčka offline, žádná odezva ze sítě ethernet po dobu X minut.

Aplikační metriky jsou částečně implementovány prostřednictvím kombinace SSM/ASM, externích skriptů (nejčastěji implementovaných v prostředí shellu a jazyce perlu) a aplikace Distribuční skript (perlová aplikace umožňující vysoce složité korelace událostí, monitoring aplikačních logů a jednoduše získávat události

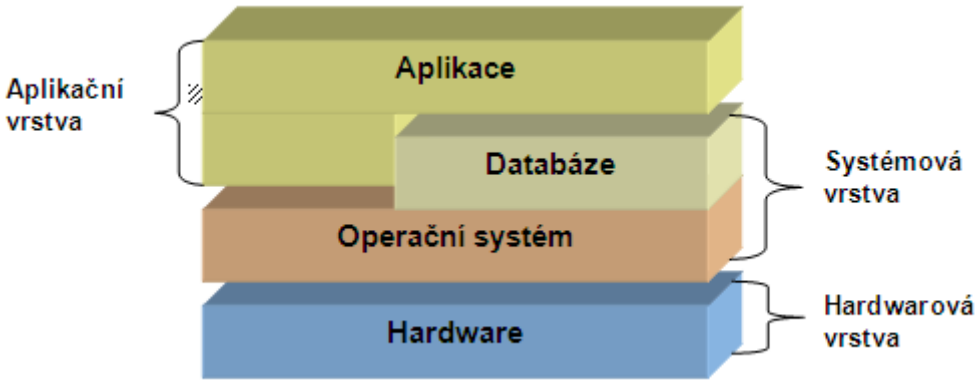
[6] Veškerá konfigurace a ovládání SSM agenta jsou implementovány prostřednictvím SNMP

prostřednictvím několika rozhraní[7] a ty pak následně po jejich korelaci doručovat do mnoha centrálních monitorovacích systémů).



Obr. 6-1 - Model závislosti business služby na vstupních monitorovacích informacích

Obr. 6-2 ukazuje rozdělení platformy business služby do tří vrstev určených pro monitorování.



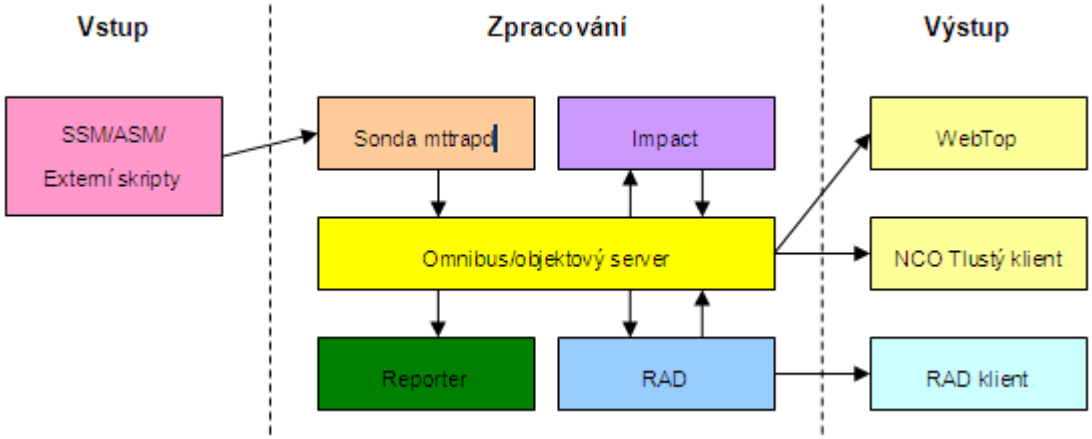
Obr. 6-2 - Vrstvy služby ICT - monitorování

Hardwarová a systémová vrstva je předmětem fault management monitorování prostřednictvím SSM agentů, externích skriptů a v případě dohledu SŘBD Oracle kombinace uložených PL/SQL procedur a SSM. Aplikační vrstva je monitorována pomocí SSM/ASM, externích skriptů a distribučního skriptu.

[7] Následující vstupní API jsou DScriptem podporována: Shell , C/C++/Java, PL/SQL (procedury v databázi Oracle, přímý zápis do roury na operačních systémech typu UNIX)

6.2.3 Implementace monitorování business služeb na TMCZ

Obr. 6-3 znázorňuje tři hlavní části monitorování a následující text popisuje každou z nich.



Obr. 6-3 - Implementační části monitorování business služeb

6.2.3.1 Vstup

Monitorování služeb na TMCZ je založeno na událostech generovaných SSM/ASM agenty. Agenti využívají interní monitorovací mechanismy nebo externí skripty ke sběru metrik. Agenti odešlou informaci ve formě SNMP trapu na mttrapd sondu v případě, že dojde překročení prahové hodnoty.

6.2.3.2 Zpracování

Část zpracování je pokryta mttrapd sondou, která poslouchá na definovaném portu a čeká na příjem SNMP trapů. Sonda přijme, transformuje příchozí SNMP trap do podoby události a následně ji doručí do objektového serveru. Události jsou obohaceny Impact serverem o důležité informace potřebné k vyhodnocení události. RAD server načte novu událost z objektového serveru a vytvoří novou syntetickou událost, v případě, že došlo ke změně stavu služby nebo její komponenty tak, jak je definováno v hierarchickém modelu. Každá příchozí událost je z centrálního objektového serveru kopírována prostřednictvím brány do databáze produktu Reporter, kde je událost uložena pro účely historického reportování a vyhodnocování SLA.

6.2.3.3 Výstup

Výstupy monitorování jsou přístupné pomocí klientské aplikace Netcool OMNIbus (tlustý klient), Netcool WebTop (webový prohlížeč) a Netcool RAD (webový prohlížeč). Výstupy z monitoringu poskytují komplexní informaci o stavu služby z hlediska stavového monitoringu.

6.2.4 Implementace SLA

Implementace SLA je zajištěna pomocí RAD komponenty, která na základě událostí v objektovém serveru mapuje tyto události do jednotlivých komponent monitorované služby. Tyto dopady jsou propagovány na základě definovaných pravidel až k nejvyšší komponentě představující celou službu. RAD umožňuje nastavit SLA hodnoty na základě hodnot výpadků služby v reálném čase. Dojde-li ke skutečnému výpadku např. dvou klíčových komponent služby (oba dva servery v databázovém clusteru), které jsou nezbytné pro fungování služby, dojde vlivem příchozích událostí a jejich mapování na komponenty služby a následné propagaci až k instanci představující službu jako celek, ke zčervenání služby. Od této chvíle počítá RAD aplikace dobu výpadku. Procentuální hodnota SLA je konvertována do časové hodnoty a následně porovnána se skutečnou dobou výpadku služby za dané období (nejčastěji 1 měsíc). Na TMCZ se počítá s následujícími parametry SLA:

- kumulativní doba výpadku služby (nízký dopad na službu, kritický dopad na službu),
- maximální doba plánovaného výpadku,
- časový prostor k údržbě služby (např. každé úterý od 2:00 do 4:00).

Doba výpadku služby v časovém prostoru pro údržbu není započítávána do výpadku pro posouzení dosažení SLA hodnot.

6.2.5 Zhodnocení stávajícího stavu

Stávající implementace monitorování na platformě Netcool poskytuje plně funkční monitorování výpadků klíčových aplikací a poskytuje tím v reálném čase centralizovaný pohled na stav a fungování služeb i zbytku IS/ICT infrastruktury z hlediska fault management a tedy stavového monitorování. Toto integrované řešení umožňuje operátorům monitorovacího centra rychle a efektivně reagovat na výpadky či snížení výkonu aplikací, databází, serverů a ostatních prvků IS/ICT. Z ekonomického hlediska toto řešení umožňuje snížení mzdových nákladů na provoz

a dohled IS/ICT, protože díky centralizovanému monitorovacímu systému, kde jsou zobrazeny události ze všech technologií a platforem, například v nočních hodinách zvládnou monitorovat všechny aplikace řádově jednotky operátorů. Výhodou řešení je dále, že umožňuje spočítat kumulativní doby výpadku služeb prostřednictvím RAD aplikace a následně vyhodnotit SLA monitorovaných služeb a aplikací, a tím přispět ke zkvalitnění poskytování těchto služeb interním i externím zákazníkům.

Nedostatkem celé monitorovací platformy je to, že poskytuje pouze statický a tím i nespojitý pohled na stav daných služeb, protože události jsou ze systému generovány pouze v případě výpadků, defektů, či překročení definovaných prahových hodnot pro jednotlivé metriky. Události jsou pak v objektovém serveru přítomny pouze po dobu trvání defektu či výpadku. Při obnovení chodu, tedy při příchodu události typu „vyřešení problému“ jsou původní události typu „problém“ čištěny snížením severity a následně odmazány z objektového serveru. Monitoring tedy nesbírá data a nevyhodnocuje je spojitě, tzn., že v případě, že nedojde-li k překročení žádné prahové hodnoty, nedojde pak ani k vygenerování události. Tímto nelze zjistit jaké byly naměřené hodnoty jednotlivých metrik (např. zatížení CPU, využití paměti, či počty běžících procesů) v době, kdy se server, aplikace či služba nenacházela v nestandardním stavu z hlediska monitorování. Tento typ monitorování dále nezachycuje funkčnost, kterou potřebuje koncový uživatel.

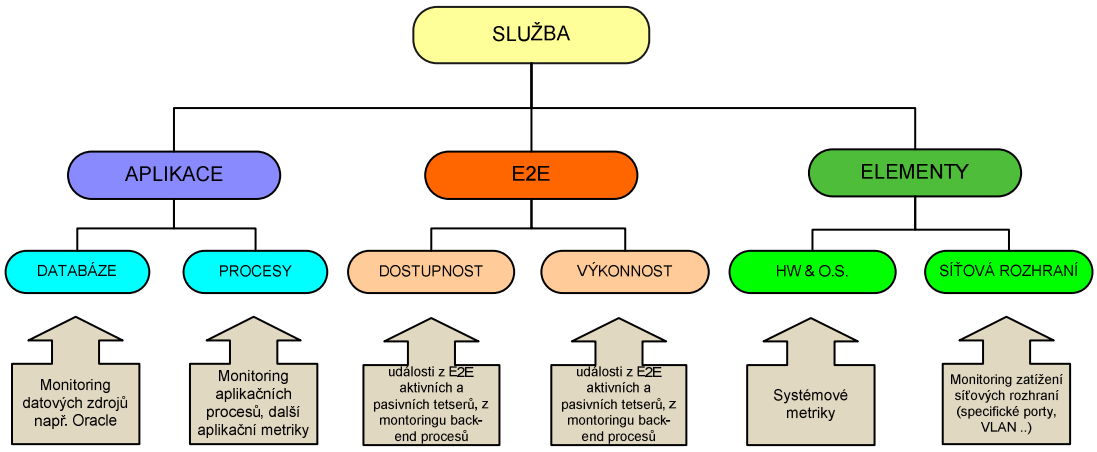
Uvažujme příklad, že máme službu fungující na několika aplikačních a databázových serverech v clusteru a fault management dohled vidí službu v korektním stavu, protože nebyly vygenerovány žádné kritické alarmy. Databáze je funkční a nejeví žádné známky problémového stavu ani defektu, síťová konektivita je zajištěna, všechny procesy aplikačního serveru zajišťující jeho korektní chod jsou běžící, server nezalogoval žádný problém. I přes všechny tyto indikátory však nemusí vlivem jiných externích okolností v aplikaci docházet k žádným transakcím, popř. nedochází k žádným požadavků ze strany koncových uživatelů. Tento jev může indikovat v době, kdy za normálních okolností dochází k desítkám tisíc transakcí či požadavků za hodinu, nestandardní stav a chování služby či dané aplikace. Způsob monitorování popsaný v kapitole *6.2.2 Stávající architektura monitorování výpadků služeb na* TMCZ neposkytuje žádné nástroje, jak odhalit tyto anomální stavy. Způsob řešení ve formě doplnění stávající architektury o E2E monitorování klíčových business aplikací, služeb, datových toků, systémových a busienss procesů (transakční monitoring) je navržen v následující kapitole *6.3 Návrh řešení*.

6.3 Návrh řešení

Z výše uvedeného textu vyplývá, že stávající monitorování výpadků a defektů aplikací, služeb a prvků IS/ICT, na kterých jsou tyto provozované, neumožňuje sledovat jejich hlubší funkcionalitu, délky trvání transakcí či jiných operací v jednotlivých systémech.

6.3.1 Cílový stav architektury monitorování

Na Obr. 6-4 je představen cílový stav architektury monitorování služeb na TMCZ. Cílový stav předpokládá rozšíření stávající systému řízení výpadků o vstupy z transakčního, E2E monitoringu a monitoringu výkonnosti služeb (vše v rámci oblasti E2E).



Obr. 6-4 - Rozšířený model závislosti služby na vstupních monitorovacích informacích

6.3.2 Počáteční výzkum

K získání všech relevantních informací potřebných pro stanovení odhadu pracnosti a celkové kalkulace projektu byla zvolena dotazníková metoda. Dotazníky byly doručeny kompetentním osobám ze strany odběratele, kterými jsou uživatelé výsledného monitorovacího systému: vlastníci business služeb, servisní manažeři a systémoví administrátoři. Cílem dotazníku je získat následující informace o službě, která má být v rámci projektu monitorována:

1. základní informace o službě:
    - název, funkcionalita,
    - kategorie z hlediska uživatelského rozhraní (WWW, tlustý klient, SMS, MMS),

- třída služby z hlediska požadavku na její funkčnost (Platinum, Gold, Silver, Bronz, popř. jiná),
- přibližný počet uživatelů,
- odhadovaný finanční dopad v případě výpadku nebo snížení výkonnosti,
- odhad dalších dopadů v případě výpadku nebo snížení kvality nebo výkonnosti služby (např. poškození dobrého jména firmy, ztráta zákazníků),
- intenzita a doba trvání výpadků (např. jednou týdně 1 hodina nedostupnosti),
- kontakty na odpovědné osoby,
- definice koncových uživatelů (interní, externí, oba typy),
- perspektivnost služby do budoucna (perspektivní - ano/ne),
- požadavky na SLA.

