Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky
Katedra informačních technologií

Studijní program: Aplikovaná informatika
Obor: Informační systémy a technologie

Diplomant: Bc. Jakub Kahoun
Vedoucí diplomové práce: Ing. Luboš Pavlíček
Oponent diplomové práce: RNDr. Dana Čermáková

Nástroje společnosti Microsoft na podporu správy síťové infrastruktury a jejich soulad s normami ITIL

školní rok 2009/2010

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval(a) samostatně a že jsem uvedl(a) všechny použité prameny a literaturu, ze kterých jsem čerpal(a).

V Praze dne

…….

podpis

Rád bych poděkoval Ing. Luboši Pavlíčkovi za věnovaný čas a cenné připomínky při vedení mé diplomové práce.

Abstrakt

Cílem této práce je vyhodnotit podporu procesů dle ITIL v. 3 pro správu IT infrastruktury v produktech společnosti Microsoft. Těžištěm je při tom Microsoft System Center Essentials jako řešení pro dohled a správu IT infrastruktury středně velkých firem.

První část práce popisuje procesy, které podporují provoz IT infrastruktury a které budou porovnávány se System Center Essentials. Popis procesů vychází z originálních publikací poslední verze ITIL.

V druhé části je zprvu popsáno portfolio produktů společnosti Microsoft, které jsou zaměřeny na správu IT infrastruktury. Potom následuje popis System Center Essentials na základě vlastního testování aplikace.

V závěru je provedeno srovnání podpory procesů dle ITIL. Pokud přímá podpora v System Center Essentials chybí, jsou zváženy další možnosti jako je customizace System Center Essentials nebo podpora prostřednictvím jiných produktů řady System Center.

Klíčová slova

ITIL, IT infrastruktura, governance, Microsoft, System Center Essentials

Abstract

The aim of this thesis is to evaluate the support of processes as described in ITIL v. 3 for managing IT infrastructure in Microsoft's product. The focus is taken on Microsoft System Center Essentials as a solution for monitoring and managing IT infrastructure in mid size businesses.

First part of this thesis describes processes which support management of the IT infrastructure and which will be assessed with System Center Essentials. Description of the processes comes from the original ITIL publications in their latest version.

The second part describes portfolio of the Microsoft products that are focused on the management of IT infrastructure. Followed by a detailed description of System Center Essentials based on the own evaluation of the application.

The final part compares the support of the ITIL processes by System Center Essentials. If there is no support by System Center Essentials, solutions by customizing the application is considered or a support by another product from the System Center family.

Keywords

ITIL, IT infrastructure, governance, Microsoft, System Center Essentials

Obsah

Úvod 1
1 ITIL 3
2 Provoz služeb 6
2.1 Správa událostí 8
2.1.1 Vznik události 10
2.1.2 Upozornění na události 10
2.1.3 Detekování události 12
2.1.4 Odfiltrování událostí 12
2.1.5 Klasifikace událostí 12
2.1.6 Korelace událostí 13
2.1.7 Trigger 14
2.1.8 Reakce na událost 15
2.1.9 Revize činností 15
2.1.10 Uzavření události 15
2.1.11 Metriky procesu 16
2.2 Správa incidentů 16
2.2.1 Vznik incidentu 18
2.2.2 Zaprotokolování incidentu 18
2.2.3 Kategorizace 18
2.2.4 Priorizace 18
2.2.5 Úvodní diagnostika 19
2.2.6 Eskalace 19
2.2.7 Řešení incidentu 19
2.3 Správa problémů 19
2.3.1 Identifikace problému 21
2.3.2 Zaprotokolování problému 21
2.3.3 Kategorizace 21
2.3.4 Priorizace 21
2.3.5 Řešení problému a diagnostika 21
2.3.6 Workaround 22
2.3.7 Zařazení mezi „Známé problémy“ 22
2.3.8 Popis řešení problému 22
2.3.9 Uzavření problému 22
2.3.10 Revize závažných problémů 22
2.3.11 Metriky procesu 22
2.4 Dohled nad síťovou infrastrukturou 23
3 Service Transition 24
3.1 Správa konfigurací 24
3.1.1 Management a plánování 26
3.1.2 Identifikace konfigurací 26
3.1.3 Správa konfigurací 27
3.1.4 Protokolování a reporting 27
3.1.5 Ověřování a audit 28

3.1.6 Metriky procesu 28
3.1.7 Požadavky na CMS 29
3.2 Správa distribuce služeb 29
3.2.1 Plánování