2. definice požadovaných KPI (dále jen indikátorů):
    - délka trvání transakce (např. délka aktivace karty SIM, doba potřebná pro přihlášení k intranetovému portálu či jiné aplikaci apod.),
    - úspěšnost a neúspěšnost transakcí (úspěšnost transakce je definována v závislosti na službě, v některých službách může být úspěšnost definována jako pouze „dokončení transakce“ v jiných službách např. „dokončení transakce v čase t s výsledkem „OK“ apod.),
    - čas odezvy (např. doba potřebná ke stažení webové stánky v intranetu nebo internetu),
    - dostupnost služby,
3. technické detaily služby:
    - jiné služby a systémy potřebné k provozu dané služby (např. závislost mezi systémy, systém A potřebuje včas vstupní data od systému B apod.),
    - definice typických výpadků a nestandardního chování služby, jak je možno detekovat tyto stavy automatizovaně,
    - určení geografické polohy koncových uživatelů dané služby (Praha, Hradec Králové, Louny popř. jiné),
    - určení síťové polohy koncových uživatelů přistupujícím ke službě (internet, intranet, RAN, popř. jiné),

4. detailní informace o KPI:
    - technická možnost měřit indikátor (možné bez úpravy služby, nemožné bez úpravy služby, možné ale složitě implementovatelné & důvody, indikátor je již měřen, nemožné & důvody,
    - data z jakých datových zdrojů je nutné vyhodnotit za účelem stanovení hodnoty indikátoru? (SQL databáze, výsledek SNMP dotazování, vstupní soubor, výsledek E2E testu, pokročilé zpracování např. kombinace různých možností),
    - zda je možné provést simulační akce, jinak prováděných koncovými uživateli, vedoucí k získání hodnot indikátoru? (možné, nemožné & důvody),
    - stanovení řádového počtu transakcí za 1 den nebo za jiný stanovený časový úsek,
    - určení přibližného času potřebného k provedení simulačního testu za účelem získání hodnoty indikátoru (např. přihlášení k aplikaci, uskutečnění operace, odhlášení).

Informace z takto strukturovaného dotazníku jsou vyhodnoceny a obohaceny o informace získané během technických konzultačních schůzek s aplikačními administrátory vybraných služeb. Následnou syntézou a analýzou získaných informací je třeba ohodnotit pracnost v následujících fázích pro každou službu:

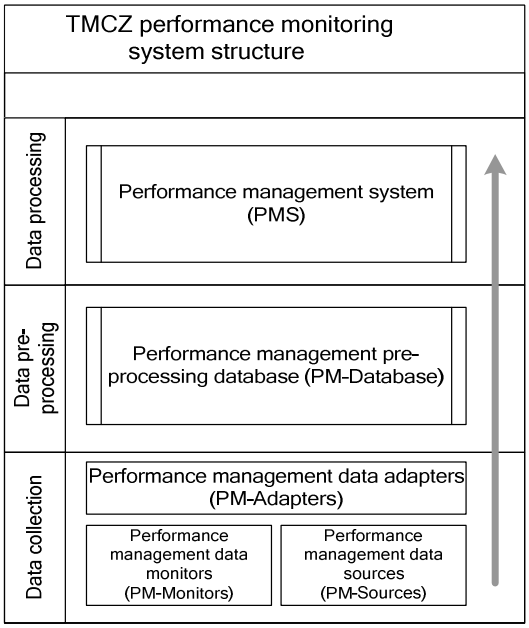
- návrh a analýza,
- implementace, testování (včetně migrace dohledu služby do produkčního prostředí),
- tvorba dokumentace,

Hlavní charakteristika zvoleného postupu při odhadu pracnosti implementace daných služeb spočívá v tom, že je-li nějaká komponenta univerzální a tedy i použita vícekrát v rámci celého projektu, je pracnost na její implementaci odhadnuta pouze jednou respektive pouze s menší pracností na její případnou modifikaci.

6.3.3 Základní architektura systému monitorování a odhad pracnosti

Budoucí systém monitorování výkonnosti služeb a aplikací je z hlediska architektury modulární. Systém je rozdělen do tří základních vrstev (viz Obr. 6-5). Odhad pracnosti vychází z architektury monitoringu a je agregován na základě dílčích odhadů pracnosti na vytvoření jednotlivých vrstev. Systém se skládá

z univerzálních modulů, které je možné sdílet několika službami, které jsou předmětem monitorování. Dalšími komponentami systému jsou specifické moduly, které mohou získávat nebo zpracovávat monitorovací data pouze pro jednu službu. Přístup používající sdílené moduly a funkcionality výrazně snižuje zátěž monitorovaných systémů, pracnost na implementaci monitoringu, a tím i náklady na realizaci celého projektu. Sytém je zaměřen jako doplňkový monitoring služeb a aplikací, a proto nejsou požadovány metriky hardware, operačního systému a databází, které jsou řešeny v rámci stávajícího fault management dohledu.



Obr. 6-5 - Architektura systému monitorování výkonnosti služeb a aplikací

6.3.3.1 Vrstva sběru dat

Vrstva sběru dat má v celé architektuře jasný cíl. V konfigurovatelných intervalech (5 min., 15 min., 1h, 1 den apod.) získávat hodnoty KPI, které mají být měřeny a doručovat je předzpracovávající databáze řízení výkonnosti služeb (Performance Management Preprocessing Database - PMPD).

Vrstvu sběru dat tvoří následující moduly: monitory řízení výkonnosti (PM-Monitors), adaptéry řízení výkonnosti (PM-Adapters), zdroje pro řízení výkonnosti (PM-Sources).

Monitory jsou moduly, které jsou používány k přímému sběru dat z monitorovacích systémů formou E2E testů. Mohou to být například roboti, databázové skripty, WWW skripty, specifické testery apod.

Adaptéry jsou moduly, které poskytují standardizované rozhraní mezi Monitory a Zdroji na straně jedné a předzpracovávající databází (PMPD) na straně druhé (např. SQL procedury, konfigurované webové služby apod.). Adaptéry mají za úkol zformátovat a předat naměřená data od Monitorů nebo data získaná ze Zdrojů do nejnižší vrstvy PMPD.

Zdroje jsou moduly, které již jsou nebo budou naimplementovány ve zdrojových systémech, které ukládají statistická data potřebná k monitorování.

Předzpracovávající databáze (PMPD) je v celém řešení zodpovědná za příjem, korelaci, agregaci a export naměřených dat do strukturovaných souborů, které jsou následně zpracovány nejvyšší vrstvou (vrstva zpracování) a uloženy do systému řízení výkonnosti (Performance Management System - PMS) pro účely další agregace a prezentace.

6.3.3.2 Vrstva předzpracování dat

Vrstva předzpracování je plně tvořena předzpracovávající databází (PMPD), která se skládá podobně jako celý monitorovací systém skládá ze tří vrstev - hrubé (raw), korelační (correlation) a agregační (aggregation), kde každá z vrstev má své datové struktury a programy a je zodpovědná za určitý typ úkolů. V PMPD jsou dále generické datové struktury a programy, které jsou sdíleny při předzpracování dat všech služeb. Podrobný popis všech vrstev, jejich činností a datových struktur je pospán v kapitole Detailní návrh.

6.3.3.3 Vrstva zpracování dat

Vrstva zpracování dat zastřešuje všechny subsystémy systému řízení výkonnosti služeb a má následující úkoly:

- přijmout předzpracovaná data v podobě strukturovaných souborů,
- dále je statisticky zpracovat a agregovat do hodinových, denních týdenních, měsíčních a ročních vzorků,
- poskytnout real-time reporty a agregované reporty,
- poskytnout celkovou prezentační vrstvu zpracovaných dat,
- umožnit integraci s FM (ve formě SNMP zpráv).

Pro zabezpečení vrstvy zpracování je navrženo implementovat řešení InfoVista Foundation, což je vysoce konfigurovatelný modulární systém řízení výkonnosti a dále slouží i pro účely reportování. Navrhované řešení je založeno na hierarchickém stromu Vist[8] a na jejich dědičnosti. To v praxi znamená, že obecné KPI, jakými jsou např. dostupnost, spolehlivost, délka trvání transakce apod., a jejich reporty jsou definovány na úrovni Visty typu „rodič“, naopak specifické indikátory na Vistě nižší úrovně typu „potomek“. Tato jednotná logika je pak uložena a organizována v univerzálních knihovnách, což v praxi umožňuje sdílet implementační logiku mezi monitorovanými službami a snížit tím pracnost a náklady na implementaci.

6.3.3.4 Výpočet pracnosti

Na základě informací z obecné architektury systému a výsledků dotazníkové metody je navržen následující vzorec výpočtu pracnosti implementace celého projektu.

TWL = wlPMPD + (wlPM_MonitorG + wlPM_MonitorG*kc*NSMG) + (wlPM_AdapterG + wlPM_AdapterG*kc*NSAG) + ∑pPM-MonitorS + ∑pPM-AdapterS + pIVShLib + ∑pIVSpLib,

kde

TWL - pracnost celého projektu v jednotce člověkoden (MD),

wlPMPD - pracnost potřebná k vytvoření generických datových a programových struktur v PMPD,

wlPM_MonitorG - pracnost na vytvoření jednoho generického Monitoru,

wlPM_AdapterG - pracnost na vytvoření jednoho generického Adaptéru,

wlPM_MonitorS - pracnost na vytvoření jednoho specifického Monitoru rozdílná v závislosti na typu služby,

wlPM_AdapterS - pracnost na vytvoření jednoho specifického Adaptéru rozdílná v závislosti na typu služby,

kc - koeficient konfigurace potřebný pro použití a nakonfigurování generického adaptéru pro další službu,

NSMG - počet služeb, u kterých bude využit generický Monitor,

NSAG - počet služeb, u kterých bude využit generický Adaptér,

[8] Vista je definovaná struktura pro ukládání zpracovaných dat

pIVShLib - pracnost na vytvoření sdílených InfoVista knihoven, které jsou použity více službami,

pIVSpLib - pracnost na vytvoření specifických InfoVista knihoven, které jsou použity pouze pro jednu službu, pracnost je rozdílná v závislosti na typu služby a počtu měřených specifických indikátorů.

Pozn.: Pracnost na vytvoření Zdrojů (PM-Sources) není kalkulována, protože není součástí projektu a je plně hrazena stranou odběratele.

6.3.3.5 Požadavky na hardware, software a databáze

Server	Hardwarové požadavky	Plánované softwarové komponenty
S1 – Produkční protředí E2E InfoVista runtime komponentový server	Sun Solaris platform 2CPU >1.1GHz rozšiřitelná do 48GB RAM, 2x72GB internal disk FC, SAN disk space 100GB	SŘBD Oracle 10g InfoVista Foundation Kit skripty na sběr dat z koncových systémů
S2 – Vývojové & testovací prostředí E2E InfoVista workshop komponentový server	Sun Solaris platform 2CPU >1.1GHz 8GB RAM, 2x72GB interní HDD FC, SAN disk space 100GB	SŘBD Oracle 10g InfoVista workshop InfoVista server VistaBridge
WW1-WW8 (8x) – Produkční prostředí pro Tevron Citratest APM Monitor	Windows/Intel, 1CPU 2Gz+, 1GB RAM	Tevron Citratest APM monitor
W9 (1x) - Vývojové prostředí pro Tevron Citratest APM Monitor a specifické testery (.NET)	Windows/Intel, 1CPU 2Gz+, 1GB RAM	Tevron Citratest APM monitor
WL1 - WL3 (3x)	Linux Debian/Intel 1CPU 2Gz+, 1GB RAM	Generické i specifické testery využívající přednosti platformy UNIX

Tabulka 6-2 - HW, DB a SW požadavky pro systém řízení výkonnosti

Legenda:

S – Server,

WW - Workstation Windows (Pracovní stanice s O.S. Windows XP sloužící jako tester, běží na ní roboti testující front-end část aplikací a specifické testery na platformě .NET),

WL - Workstation Linux (Pracovní stanice s O.S. Linux Debian sloužící k provozu specifických testerů závislých využívající prostředí O.S. Linux),

APM - Application Performance Monitoring (Nástroj sloužící k monitoring výkonnosti aplikací - robot),

Tevron Citratest - název produktu spadajícího do kategorie APM umožňující simulaci chování koncového uživatele v předem definovaných intervalech.

6.3.4 Projekt Monitor

Projektem Monitor bude vytvořena platforma pro monitoring dostupnosti a výkonnosti vybraných služeb. Touto platformou bude dosaženo následujících cílů:

- poskytnout prostřednictvím testů E2E definované výkonnostní charakteristiky (čas odezvy, zatížení, doba trvání transakcí, úspěšnost transakcí apod.) vybraných aplikací, služeb a business procesů,
- poskytnout on-line reporty výkonnosti koncovým uživatelům (business vlastníci služeb, servisní manažeři a aplikační administrátoři),
- poskytnout vazbu E2E výkonnostních charakteristik na odpovědnosti jednotlivých pracovních skupin provozu IT a TSCZ,
- integrovat monitoring se stávajícím dohledem služeb z hlediska fault managementu (integrace ve formě doručení alarmu do FM platformy v případě, že naměřené hodnoty indikátorů překročí definované prahové hodnoty),
- implementovat notifikaci prostřednictvím SMS a e-mailu koncovým uživatelům dle předem stanovených prahových hodnot.

Systém Monitor pokryje následující typy KPI:

- aktivní testování jednotlivých aplikací tak, aby testy simulovaly chování koncových uživatelů (zpravidla testování front-end části aplikací na indikátory typu: doba odezvy, dostupnost aplikace, doba stažení webové stránky aplikace, doba nutná pro přihlášení k aplikaci, doba nutná pro odhlášení, měření doby individuálních akcí v závislosti na typu aplikace, úspěšnost akcí apod.),
- pasivní monitoring výkonnosti aplikací a systémů formou sběru dat o jednotlivých transakcích a operacích provedených ve zdrojovém systému a jejich následné korelace a agregace (nejčastější indikátory jsou např. délka trvání transakce, úspěšnost a neúspěšnost transakcí vyjádřená poměrovou veličinou, počty úspěšných a neúspěšných transakcí vyjádřené absolutními čísly, počty otevřených a uzavřených transakcí v systému apod.),
- monitoring výkonnosti business a systémových procesů (bude implementován pomocí sběru, korelace a agregace zpráv z middleware a jejich následná korelace z daty z koncových systémů, součástí je i analýza kvality datových toků mezi jednotlivými back-end systémy).

6.3.5 Požadavky na funkcionalitu

Transakcí se z pohledu monitorování výkonnosti chápe proces začínající založením požadavku v transakčním systému (např. operátorem TMCZ), pokračující zpracováním ve všech relevantních subsystémech (subtransakce) a končící výsledným stavem požadavku. Za účelem komplexního pohledu na celou transakci je požadováno získávat monitorovací data jak o transakci jako celku, tak i o jednotlivých dílčích subtransakcí. Pro účely monitorování transakčních systémů je vyžadován výpočet a prezentace údajů jak z krátkodobého, tak z dlouhodobého hlediska, tzn. výpočet a prezentace výsledků by měla probíhat s následujícími časovými granularitami:

- měření a výsledky v reálném čase (15 minutové vzorky dat),
- hodinové vzorky (měření či agregace 15 minutových vzorků dat),
- denní vzorky (měření či agregace hodinových vzorků dat),
- týdenní (agregace hodinových vzorků dat)

V rámci monitorování výkonnosti by měly být sledovány následující typy výkonnostních indikátorů dle jednotlivých druhů požadavků:

Celkové statistiky transakce jako celku:

- počet nově přijatých resp. otevřených transakcí za příslušnou časovou periodu (reálný čas - 5 či 15 minut, hodina, den, týden, měsíc, rok),
- počet úspěšně obsloužených požadavků transakčním systémem za příslušnou časovou periodu,
- počet chybně zpracovaných požadavků transakčním systémem za příslušnou časovou periodu,
- počet úspěšně obsloužených požadavků do určitého počtu hodin od založení požadavku za příslušnou časovou periodu,
- průměrná, maximální a minimální doba zpracování v rámci transakce za příslušnou časovou periodu.

Statistiky pro jednotlivé subtransakce:

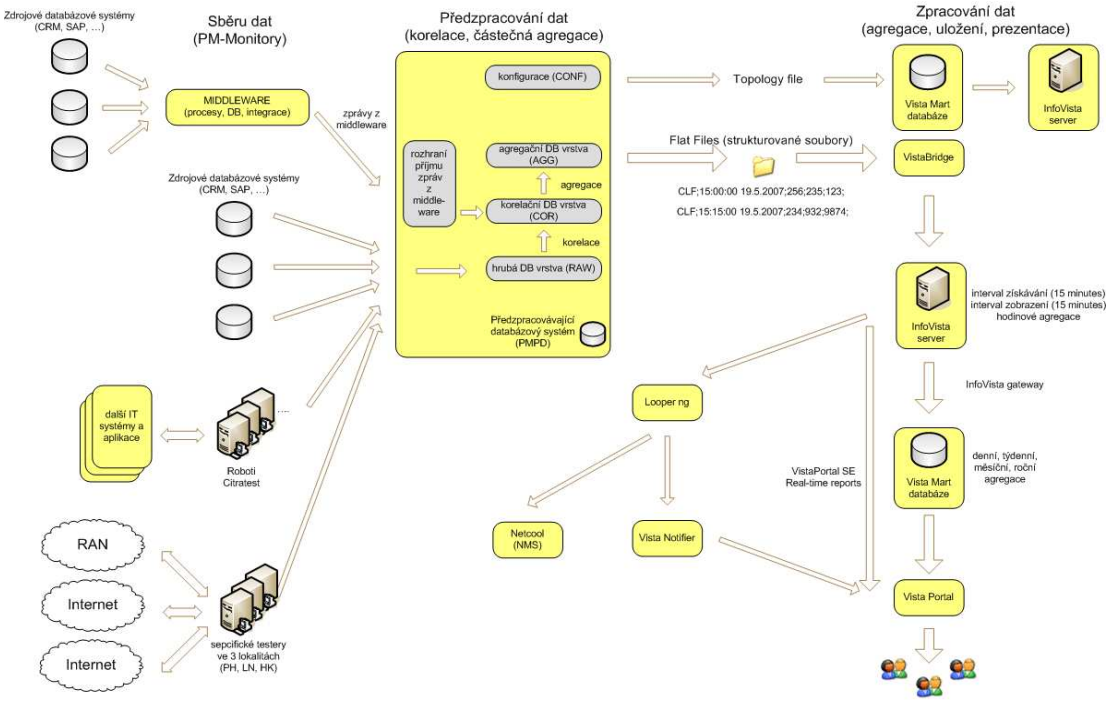
- počet nově přijatých resp. otevřených požadavků v rámci subtransakce za příslušnou časovou periodu (reálný čas – 5 či 15 minut, hodina, den, týden, měsíc, rok),
- počet úspěšně obsloužených požadavků v rámci subtransakce za příslušnou časovou periodu,

- počet chybně zpracovaných požadavků v rámci subtransakce za příslušnou časovou periodu,
- průměrná, maximální a minimální doba zpracování požadavku v rámci subtransakce za příslušnou časovou periodu.

Nad všemi indikátory bude možné nastavit prahové (mezní) hodnoty, jejichž dosažení u příslušného indikátoru, signalizuje problémy transakčního systému resp. subsystému. V případě překročení prahových hodnot musí být monitorovací systém schopen odeslat odpovídající notifikaci ve formě SNMP zprávy do fault management systému. Naměřené hodnoty musí být graficky reprezentovatelné v krátkodobém i dlouhodobém časovém horizontu. Hodnoty musí být dále exportovatelné do různých formátů pro účely dalšího zpracování výsledků.

6.3.6 Návrh architektury systému

Na Obr. 6-6 je znázorněn detailní návrh architektury systému monitorování business aplikací, služeb a business procesů na TMCZ. Celý systém je rozdělen na 3 základní fáze, kterými prochází životní cyklus monitorovacích dat. Každá fáze je technologicky zabezpečena jednotlivými softwarovými komponentami, které jsou spolu provázány integračními moduly.



Obr. 6-6 - Detailní architektura systému monitorování

6.3.6.1 Funkcionality fáze sběru dat

Fáze sběru dat je primárně určena k periodickému získávání hodnot KPI pro jednotlivé služby specifikovaných v analýze monitorování. V závislosti na typu a charakteru služby jsou v rámci fáze sběru dat prováděny následující typy operací a měření:

- aktivní testování - testují se zpravidla front-end části aplikací na indikátory typů doba odezvy, dostupnost aplikace, doba stažení specifikované webové stránky v rámci aplikace, doba potřebná pro přihlášení k aplikaci, doba potřebná pro odhlášení, doba potřebná pro provedení individuálních operací v závislosti na typu aplikace (např. vyhledání zákazníka, založení požadavku atd.), úspěšnost provedení operace apod.,
- pasivní monitoring - výkonnost některých služeb či aplikací je zjišťována formou sběru dat o jednotlivých transakcích v back-end částech zdrojových systémů; nejčastější indikátory pasivního monitorování jsou počty otevřených, uzavřených, úspěšných a neúspěšných transakcí vyjádřené absolutními čísly, úspěšnost a neúspěšnost transakcí vyjádřené poměrovými veličinami, délka trvání transakce apod.,
- monitorování výkonnosti systémové časti business procesů - systémové části business procesů jsou charakteristické tím, že přesahují hranice jedné služby či systému. Systémová část business procesu je založena na informačním toku, který slouží k interakci mezi jednotlivými back-end systémy, které jsou zapojeny do části business procesu. Tyto informace jsou přenášeny ve formě strukturovaných zpráv prostřednictvím procesů na vrstvě middleware. Monitorování je tedy založeno na sběru, korelaci a agregaci zpráv z middleware řešení.

6.3.6.2 Technologické zajištění fáze sběru dat

V této kapitole jsou podrobněji popsány technologie, kterými je zajištěna implementace sběru monitorovacích dat. Technologie sběru dat jsou rozděleny dle typu měření analogicky tak, jak jsou rozděleny v kapitole *6.3.6.1 Funkcionality fáze sběru dat*.

Aktivní monitorování je zajištěno několika možnými způsoby, které závisí na charakteru a povaze monitorované aplikace či služby. Většina front-end částí monitorovaných aplikací je testována prostřednictvím simulačních testů

definovaných v programu Tevron Citratest, což je softwarový robot umožňující vytvořit scénář, který následně simuluje v předem definovaném intervalu (nejčastěji každých 15 nebo 5 min.) chování koncového uživatele. Scénář je rozdělen do několika kroků, jejichž úspěšnost provedení a délka trvání je měřena a následně uložena k dalšímu zpracování do předzpracovávající databáze. Následující kroky jsou typickou názornou ukázkou scénáře v aplikaci Marketing Manager, která je spolu s ostatními předmětem monitorování:

1. start klientské aplikace (robot klikne v prostředí O.S. Windows XP na Start – Programy – CitrixApplication – MarketingManager),
2. přihlášení do klientské aplikace (robot vyplní testovací jméno a heslo k aplikaci),
3. test individuální akce „Hledat firmu“ v rámci aplikace (robot klikne v menu na položku „Data“, dále „Hledat firmu“, vyplní testovací název firmy a potvrdí stisknutím klávesy „Enter“),
4. odhlášení od aplikace (robot se odhlásí od klientské aplikace).

Součástí scénáře jsou i definované časové limity (timeouty) pro jednotlivé kroky scénáře i pro scénář jako celek. Takto definovaný scénář je pravidelně spouštěn a prováděn prostřednictvím plánovače úloh v systému Windows XP. Výsledky měření jsou po skončení běhu scénáře zapsány prostřednictvím ODBC konektoru do raw struktur předzpracovávající databáze. Jelikož robot využívá grafické objekty operačního systému, může současně testovat pouze jeden scénář, a proto je třeba důkladně plánovat jeho zdroje. Při typické délce jednoho scénáře 2 – 3 minuty a intervalu spouštění 15 minut, je tedy možno jedním robotem implementovat 5 – 7 scénářů. V rámci monitorování je pro produkční prostředí navrženo dle kapitoly *6.3.3.5 Požadavky na hardware, software a databáze* 8 pracovních stanic s 8 roboty, což plně pokrývá potřeby počtu scénářů pro jednotlivé služby.

Některé testy aktivního monitorování není možné z různých např. licenčních důvodů provádět robotem Citratest. Typickým příkladem je služba ISS (Integrated Shop System), kde je potřeba testovat stažení stránky aplikace umístěné na ISS serveru v Praze z několika desítek serverů umístěných v městech po celé České republice všude tam, kde jsou značkové prodejny TMCZ. V takovém případě není možné nainstalovat roboty na všechny servery, a proto je k monitorování použit specificky implementován tester na platformě .NET, který následně distribuován na všechny prodejny. Tester je pak prostřednictvím fault management komponenty

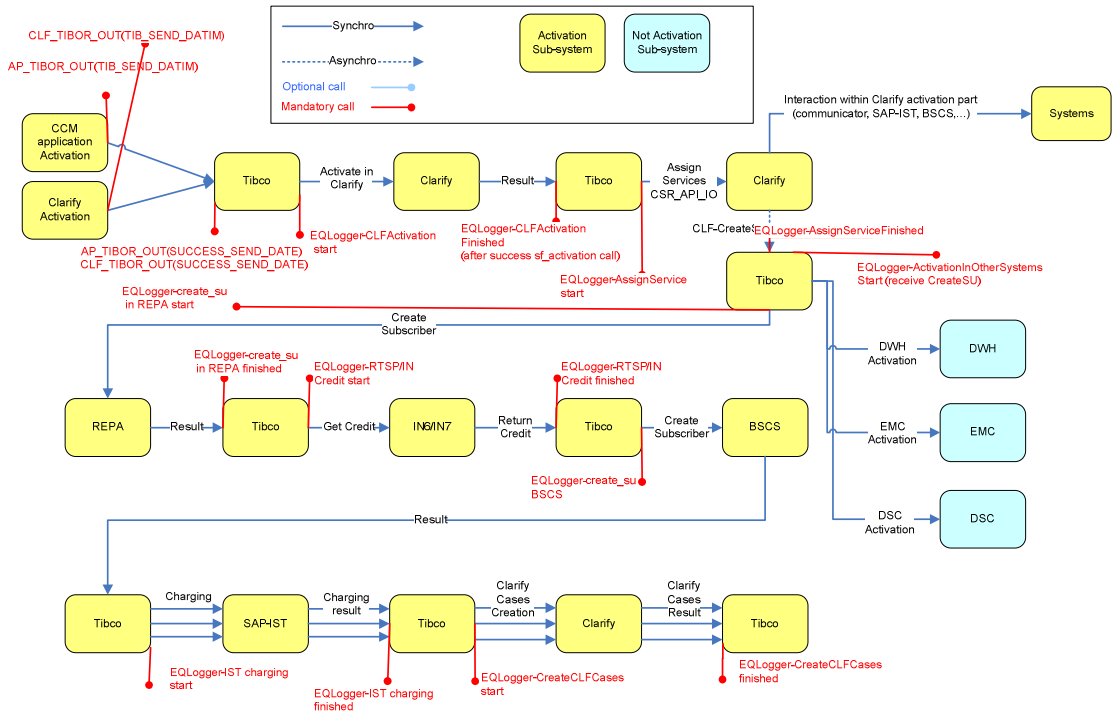
SSM agenta periodicky spouštěn a test prováděn. Jako integrační komponenta pro doručení výsledků z několika desítek serverů umístěných v prodejnách TMCZ je použita webová služba nakonfigurovaná tak, aby uložila výsledky měření do raw struktur předzpracovávající databáze. Dalšími typy aktivních monitorovacích testerů jsou takové testery, které testují nějaké specifické služby či technologie, jakými jsou například WAP či Downloads (služba sloužící ke stažení různorodého obsahu – Java hry, loga apod. prostřednictvím SMS, MMS a WAPu), které nejsou podporovány aplikací Citratest. Tyto testery jsou implementovány na platformě Linux/Java/Perl a jsou rozmístěny na 3 pracovních stanicích v lokalitách Praha, Hradec Králové a Louny. Testery pak ukládají své výsledky přímo připojením do předzpracovávající databáze.

Pasivní monitorování tj. sběr informací o prováděných transakcích ze zdrojových transakčních systémů je ve většině případů implementován pomocí PL/SQL programů, které jsou uloženy v raw vrstvě předzpracovávající databáze a periodicky spouštěny v předem definovaném časovém intervalu (nejčastěji 15 minut). Tyto programy pak prostřednictvím databázových spojení se zdrojovým databázovým systémem získávají data o transakcích za posledních 15 minut a ukládají je do raw struktur předzpracovávající databáze. V případech, kde není možné z různých důvodů použít databázové spojení jsou implementovány speciální datové pumpy (nejčastěji naprogramované v jazycích Java a Perl), které mají za úkol analogicky získat data o transakcích ze zdrojového systému a uložit je do předzpracovávající databáze.

Monitorování business procesů je implementováno na základě příjmu, korelace a agregace zpráv z Tibco middleware. Tibco middleware je robustní systém umožňující propojení jednotlivých back-end systémů, jakými jsou např. CRM, Datové sklady, ERP, systém dobíjení předplacených SIM karet atd. Řešení middleware se používá v organizacích s vysokým stupněm heterogenity platforem. Propojení je založeno na zasílání strukturovaných zpráv. Prostřednictvím Tibco Randevous[9] produktu jsou zprávy v XML nebo enterprise formátu směrovány ze zdrojového back-end systému do cílového back-end systému. Zprávy v XML formátu v rámci definovaných business procesů podléhají XSLT transformacím.

[9] Tibco Randevous je nejstarším produktem z rodiny Tibco implementující transparentní messaging systém postavený na protokolu UDP.

K návrhu a implementaci procesů je použit software Tibco Business Works, což je v podstatě distribuovaný workflow engine. Propojením více business systémů vzniká workflow business procesu. Workflow jako celek i jednotlivé jeho části jsou předmětem monitorování. Na Obr. 6-7 je graficky znázorněn proces *Aktivace* včetně měřících bodů v rámci monitorování.



Obr. 6-7 - Ukázka workflow systémové části business procesu Aktivace

Jednotlivé Business Works procesy je nutné modifikovat tak, aby posílaly vybrané zprávy týkající se vybraných workflow do předzpracovávající databáze tak, aby bylo možné měřit délky trvání, úspěšnosti transakcí a subtransakcí. V předzpracovávající databázi je instalováno vstupní API nazvané TIBOR, což je sada databázových struktur, funkcí a procedur umožňující příjem velkého počtu[10] takto strukturovaných zpráv. V rámci předzpracovávající databáze je implementována komponenta Tibco procesor, který slouží k vyčítání zpráv ze vstupního API a jejich následné korelace do korelačních struktur. Procesor je detailně popsán v rámci technologického zabezpečení fáze předzpracování dat.

[10] V rámci monitorování systémových částí obchodních procesů jsou přijímány statisíce až miliony Tibco zpráv za den. Z toho vyplývá, že práce se vstupním API je režijně velmi náročná.

6.3.6.3 Funkcionality fáze předzpracování dat

V této podkapitole jsou popsány hlavní úkoly, které jsou řešeny v rámci fáze předzpracování dat.

Hlavním úkolem fáze předzpracování dat je příjem naměřených pětiminutových, desetiminutových nebo patnáctiminutových vzorků dat, jejich korelace a parciální agregace. Parciální agregace zajišťuje počítání maximálních, minimálních a průměrných hodnot výkonnostních indikátorů otevřených, uzavřených, úspěšných, neúspěšných transakcí, úspěšnosti, neúspěšnosti a dostupnosti již na úrovni předzpracovávající databáze, protože v rámci patnáctiminutového vzorku dat lze získat ze zdrojového systému více než jednu transakci[11]. U aktivního monitorování získáváme zpravidla výsledek jednoho E2E testu, a proto zde parciální agregace nemá význam. Přesto však jsou data parciálně agregována, protože se může v budoucnu objevit požadavek na změnu frekvence provádění testů např. z 15 minut na 5 minut. V takovémto případě bychom získali během 15 minut tři naměřené vzorky dat, ze kterých je za předpokladu zpracování dat v patnáctiminutových intervalech nutné spočítat průměrné, maximální a minimální hodnoty.

Výsledky měření jsou ukládány do instancí. Pro každou monitorovanou službu jsou definovány instance, které jsou rozděleny do čtyřech úrovní dle následujícího schématu: ServiceName(název služby) – TransactionName(jméno transakce) – TypeName(název typu transakce) – SubTypeName (název podtypu transakce). Čtyřúrovňové členění transakcí se v praxi ukazuje jako dostatečné.

Dalším úkolem fáze předzpracování dat je uložení a použití dvou typů parametrů zpracování dat:

- prvním typem parametrů jsou tzv. „raw“ parametry, které se používají již v samotné fázi předzpracování dat. Tyto parametry jsou závislé na instancích měření. Způsob uložení parametrů respektuje dědičnost tak, že instance v hierarchii níže dědí hodnoty parametrů z instancí, které jsou v hierarchii úrovní výše, za předpokladu, že nejsou hodnoty parametrů přepsány na nižší

[11] Například v rámci služby REPA, která slouží ke zpracování transakcí dobíjení předplacených SIM karet prostřednictvím TMCZ partnerů (např. bankomaty ČS a.s., GLOBUS terminály, SAZKA terminály apod.), dochází v průběhu dne v rámci intervalu 15 minut k tisícům transakcím ve zdrojovém transakčním systému.

úrovni. Tento typ parametrů slouží zpravidla k rozlišení, zda je transakce úspěšná či nikoliv již na úrovni předzpracování dat. Typickým příkladem takového „raw“ parametru je délka trvání transakce (transactionDuration). V případě, že délka trvání transakce je vyšší než tento raw parametr, je transakce označena za pomalou. Takto pomalá transakce pak negativně ovlivňuje úspěšnost transakčního systému resp. úspěšnost E2E testů,

- druhým typem parametrů jsou prahové hodnoty, které jsou propagovány do fáze zpracování pomocí soboru topologie (Topology File) tak, jak je patrné z Obr. 6-6. Tyto prahové hodnoty pak umožňují zasílání alarmů do fault management systému, popř. emailové či SMS notifikace v případě jejich překročení. Příkladem může být například prahová hodnota pro úspěšnost transakcí definována takto: „Klesne-li úspěšnost transakcí pod 90 %, odešli alarm reprezentující stav menší problém; klesne-li však úspěšnost transakcí pod 80 %, odešli kritický alarm“. Jiným příkladem může být prahová hodnota týkající se délky zpracování transakce či délky trvání E2E testu definovaná následovně: „Překročí-li průměrná doba zpracování transakce resp. trvání E2E testu první prahovou hodnotu 300 sekund, odešli alarm reprezentující stav menší problém; překročí-li průměrná doba zpracování transakce druhou prahovou hodnotu 500 sekund, odešli kritický alarm“,
- zasílání alarmů a notifikací je řešeno prostřednictvím vrstvy zpracování dat v systému InfoVista, konkrétně komponentou Vista Notifier, a proto je jim věnována větší pozornost v následující kapitole. Fáze předzpracování dat je pouze zodpovědná za definici prahových hodnot pro jednotlivé instance a jejich poskytnutí do fáze zpracování.

Posledním úkolem fáze předzpracování dat je pravidelné exportování předzpracovaných a parciálně agregovaných dat do strukturovaných souborů (flat files), které jsou bezprostředně importovány do komponenty VistaMart performance řešení InfoVista.

6.3.6.4 Technologické zabezpečení fáze předzpracování dat

Fáze předzpracování dat je technologicky zabezpečena soustavou databázových struktur (tabulky, pohledy, sekvence atd.) a programů (PL/SQL balíky obsahující funkce a procedury zodpovědné za příjem, korelaci a agregaci dat)

v prostředí SŘBD Oracle 10g. Pro tyto účely slouží jedna instance databáze, která je logicky rozdělena do tří vrstev „raw“, korelační a agregační. Každá vrstva je zodpovědná za specifický typ úkolů. Raw vrstva slouží k příjmu a uložení nezpracovaných monitorovacích dat. Korelační vrstva má za úkol provést korelaci dat takovým způsobem, aby bylo možné data parciálně agregovat. Korelace je prováděna:

- u služeb, kde jsou data získávána z více datových zdrojů,
- u služeb, kde charakter měření tuto korelaci vyžaduje (např. data je nutné transformovat z řádku do sloupců (data pivoting), tak aby bylo možné odečíst začátky a konce transakcí za účelem zjištění délek trvání apod.),
- u služeb využívajících Tibco middleware, Tibco zprávy jsou přijímány a následně korelovány do korelační tabulky. Jedna Tibco zpráva reprezentuje začátek subtransakce a jiná představuje konec subtransakce. Tyto zprávy je tedy třeba korelovat za účelem zjištění délky trvání subtransakce a transakce jako celku.

Agregační vrstva provádí parciální agregaci, tj. spočítání maximálních, minimálních a průměrných hodnot jednotlivých výkonnostních indikátorů v rámci agregačního intervalu. Dojde-li v rámci jednoho agregačního intervalu k získání dat o více než jedné transakci, což je typické pro pasivní monitoring, je nutné data parciálně agregovat.

Následující text popisuje implementační pravidla a notace pro zajištění předzpracování dat v rámci předzpracovávající databáze. V databázi jsou uloženy databázové objekty, které tvoří tabulky, pohledy, sekvence, triggery, databázové linky (spojení do zdrojových databázových systémů), synonyma a balíky obsahující procedury a funkce. Objekty jsou rozděleny na generické a specifické. Generické objekty jsou sdíleny předzpracováním dat pro více služeb a naopak specifické objekty náleží konkrétním službám. Objekty, jejichž název obsahuje prefix „G_“ jsou generické jako například tabulka obecných parametrů G_PARAMS, kde jsou uloženy generické parametry všech služeb. Specifické objekty pak obsahují ve svém názvu jeden z prefixů „R_“, „C_“ nebo „A_“. Objekty, jejichž název obsahuje prefix „R_“ jsou objekty, které z hlediska výše zmíněné metodiky zpracování patří do „raw“ vrstvy. Jedná se zpravidla o tabulky sloužící k uložení nově přijatých nezpracovaných dat, pohledy umožňující výpočet výkonnostních indikátorů a balíky, které zajišťují příjem dat ze zdrojových systémů. Objekty, jejichž název obsahuje

prefix „C_“ náleží korelační vrstvě. Jedná se obdobně o korelační tabulky, pohledy a balíky, které zajišťují datovou korelaci. Posledním typem objektů jsou objekty s prefixem „A_“ náležící agregační vrstvě. Do agregačních tabulek jsou agregačními procedurami a funkcemi pro jednotlivé služby ukládány parciálně agregovaná data, která jsou následně z těchto tabulek exportována do strukturovaných souborů.

Velmi významným rysem předzpracovávající databáze je funkcionalita, která umožňuje získat data ze zdrojového systému i po obnovení v rámci případného výpadku. Tato funkcionalita je nejvíce využívána u pasivního monitorování, kde jsou data o transakcích získávána ze zdrojových databázových systémů prostřednictvím databázových spojení. Za předpokladu, že je zdrojový systém nedostupný, nebo že dojde k přerušení síťového spojení mezi serverem, kde reziduje předzpracovávající databáze a serverem hostujícím zdrojový databázový systém, není možné v reálném čase získat data o prováděných transakcích, a proto tak zajistit monitoring v reálném čase. Poté, co dojde k obnovení síťového spojení či obnovení výpadku zdrojového systému, je možné transakce, které náleží do předchozích časových intervalů zpětně získat a doručit k předzpracování tak, aby nedošlo k výpadku v měření. Dle nastavení parametru maximální doby zpracování (maxProcessing) v minutách, se pak každý následující interval zpracují data za více časových intervalů odpovídajícím tomuto parametru a tím je možné „dohnat“ zpracování do reálného času tak, aby nevznikla žádná mezera v měření.

Tuto funkcionalitu je možné demonstrovat na následujícím příkladu. Ze zdrojového systému jsou transakční data sbírána, korelována a agregována předzpracovávající databází PMPD v pravidelných patnáctiminutových intervalech. Poslední úspěšný běh funkce zajišťující načtení a sběr dat proběhl v 3:30 ráno. Poté došlo v 3:38 k výpadku síťového spojení mezi servery hostující zdrojový systém a PMPD. V 3:45, tj. další plánovaný čas běhu předzpracování dat, zjistila funkce PMPD, že není funkční spojení do zdrojového systému. Běh funkce byl ukončen a do operačního logu funkce oznámila tuto skutečnost. Takto se děje každých 15 minut při spuštění této funkce. Jelikož nedošlo k úspěšnému získání zdrojových dat, nebylo možné provést korelaci ani agregaci, tj. čas poslední korelace i agregace se zastavil v čase 3:30. Po obnovení výpadku spojení v 4:24, tj. za necelou hodinu, dojde v 4:30 ke spuštění funkce zodpovědné za sběr dat. Funkce zjistí, že v době spuštění je již o hodinu více a poslední data jsou hodinu stará. Na základě parametru maxProcessing, který je nastaven na 60 minut, funkce provede sběr dat 4x

po sobě (4x 15 minut) tak, aby „dohnala“ ve zpracování výpadek spojení. Korelace a agregace se zachovají obdobně a tím dojde v jednom běhu k exportu 4 strukturovaných souborů obsahující předzpracovaná data za poslední hodinu zpět. V dalších bězích již proběhnou všechny vrstvy předzpracování standardně. Konzistence dat je v rámci jejich předzpracování kromě databázových omezeních řízena soustavou parametrů rozdělených dle vrstev zpracování.

6.3.6.5 Funkcionality fáze zpracování dat

Hlavní úkoly fáze zpracování dat jsou následující:

- příjem předzpracovaných dat (předzpracované pěti, deseti patnáctiminutové, u některých služeb hodinové vzorky dat),
- další zpracování v podobě agregace do hodinových, denních, týdenních měsíčních a ročních dat. Hodinová data jsou agregována z pěti, deseti nebo patnáctiminutových vzorků dat. Služby, které mají nejmenší granularitu předzpracování 1 hodinu jsou ve fázi zpracování nejprve agregovány do denních vzorků,
- prezentace dat v reálném čase v podobě real-time grafických reportů (období dat od současnosti 24 hodin zpět). V těchto reportech jsou skutečně vidět naměřené a předzpracované hodnoty pěti, deseti a nejčastěji patnáctiminutových vzorků dat,
- uložení, archivace a prezentace dat starších než real-timeových do datového skladu; data jsou prezentována v podobě detailních reportů.

6.3.6.6 Technologické zabezpečení fáze zpracování dat

Fáze zpracování dat je zabezpečena z převážné části specializovaným performance management řešením InfoVista Foundation. Některé další úlohy, jakými jsou např. importování předzpracovaných dat, importování topologického souboru obsahující parametrizaci pro všechny monitorované služby apod., jsou zabezpečeny menšími integračními programy na platformách Perl, Java a Unix Shell. InfoVista Foundation v rámci projektu monitorování služeb, aplikací, datových toků a business procesů je tvořena několika základními komponentami: VistaBridge, InfoVista server, VistaMart, InfoVistaGateway, InfoVista Portal, VistaCockpit a VistaNotifier. Tok zpracování dat je nejlépe zřejmý z *Obr. 6-6 - Detailní architektura systému monitorování*. Bezprostředně po exportu předzpracovaných dat

do strukturovaných souborů (flat files) jsou tyto importovány do komponenty VistaBride, která je zodpovědná za jejich korektní příjem. Následně jsou data předána InfoVista serveru, který poskytuje data pro real-time reporty. InfoVista server vytvoří z patnáctiminutových vzorků hodinové agregace, které jsou pomocí komponenty InfoVista Gateway odeslány do části VistaMart, kde dojde k uložení a archivaci těchto dat. Veškerá naměřená on-line data, včetně těch agregovaných jsou dostupná svým uživatelům v prostředí webového InfoVista Portálu, kde jsou data zobrazena ve formě displetů (obdoba portletů, servletů v teorii informačních portálů). VistaCockipt je komponenta hrající úlohu dispečera, který řídí jednotlivé datové toky a spouští jednotlivé komponenty. VistaNotifier slouží ke generování alarmů v případě překročení stanovených prahových hodnot pro jednotlivé výkonnostní indikátory. Tyto alarmy jsou pak následně doručeny v podobě SNMP trapů na mttrapd sondu v rámci integrace s fault management systémem Netcool. Takto generované alarmy mohou být po patřičném nakonfigurování zdrojem pro emailovou a SMS notifikaci, která je součástí celého monitorovacího řešení.

6.4 Zhodnocení případové studie

Rozšíření původního systému stavového monitorování o E2E a transakční monitoring vybraných služeb poskytuje spojité informace o výkonu a dostupnosti monitorovaných služeb. Díky nasazení tohoto typu monitoringu lze měřit výkonnost a dostupnost celé služby za delší časové období. Monitorovací rámec navržený ve 3 fázích a předzpracování ve 3 vrstvách plně respektuje metodu monitorování a umožňuje tak efektivně získávat hodnoty KPI, které jsou definované v analytické fázi ve spolupráci s business vlastníky daných služeb. V praxi se ukázalo, že původní požadavek a záměr monitorovat touto metodou pouze technologické části služeb, byl záhy rozšířen o požadavek na monitoring i dalších částí, jakými jsou např. lidské zdroje, marketingové a business KPI. Příkladem business KPI může být poměr zákazníků, kteří v rámci průběhu nějakého business procesu zrušili objednávku na službu či produkt vůči těm, kteří ji potvrdili a dokončili. Podmínkou pro nasazení monitoringu výše zmíněného je existence dat, ze kterých lze požadovaná KPI změřit.

7 Závěrečné shrnutí

Hlavním cílem práce bylo navrhnout metodu zavádění monitorování aplikací, služeb a business procesů v rámci vybraných oblastí podpory jejich řízení na taktické a operativní úrovni. Mezi hlavní oblasti řízení byla vybrána řízení výpadků a řízení výkonnosti, která jsou často nazývána mezi odbornou veřejností jako fault a performance management.

Dílčím cílem disertační práce bylo metodu aplikovat na případové studii zavedení monitorování aplikací, služeb a business procesů pro vybranou telekomunikační společnost.

Splněním hlavního cíle došlo k tomu, že navržená metoda monitorování má strukturu, kterou lze shrnout v následujících bodech:

1. Vytvoření metody na základě vybraného metodického rámce ITIL determinuje její procesní podobu. Metoda definuje proces nasazení monitorování, který se skládá z dvou dílčích procesů:
    a. procesu stavového monitorování - popisující nasazení nástroje oblasti řízení výpadků, který umožňuje monitorovat infrastrukturní části předmětné služby: metriky hardware, operační systém, síťové prvky, databáze, aplikační procesy atd.
    b. procesu transakčního monitorování - popisující nasazení nástroje pro oblast řízení výkonnosti transakcí, který umožňuje monitorovat funkčnost služby z hlediska schopnosti obsluhovat požadavky uživatelů - transakce. Vzhledem k podobné povaze získávaných dat je v rámci tohoto dílčího procesu popsáno i nasazení monitorování z pohledu koncového uživatele (E2E), kde jednotlivé transakce představují E2E testy.
2. Metoda je tvořena soustavou logicky na sebe navazujících aktivit, přičemž pro každou aktivitu procesu jsou definovány její:
    a. vstupy,
    b. výstupy,
    c. nástroje a techniky,
    d. role,
    e. odpovědnosti.

Pro vizuální znázornění metody je použit jako nástroj vývojový diagram.

3. V rámci dílčího procesu stavového monitorování jsou navrženy nezbytné výstupy v podobě dokumentů, jejichž šablony jsou uvedeny v přílohách C, D:
    a. Analytický dokument služby - klíčový dokument obsahující analýzu a technický návrh monitorování vybrané služby,
    b. Dokument specifikace metrik - dokument obsahující seznam definovaných metrik a jejich parametrů, které jsou předmětem stavového monitorování,
4. V rámci dílčího procesu transakčního monitorování jsou navrženy nezbytné výstupy v podobě dokumentů, jejichž šablony jsou uvedeny v přílohách E, F, G:
    a. Dotazník služby - slouží k získání prvotních informací o službě ve strukturované formě,
    b. Analytický dokument služby - klíčový dokument obsahující analýzu a technický návrh monitorování vybrané služby,
    c. Dokument specifikace KPI - dokument obsahující seznam a popis definovaných KPI, které jsou předmětem transakčního monitorování.
5. Metoda je integrována do metodického rámce prostřednictvím vazeb jejích vstupů a výstupů s procesy metodického rámce.

Před samotnou tvorbou metody monitorování byl proveden teoreticko-vědecký výzkum předmětné oblasti týkající se dostupných metodických rámců pro řízení IS/ICT a poskytování ICT služeb. V rámci předmětné oblasti byly vybrány a popsány rámce CMM, EUP, ITIL a COBIT, ze kterých byla vybrána metodika ITIL, na které je metoda založena. Výsledkem studia předmětné oblasti je, že existuje celá řada technologických nástrojů pro zajištění monitoringu, avšak neexistuje žádný obecný, univerzální postup popisující nasazení a provoz monitorování v podniku. Metoda monitorování poskytuje systematický postup zavádění monitorování, který vede k časově a zdrojově efektivnější realizaci.

Dílčí cíl disertační práce se podařilo naplnit tak, že metoda monitorování byla aplikována v rámci případové studie úspěšného nasazení transakčního a E2E monitorování služeb ICT ve vybrané telekomunikační společnosti. V případové studii je nejprve zanalyzována výchozí situace stavu monitoringu služeb ICT v této

organizaci, následně je podle metody navrženo a realizováno řešení spočívající v rozšíření stavového monitorování o transakční a E2E monitorování vybraných 45 služeb. V rámci návrhu je nejprve proveden počáteční výzkum sloužící k získání základních obchodně-technických informací (včetně požadovaných KPI) o vybraných službách formou strukturovaného dotazníku, poté jsou popsány požadavky na funkcionalitu monitorování a navržena architektura systému monitorování dle nové metody tak, že je monitoring nasazen ve třech fázích: sběr, předzpracování a zpracování monitorovacích dat. Předzpracování, klíčová část v celém procesu, je provedeno ve třech vrstvách: hrubé, korelační a agregační vrstvě, kterými procházejí monitorovací data v jeho průběhu tak, jak je popsáno v nové metodě. Před implementací monitoringu každé služby bylo nutné vyplnit tři klíčové dokumenty celého procesu: dotazník služby, analytický dokument služby a dokument specifikace metrik, které slouží po jejich schválení zodpovědnými osobami jako vstupní informace pro implementaci monitoringu dané služby.

Stanovení hlavního cíle práce vedlo k definici a popsání metody zavádění monitorování pouze pro vybrané disciplíny řízení IS/ICT, kterými jsou řízení výpadků a řízení výkonnosti, dle dostupných informací z oboru, nejvýznamnější oblasti řízení a správy ICT. Metoda v současné podobě nepopisuje nasazení dalších nástrojů z oblastí řízení IS/ICT, jakým je například bezpečnostní monitorování, jehož nasazení by bylo přínosné do metody v budoucnu zapracovat.

8 Použité zdroje

[1] BAILEY, J. T. - HEJDY S. R. *Why Is Total Cost Of Ownership (TCO) Important?* [on-line]. c2003-11. <http://www.darwinmag.com/read/110103/question74.html>.

[2] BARTOŇ, P. *Provoz jednotného dohledu ICT služeb pro ČD a SŽDC provozovaných na telekomunikační infrastruktuře obou subjektů* [online].Vědeckotechnický sborník. ČD č.22. Praha: GŘ ČD a.s., 2006 <http://www.cdrail.cz/VTS/CLANKY/vts22/2210.pdf>.

[3] BASL, J. – NOVOTNÝ, O. *ITIL a Cobit řídí komunikační technologie* [online]. Moderní řízení, Červen 2004. <http://modernirizeni.ihned.cz/1-10005770-14454590-600000_detail-84>.

[4] BĚLINA, R. SLA & Dohledový systém: Praktický pohled na propojení byznys služeb a IT infrastruktury – Jak ušetřit peníze? In *Systémová integrace 2001*. *Sborník příspěvků z mezinárodní konference pořádané Českou společností pro systémovou integraci*. ČSSI. 1. vydání. Praha: ČSSI ,2001. s. 206–210.

[5] CARRALI, R.A. – WILSON, R.W. *The Challenges of Security Management* [online]. Software Engineering Institute, 2004. 15 p. <www.cert.org/archive/pdf/ESMchallenges.p df>.

[6] CATHOOR, F., et al. *Power Aware Communications for Wireless Optimized personal Aera Network* [online]. Pacwoman Consortium, October 2002. 92 p. <www.imec.be/pacw oman/Deliverables/WP2/WP2-MOT-D2.1_system_requirements-07-10-2002-V1.0.doc>.

[7] CATHOOR, F., et al. *WP2 - System Architecture and Specifications* [on-line].8.10.2002 [cit. 2007-07-02]. <www.imec.be/pacwoman/Deliverables/WP2/WP2-MOT-D2.1_system_requirements-07-10-2002-V1.0.doc>.

[8] CISCO SYSTEMS INC. *Internetworking Technologies Handbook.* 3rd edition Cisco Press, 2000. 280 s. ISBN 1587050013.

[9] COHEM, Y. *Simple Network Management Protocol* [on-line]. c2007-05 [cit. 2007-05-27]. <http://www2.rad.com/networks/1995/snmp/snmp.htm>.

[10] CONTI, P. – LABETOULLE, J. – MARCUS, C – CHEIKRHOUHOU, M. Network *Management System with Intelligent Agents*. [online]. 1998 [cit 2009-03-28]. <http://www.hpovua.org/PUBLICATIONS/PROCEEDINGS/5_HPOVUAWS/73.pdf>.

[11] DMTF. *Web-Based Enterprise Management (WBEM)* [on-line]. 2008 [cit.2009-03-28]. <http://www.dmtf.org/standards/wbem>.

[12] DOHNAL, J., POUR, J. *Řízení podniku a IS/IT v informační společnosti*. Praha: VŠE, 1999. ISBN 80-7079-023-7.

[13] EDWARDS, A. W. - WHITAKER, R. J. *Simple Fault Management: A Functional View of Root Cause Analysis and Correlation* [on-line]. 2001 [cit. 2007-05-27]. <htttp://www.tavve.com/uploadedFiles/EW_White_Paper.pdf>.

[14] E-ISO. *ISO 27001*. [on-line]. c2006 [cit. 2009-02-16]. <http://www.eiso.cz/poradenstvi/nase-sluzby/ISO-27001/>.

[15] EMF Enhanced Management Framework [online]. c2006. <http://www.tbs-sct.gc.ca/emf-cag/index-eng.asp>.

[16] eTOM enhanced Telecom Operations Map [online]. c1990-2009. <http://www.tmforum.org/BusinessProcessFramework/1647/home.html>.

[17] FRINTS, M. *Possibilities of Peer-to-Peer Technology in Network Management* [online]. December 2006. 55 p. Master Thesis at University of Twente. <http://dacs.ewi.utwente.nl/assignments/completed/master/reports/Thesis_Martijn_Frints.pdf>.

[18] GARTNERS. *2006 Press Release*. [on-line]. 2007. 3p. [cit. 2007-08-27]. <http://www.gartner.com/press_releases/asset_153547_11.html>.

[19] GARTNERS. *Forecast: IT Operations Management Software, Worldwide, 2006-2011*. [on-line]. 2007. 19p. [cit. 27.8.2007]. <http://www.gartner.com/DisplayDocument?id=502102>.

[20] Harris Kern's Computing Institute [online]. c2002. <http://www.harriskern.com>.

[21] HEWLET-PACKARD. *HP OpenView Operations Administrator's Reference*. October 2006.

[22] HEWLET-PACKARD. *HP OpenView Operations Concepts Guide UNIX*. November 2005.

[23] CHARVÁT M., *Poznejte výkonnost svých klíčových systémů a procesů.* Praha: NextiraOne Czech s.r.o., 2008, 3s.

[24] IBM. *Tivoli Netcool/Impact Administration Guide* [online]. Version 5.1. c2008. <http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcoolimpact.doc/imag.pdf>.

[25] IBM. *Tivoli Netcool/OMNIbus documentation* [online]. c2006. <http://publib.boulder. ibm.com /infocenter/tivihelp/v8r1/index.jsp?toc=/com.ibm.netcool_OMNIbus.doc/toc.xml>.

[26] ITGI, COBIT 4.1 Executive Summary and Framework [on-line]. 2007. 29p. [cit. 2008-06-0]. <http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172>.

[27] ITGI. *COBIT 4.1 Executive summary* [online]. c2007. 28 s.<www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=39073>.

[28] JELÍNEK, P. – ŠILD, V. – VOŘÍŠEK, J. Kategorizace a architektury informatických služeb. *Systémová integrace 3/2007*, 2007, roč. XIV, č. 3. ISSN 1210-9479.

[29] KLAŠKA, L. *Správa počítačových sítí* [on-line]. 6.6.2000 [cit. 2007-05-27]. <http://www.svetsiti.cz/view_list.asp?rubrika=Tutorialy&temaID=23>.

[30] KRAMOSIL, P. Monitoring a konsolidace bezpečnostních událostí. *DSM data security management*, 2006, roč. X, č. 5, s.50 - 51. ISSN 1211-8737.

[31] MATUŠKA, M. *Metakonfigurační metoda řízení podnikových komunikací – řízení komunikační infrastruktury*. Praha, 2006. 152 s. Disertační práce na katedře IT, VŠE.

[32] MENDEL, T. – GARBANI, J. P. *IT Management Software Market* [online]. March 2007. 19p.<http://www.forrester.com/Research/Document/Excerpt/0,7211,41738,00.html>.

[33] MICROMUSE. *Netcool/OMNIbus 3.6 Administration Guide*. Version 1.0. c2003.

[34] MICROMUSE. *Netcool/Realtime Active Dashboards 3.0 Administration Guide*. c2006.

[35] MICROMUSE. *Netcool/Webtop 1.3.1 Administration guide* [online]. c2004. <http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_wt.doc_2.0/ag/we131ag.pdf>.

[36] OGC. *ITIL Service Delivery v2.0.* [CD-ROM] London, May 2001 [20.9.2008]. ISBN 9780113308934.

[37] OGC. *ITL Service Support v2.0.* [CD-ROM] London, October 2000 [17.10.2008]. ISBN 0113300158.

[38] PAULK, C.M., et al. The Capability Maturity Model for Software Version 1.1. [online]. Software Engineering Institute, Pittsburgh 1996. http://www.sei.cmu.edu/pub /documents/93.reports/pdf/tr24.93.pdf>.

[39] POMIKÁLEK, J. *Sledování sítě (SNMP, MRTG, Nagios)* [on-line]. [cit. 2007-05-20].<http://www.fi.muni.cz/~kas/p090/referaty/2003podzim/skupina10/snmp.html#motivace>.

[40] POUR, J. – GÁLA, L. – ŠEDIVÁ, Z. *Podniková informatika.* 2., přepracované a aktualizované vydání. Praha: Grada Publishing, 2009. 496s. ISBN 978-80-247-2615-1.

[41] POUR, J. Potřeba změn v řízení IS/IT. In *Systémová integrace 2001*. *Sborník příspěvků z mezinárodní konference pořádané Českou společností pro systémovou integraci*. ČSSI. 1. vydání. Praha: ČSSI, 2001. s. 297–304.

[42] ŘEPA, V. *Podnikové procesy: Procesní řízení a modelování.* 2., přepracované a aktualizované vydání. Praha: Grada Publishing, 2007. 288s. ISBN 978-80-247-2252-8.

[43] SCOTT, W.A. *Introduction to the Enterprise Unified Process* [online]. October 2005, [cit. 8.5.2008]. <www.enterpriseunifiedprocess.com/downloads/eupIntroduction.pdf>.

[44] SKÁLA, J. *CobiT® 4.1 a jeho vztah k ITIL®*. [on-line]. 6.2. 2008. 20p. [cit. 2008-06-10]. <www.itsmf.sk/index.php?option=com_docman&task=doc_view&gid=111>.

[45] UBIK, S. *Trendy v monitorování vysokorychlostních počítačových sítí* [online]. 2007. <www.ist-lobster.org/publications/articles/sdel_tech.pdf>.

[46] UČEŇ, P., a kol. *Metriky v informatice: Jak objektivně zjistit přínosy informačního systému*. 2. vydání. Praha: Grada Publishing, 2001. 140s. ISBN 80-247-0080-8.

[47] VOŘÍŠEK, J. *Model SPSPR* [online]. 2001. <http://nb.vse.cz/~vorisek/FILES/Clanky/2001_SPSPR.htm>.

[48] VOŘÍŠEK, J. Model "SPSR" - model řízení podnikové informatiky. In *Systémová integrácia 2001. Sborník z mezinárodní vědecké konference.* Demanovská Dolina, TU Žilina. 2001. str.5-18. ISBN 8-7100-880-X

[49] VOŘÍŠEK, J. *Strategické řízení informačního systému a systémová integrace.* Vydání 1. Praha: Management Press, 1999. 321s. ISBN 80-85943-40-9.

[50] VOŘÍŠEK, J. *Trendy IS/ICT, na které musí uživatelé a dodavatelé reagovat* [online]. <http://nb.vse.cz/~vorisek/FILES/Clanky/2005_Trendy_ISICT_a_reakce_na_ne.doc>.

[51] W3C. *Extensible Markup Language (XML) 1.0 Third Edition*.[online]. W3C Recommendation, 2004. <http://www.w3.org/TR/2004/REC-xml-20040204>.

[52] W3C. *XSL Transformations (XSLT) 1.0* [online]. W3C Recommendation, 1999. <http://www.w3.org/TR/xslt>.

[53] YUHANNA,N. – GARBANI J.- P. *The DBMS Management Software Market. Focus Shifting To Centralized, Integrated, And Heterogeneous Management* [online]. Forrester Research, June 2007. 4 p. <http://ca.com/files/IndustryAnalystReports/the_dbms_ management_software.pdf>.

9 Seznam použitých pojmů a zkratek

Pojem/Zkratka	Vysvětlení
Architektura monitorování	Architektura monitorování představuje jednotlivé stavební bloky, které vytvářejí systém monitorování. Jedná se o veškerý hardware, databáze, aplikační software a vyvinutý framework potřebný k provozu monitorování služeb IS/ICT.
ACDS	Akceptační dokument služby - dokument obsahující popis akceptačních testů a informací potvrzujících korektní a funkční nasazení monitorování služby (šablona je součástí metody monitorování).
ADS	Analytický dokument služby - dokument popisující analýzu implementace zavedení monitorování konkrétní služby (šablona je součástí metody monitorování).
API	Application Programming Interface - Aplikační programové rozhraní k nějaké softwarové či hardwarové entitě představuje soustavu funkcí, procedur a knihoven, které jsou využity při programování dalších funkcionalit.
ASM	Application Service Monitor - aplikace společnosti IBM/Micromuse rozšiřující funkcionalitu SSM ve formě dalšího sub-agenta tím, že umožňuje monitorovat dostupnost a výkonnost řady komerčních serverových a databázových produktů, jakými jsou například SAP, SŘBD Oracle, IBM WebSphere server apod.
Asset Management	Systémy řízení a správy provozních zdrojů (i neinformatických) organizace. Poskytují evidenci majetku podniku a mají návaznost na ERP aplikace.
Automatizace	Automatizace je funkce centrálního dohledového systému umožňující detekovat změny ve stavu uložených alarmů a vyvolat automatické reakce na tyto změny bez nutnosti zásahu operátora.
BSC	Base Station Controller - funkční komponenta GSM architektury, která je zodpovědná za alokaci radiového zdroje pro mobilní stanici, správu frekvence a přeladění mobilní stanice při přechodu mezi jednotlivými BTS.
BTS	Base Transceiver Station - zařízení v síti GSM umožňující mobilním stanicím komunikovat se sítí GSM.
CI	Configuration Item - konfigurační položka v rámci CMDB.
CIM	Common Information Model - standard definující management informace pro systémy, sítě, aplikace a služby IT.
CMDB	Configuration Management Database - databáze obsahující konfigurační položky komponent infrastruktury IS/ICT.
CMM	Capability Maturity Model - metodika je založená na procesním modelu představující sadu praktik, které popisují základní charakteristiky efektivních procesů v rámci organizace.
COBIT	Control Objectives for Information and Related Technologies - metodika řízení IS/ICT, která se nejvíce zaměřuje na

	strategické řízení podniku.
Configuration Management	Jedna z oblastí rámce ITIL poskytující logický model infrastruktury IS/ICT a na ní provozovaných služeb.
CPU	Central Processing Unit - výpočetní jednotka počítačového systému (procesor).
CRM	Customer Relationship Management - řízení vztahů se zákazníky s cílem maximalizovat loajalitu zákazníků a v důsledku toho i ziskovost podniku. Aplikace CRM stále více využívají potenciálu a možností internetu.
Data	Data jsou jednotkou informací a představují vhodný způsob jejich záznamu, který se může lišit s ohledem na použitou technologii nebo schopnost příjemce (člověk nebo počítač) data vnímat a interpretovat.
DBMS	Database Management System - software pro správu databází.
Deduplikace	Deduplikace je pojem z oblasti stavového monitorování představující nahrazení opakovaného výskytu alarmu pocházejícího ze stejné části infrastruktury (např. ze stejného routeru, serveru apod.) jedním alarmem s uvedením počtu jeho výskytů.
DHS	Definitive Hardware Store - obsahuje náhradní HW součástky udržované na stejné úrovni jako jsou produkční pro případ nutnosti obnovení systémů.
DSL	Definitive Software Library - knihovna, která obsahuje veškeré hlavní kopie instalovaných verzí software a k nim související dokumentace.
DSM	Dokument Specifikace Metrik - dokument obsahující seznam definovaných metrik s jednotlivými parametry (šablona dokumentu je součástí metody monitorování)
E2E monitoring	End To End monitoring - monitorování aplikace či služby z pohledu koncového uživatele simulováním požadavků a transakcí, které by běžně prováděl koncový uživatel.
EMF	Enhanced Management Framework - integrovaný model řízení investic do IT/IM v kanadských vládních institucích (Information Technology/Information Management) obsahující sadu principů, nejlepších praktik, metodik a šablon. Metodika
EMS	Event Management Systems - dohledové systémy pro zpracování událostí a alarmů z infrastruktury.
ERP	Enterprise Resource Planning - Řízení podnikových zdrojů je aplikační software v informačním systému, který umožňuje řízení a koordinaci všech disponibilních podnikových zdrojů a aktivit s cílem zajištění potřeb trhu i vlastního podniku.
eTOM	enhanced Telecom Operations Map - metoda publikovaná TM forem; formou průvodce popisuje celkový rozsah business procesů vyžadovaných poskytovateli služeb; metoda definuje klíčové procesy a prvky a jejich vztahy mezi nimi.
EUP	Enterprise Unified Process - metodika, rozšiřující RUP (Rational Unified Process) zaměřující se na řízení vývoje, provozu a podpory informačních systémů podniku
Fault Management	Oblast řízení IS/ICT představující rozsáhlou skupinu

	automatizovaných funkcí, které mají za úkol odhalit, izolovat a opravit výpadky či defekty v infrastruktuře.
Firewall	Firewall je zařízení sloužící k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení.
Forenzní analýza	Ex-post analýza historických bezpečnostních dat umožňující vyhledání a odhalení případných bezpečnostních incidentů.
FSC	Forward Schedule of Changes - plán budoucích změn obsahující detaily všech změn schválených k implementaci a jejich časový harmonogram.
GSM	Groupe Spécial Mobile - globální systém pro mobilní komunikaci je světovým standardem pro mobilní telefony a sítě.
HR	Human Resources - oddělení pro řízení lidských zdrojů, z informatického hlediska je to aplikace pro řízení lidských zdrojů v podniku.
HTML	Hyper Text Markup Language - hypertextový značkovací jazyk používaný k tvorbě webových stránek a aplikací.
HTTP	Hyper Text Transfer Protocol - internetový protokol z rodiny protokolů TCP/IP určen původně k přenosu hypertextových dokumentů. Rozšířením o další technologie se v současnosti dá použít i k přenosu dalších typů souborů. Spolu se standardem pro přenos dat XML se hojně využívá ve webových službách.
HUB	Rozbočovač je aktivní prvek počítačové sítě s hvězdicovou topologií umožňující její větvení.
IDS	Intrusion Detection System - systém umožňující detekovat narušení bezpečnosti infrastruktury IT. Systém rozumí podstatě síťových protokolů, a tím umožňuje rozpoznat určité signatury, které naznačují bezpečnostní útoky.
ICT	Information and Communication Technologies - Informační a komunikační technologie.
IS/ICT	Information Systems/Information and Communication Technologies - Informační Systémy/Informační a komunikační technologie
ISACA	Information Systems Audit And Control Association - světová organizace zastřešující profesionály z oblasti informačních systémů. Zabývá se auditem, řízením a bezpečností informačních systémů.
ITGI	Information Technology Governance Institute - nezávislá výzkumná instituce založená na konci 80. let, která vyvinula metodický rámec COBIT.
ITIL	Information Technology Infrastructure Library - metodický rámec používaný k řízení IT, který má původ ve vládní instituci ve Velké Británii v 80. letech.
ITOM	IT Operations Management - řízení provozu informačních technologií.
itSFM	information technology Service Management Forum - mezinárodní nezávislá a nezisková organizace účelově se věnující všem aspektům řízení služeb informačních a komunikačních technologií. Standardem pro řízení IS/ICT je

	pro itSFM brán metodický rámec ITIL.
ITSM	Information Technology Service Management - disciplína zabývající se řízením systémů a služeb založených na informačních technologiích.
J2EE	Java 2 Enterprise Edition - přístup k návrhu, vývoji a nasazení vícevrstvých aplikací založených na jazyce Java.
JMAPI	Java Management API - java aplikační programové rozhraní využívané pro tvorbu management aplikací.
JMX	Java Management eXtensions - nahrazuje JMAPI a slouží jako jednotný framework pro vytváření objektově orientovaných management aplikací.
JRMI	Java Remote Method Invocation - vzdálené volání metod programovací platformy Java umožňuje vytvářet distribuované Java aplikace, ve kterých lze metody vzdálených objektů volat z dalších virtuálních strojů (JVM) umístěných na různých počítačích.
Korelace	Korelace ve stavovém monitorování představuje analýzu nad příchozími alarmy v dohledovém systému (například určení alarmů představujících problém a vyřešení problému, párování zdánlivě nesouvisejících alarmů apod.). Korelace v oblasti monitorování E2E, výkonnosti a transakcí představuje párování transakcí a jejich částí (subtransakcí) na základě definovaných vazeb a vztahů.
KPI	Key Performance Indicator - procesně orientovaný postup, který se zaměřuje na poskytování informatických služeb na základě potřeb podniku s důrazem na přínos zákazníkovi.
KVI	Klíčový Výkonnostní Indikátor - viz KPI.
MD	Man Day - člověkoden - pracovní jednotka, v jednotkách MD je odhadována pracnost projektu.
Metrika	Pojem z oblasti stavového monitorování definující předmět monitorování. Metrika generuje po překročení prahové hodnoty alarm, který je doručen do dohledového systému.
Middleware	Počítačový systém z oblasti integrace podnikových aplikací (EAI) umožňující propojit heterogenní back-end systémy.
MMS	Multimedia Messaging Service - služba v síti GSM umožňující zasílání a přijímání multimediálních zpráv (zpráv obsahující obrázky, audio a video).
MSP	Monitoring Service Provider - poskytovatel služeb monitorování aplikací, systémů a služeb prostřednictvím internetu.
OCG	Office Of Government Commerce - vládní instituce Velké Británie, která vyvinula v 80. letech rámec ITIL jako koncept řízení služeb IS/ICT.
ODBC	Open Database Connectivity - standardní metoda využívající softwarové API pro přístup k databázím. Cílem je umožnit přístup ke všem datům jakékoliv aplikace bez ohledu na to, jakým systémem SŘBD jsou data řízena.
OLA	Operational Level Agreement - dohoda definující procesy a vztahy pro interní dodavatele služeb ICT za účely dosažení SLA.

OS	Operating System - Operační systém je základní program počítačového systému umožňující komunikovat s jednotlivými hardwarovými zařízeními.Vytváří rozhraní mezi hardware a aplikacemi.
Performance Management	Řízení výkonnosti představuje soustavu nástrojů a procesů monitorující výkonnost sítě a jejích prvků, aplikací, systémů, serverů a následně i služeb na nich provozovaných.
PL/SQL	Procedural Language/Structured Query Language - procedurální nadstavba nad jazykem SQL vyvinutá společností Oracle používaná v SŘBD stejného výrobce.
PMPD	Performance Management Preprocessing Database - předzpracovávající databáze využívaná při E2E/transakčním monitorování. Tato databáze poskytuje framework pro monitorování. Skládá se ze tří vrstev hrubé, korelační a agregační.
Portlet	Označení pro komponentu v prostředí J2EE, která zajišťuje určitou funkcionalitu či skupinu funkcionalit, často se vizuálně podobá oknu z většiny operačních systémů.
RAD	Real-time Application Dashboard - aplikace z produktové platformy Netcool společnosti IBM z oblasti řízení služeb IT. Umožňuje modelovat službu tvorbou jednotlivých komponent, do kterých lze mapovat příchozí alarmy a tím i definovat dopad těchto alarmů na komponentu i službu jako celek.
RAN	Radio Access Network - část mobilního telekomunikačního systému vytvářející rozhraní mezi mobilní stanicí a jádrem sítě.
RCA	Root Cause Analysis - analýza příčiny vzniku problémů a událostí.
RFC	Request For Change - dokument nebo záznam navrhující způsob změny některé komponenty infrastruktury IS/ICT.
ROCE	Return On Capital Employed - koeficient vyjadřující výkonnost a ziskovost kapitálové investice.
ROI	Return On Investments - Vyčíslený návrat z investice do ICT.
RUP	Rational Unified Process - iterativní metodický rámec pro vývoj a nasazení software v organizaci.
Security Management	Řízení bezpečnosti informačních technologií popisuje aktivity nezbytné k ochraně informačních aktiv podniku proti riziku jejich ztráty, poškození nebo neoprávněnému zneužití.
Service Management	Oblast řízení služeb - z hlediska monitorování umožňuje definovat strom služby skládající se z jednotlivých komponent, do kterých jsou propagovány alarmy z dohledového systému. Tyto alarmy pak následně určují dopad na jednotlivé komponenty služby včetně jejich propagace na komponenty vyšších úrovní.
SCM	Supply Chain Management - řízení všech procesů v rámci dodavatelského řetězce počínaje zajištěním surovin pro první článek řetězce přes zhotovení produktu a konče dodávkou konečnému spotřebiteli posledním článkem řetězce. Tyto procesy se integrují na bázi informačních a komunikačních technologií a zahrnují činnosti uvnitř i vně podniku.

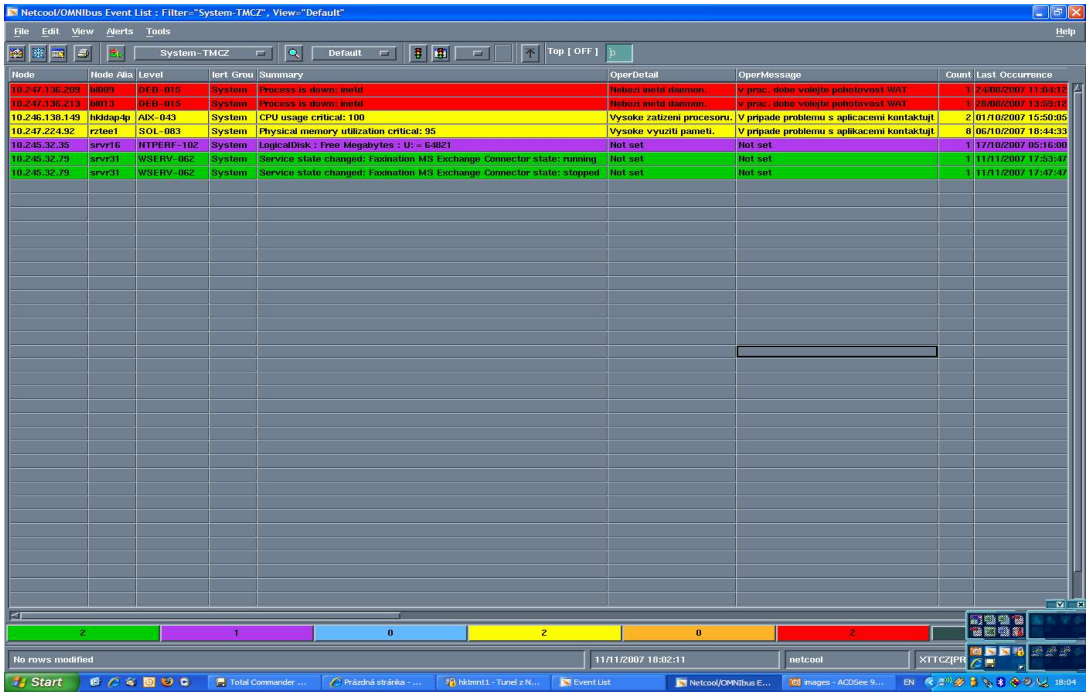
SIEM	Security Information Event Management - systémy pro zpracování bezpečnostních událostí z infrastruktury IS/ICT.
SLA	Service Level Agreement - formální dohoda mezi zákazníky a poskytovateli služeb o úrovni poskytování dané služby.
SLM	Service Level Management - soustava procesů z oblasti Service Delivery metodického rámce ITIL zodpovědných za definici poskytovaných služeb a stanovení jejich úrovně.
SLR	Service Level Requirements - dokument specifikující business požadavky na službu IT. Tyto požadavky definují vlastníci služeb.
SME	Small Medium Enterprise - malé a středně velké (podniky).
SMS	Short Message Service - služba v prostředí sítě GSM zabezpečující přenos krátkých textových zpráv mezi mobilními stanicemi.
SNMP	Simple Network Management Protocol - standardizovaný protokol z aplikační vrstvy soustavy protokolů TCP/IP sloužící potřebám správy sítí a jejich prvků.
SOA	Service Oriented Architecture - architektura aplikací, ve které jsou všechny funkce a služby definovány pomocí popisného jazyka a mají svá rozhraní, která jsou volána za účelem vykonávání business procesů.
SOC	Security Operation Center - organizační jednotka podniku zabývající se bezpečnostními problémy na organizační i technické úrovni.
SPOC	Single Point Of Contact - jednotné místo a způsob kontaktu s organizací či organizační jednotkou. Poskytovatelé služeb poskytují SPOC v podobě Service Desk, kde mají možnost uživatelé a zákazníci kontaktovat poskytovatele.
SPOF	Single Point Of Failure - část systému, která když selže, dojde tím k zastavení fungování celého systému. Takovéto části systému je nutné eliminovat za účelem získání vyšší dostupnosti systému či služby.
SQL	Structured Query Language - standardizovaný dotazovací jazyk, který se používá pro práci s daty v relačních databázích.
SŘBD	Systém Řízení Báze Dat - viz DBMS.
SSM	System Service Monitors - aplikace společnosti IBM/Micromuse běžící ve formě démonu měřící dostupnost a výkonnost hostovaných systémů a aplikací na nich provozovaných.
TCO	Total Cost of Ownership - metodika určena ke stanovení celkových nákladů spojených s pořízením, vlastněním a provozem nových IS/ICT nebo jejich jednotlivých částí po dobu životního cyklu.
TCP/IP	Transmission Control Protocol/Internet Protocol - soustava protokolů používaných ke komunikaci v sítí Internet a dalších podobných sítích.
Threshold	Prahová hodnota - nastavuje se u metrik a KPI. Jakmile nabude metrika či indikátor hodnoty vyšší než prahové, dochází k vygenerování alarmu a jeho následného doručení do dohledového systému.

Tibco MW	Tibco MiddleWare - middleware řešení dodávané společností Tibco.
TibOr	Tibco/Oracle interface - programové rozhraní mezi middleware Tibco a Oracle DB.
TMCZ	T-Mobile Czech a.s.
Transakce	Transakcí se z pohledu transakčního monitorování rozumí proces začínající založením v transakčním systému pokračující dílčím zpracováním požadavku všemi nezbytnými subsystémy (rozpad transakce na subtransakce) a končící výsledným stavem požadavku
Transakční monitorování	Monitorování transakcí představující sběr, korelaci a agregaci dat z transakčních systémů a subsystémů potřebných k určení hodnot definovaných KPI (typicky: počty otevřených, uzavřených, úspěšných, neúspěšných transakcí a subtransakcí, maximální, minimální a průměrná délka transakce a subtransakce, dále pak odvozené indikátory: podíl úspěšných a neúspěšných transakcí a subtransakcí, dostupnost transakčního systému apod.).
UDP	User Datagram Protocol - nestavový protokol soustavy protokolů internetu umožňující data-gramový způsob přenosu dat v paketově přepínaných počítačových sítích. UDP využívá minimální zdroje k přenosu dat, a tak není doručení paketů v rámci UDP nijak garantováno.
WAP	Wireless Application Protocol - protokol umožňující uživatelům mobilních telefonů získávat informace z internetu prostřednictvím WWW stránek vytvořených v hypertextovém jazyce WML (Wireless Markup Language).
Web Server	Webový server - zprostředkovává standardní komunikaci mezi portálem a koncovým zařízením prostřednictvím protokolu HTTP.
Workflow	Řízení pracovních toků - systém poskytují automatizaci celého nebo části podnikového procesu, během kterého jsou dokumenty, informace nebo úkoly předávány od jednoho účastníka procesu ke druhému podle sady procedurálních pravidel.
Work-around	Dočasné vyřešení problému.
WWW	World Wide Web - jedna z nejrozšířenějších služeb internetu umožňující propojovat hypertextové dokumenty v síti.
UC	Underpinning Contract - dokument právního charakteru tvořící dohodu o poskytování služeb externími dodavateli.
UMTS	Universal Mobile Telecommunication System - systém 3. generace mobilních sítí a telefonů.
UTM	Unified Threat Management - komplexní bezpečnostní software obsahující řešení ochrany proti více typům bezpečnostních rizik
XML	eXtensible Markup Language - značkovací jazyk vycházející z jazyka SGML sloužící k popisu dat. V současnosti je XML standardizovaným formátem pro výměnu informací.

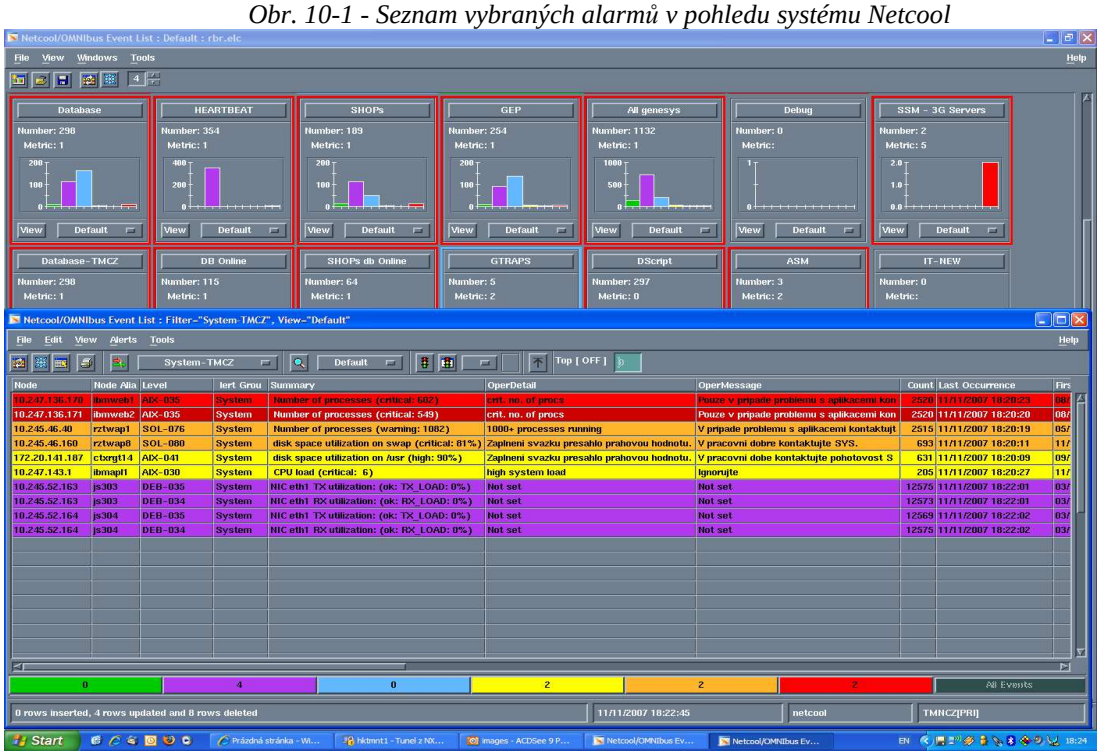
10 Přílohy

10.1 Přílohy A - B - ukázky obrazovek a reportů

10.1.1 Příloha A - Alarmy v dohledovém systému Netcool

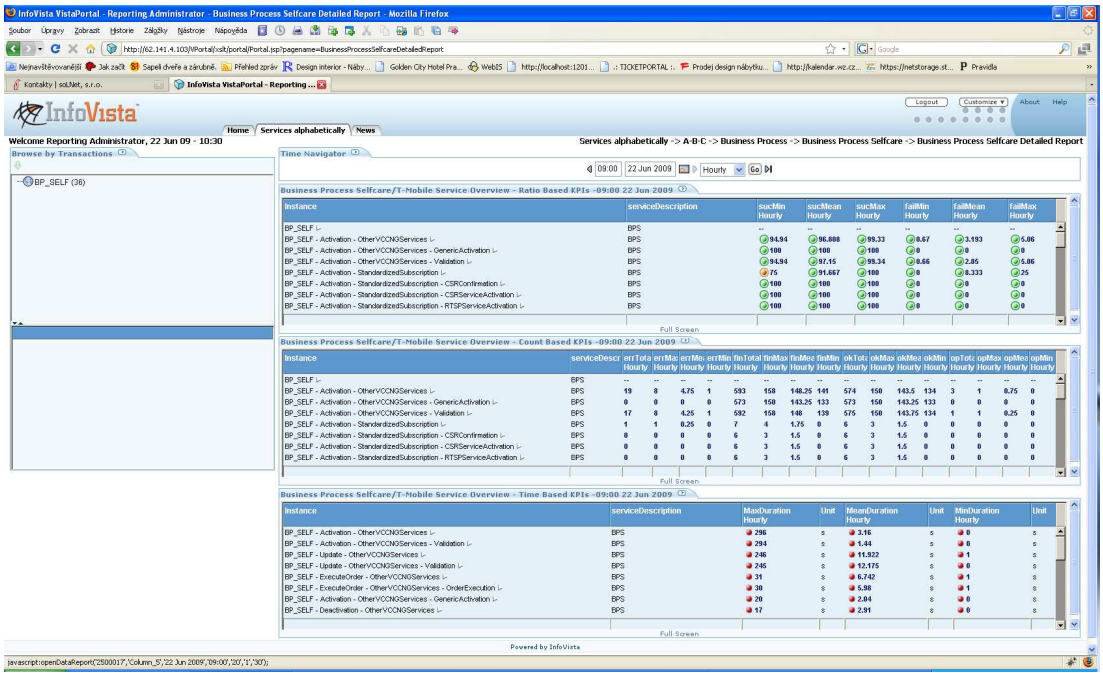


Obr. 10-1 - Seznam vybraných alarmů v pohledu systému Netcool

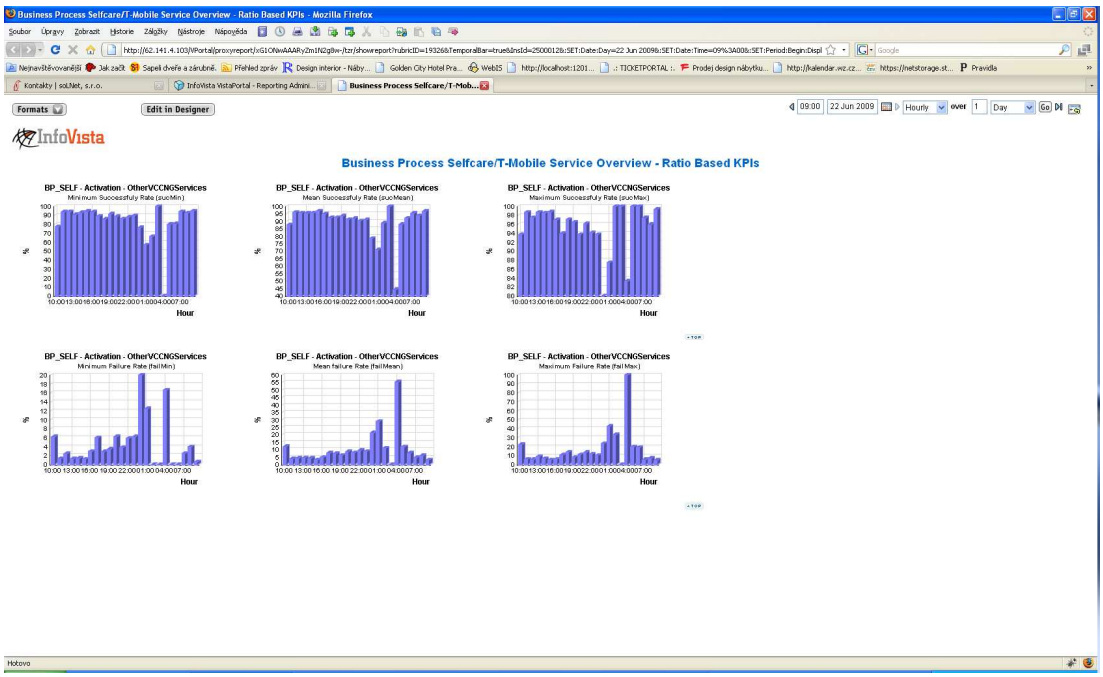


Obr. 10-2 - Seznam vybraných alarmů v systému Netcool, statistické informace v oknech

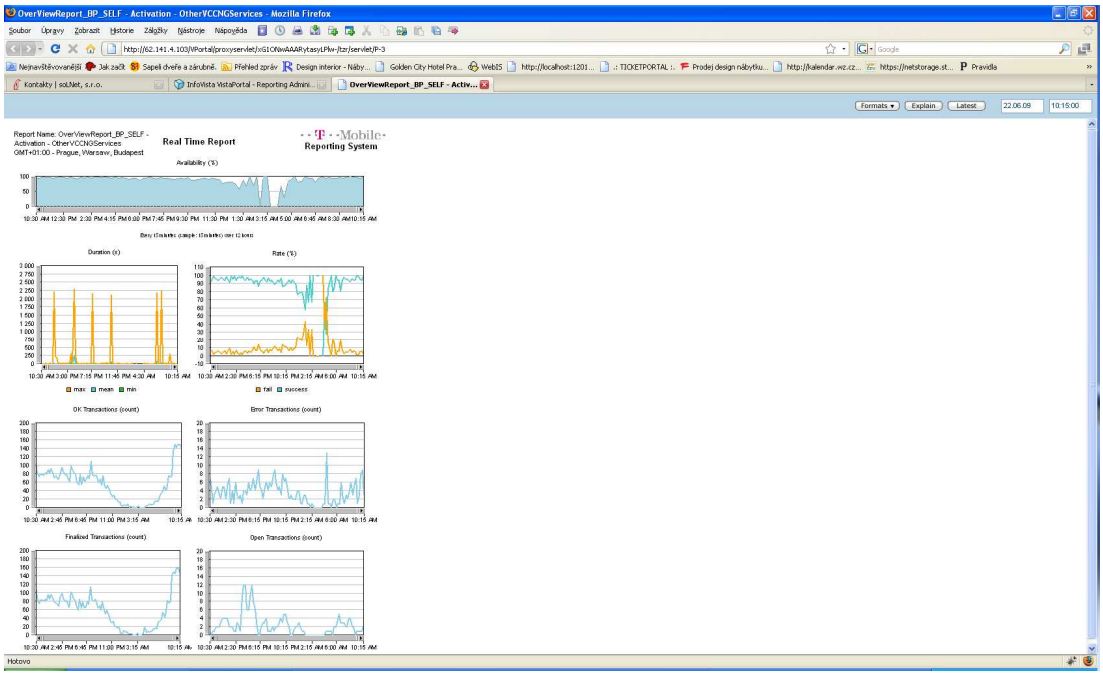
10.1.2 Příloha B - InfoVista reporty



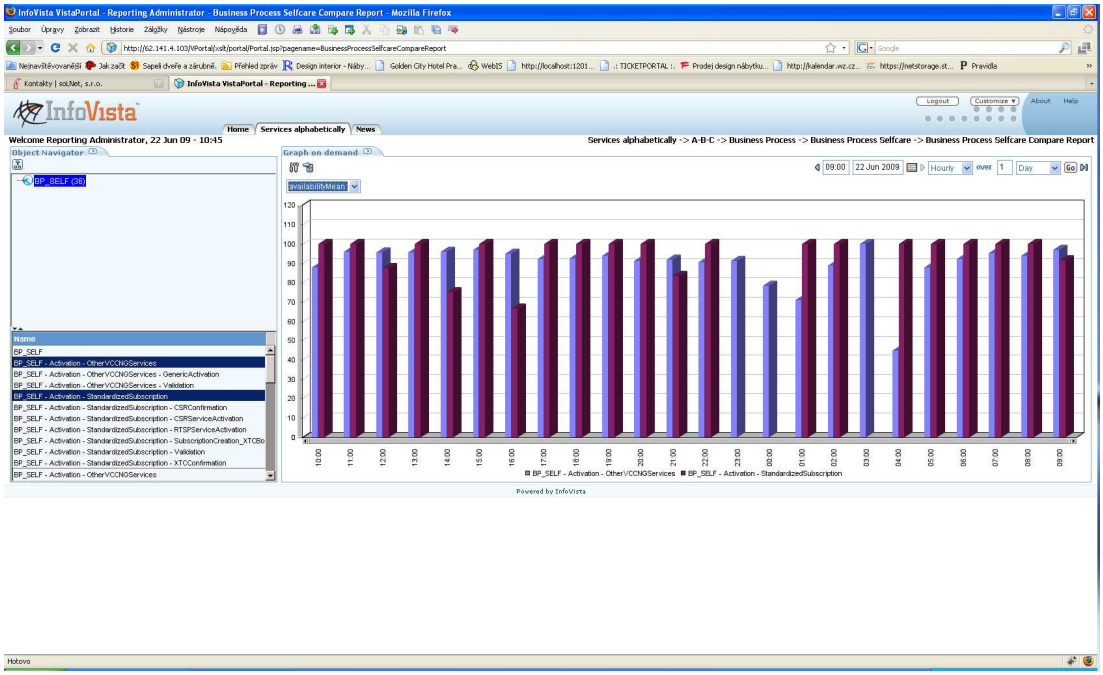
Obr. 10-3 - Business procesy - InfoVista detailní report



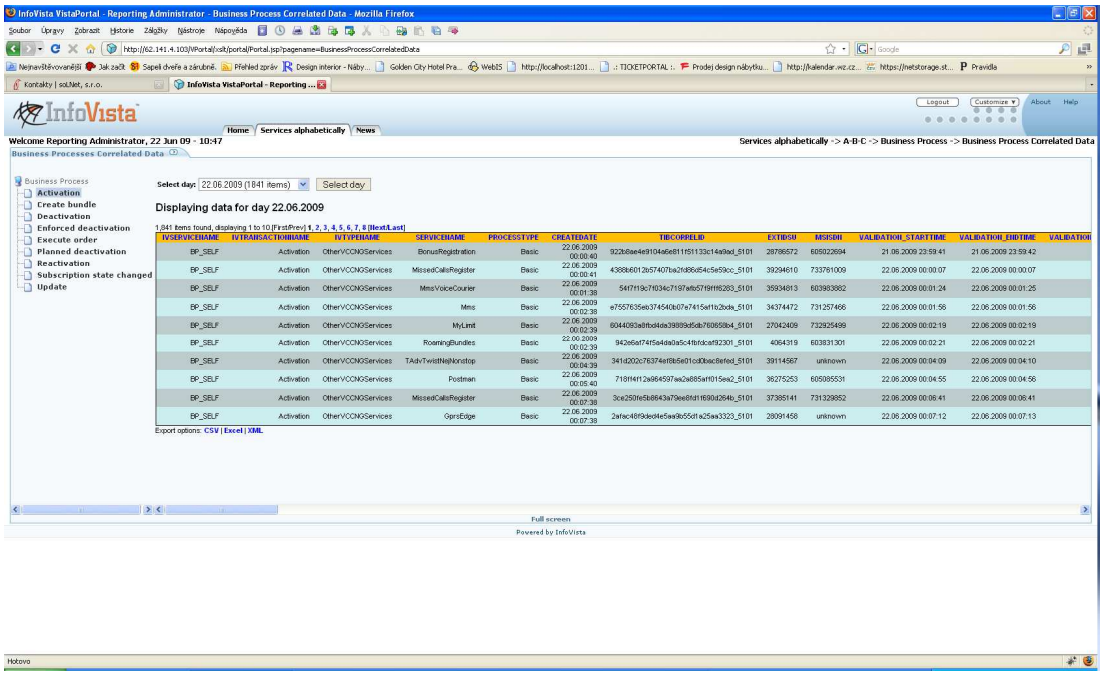
Obr. 10-4 - Business procesy - InfoVista grafický detailní report



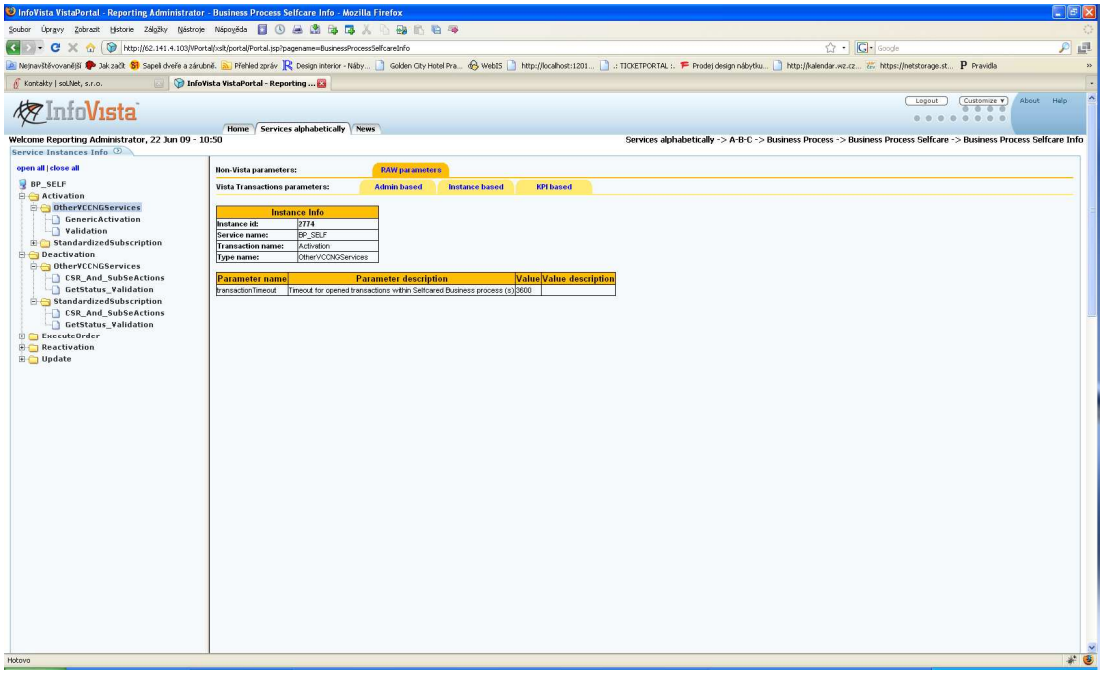
Obr. 10-5 - Business procesy - InfoVista real-time data report



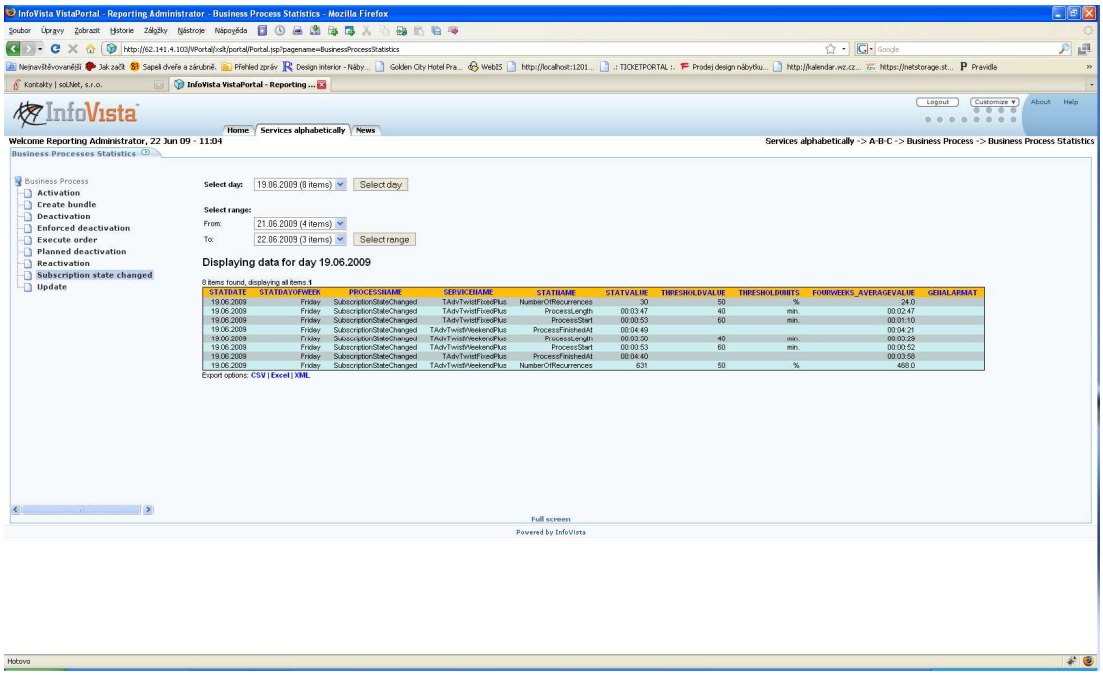
Obr. 10-6 - Business procesy - InfoVista compare report



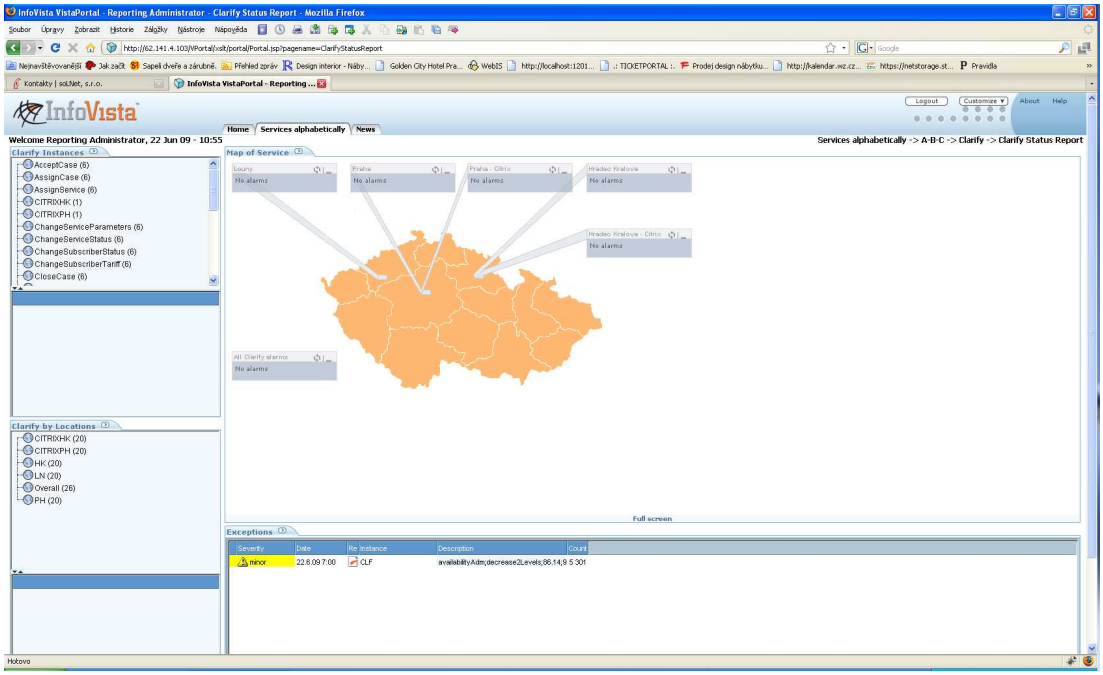
Obr. 10-7 - Business procesy - InfoVista report korelovaných dat



Obr. 10-8 - Business procesy - InfoVista report nastavení hodnot parametrů monitorování



Obr. 10-9 - Business procesy - Specializovaný report statistik



Obr. 10-10 - CRM - InfoVista status report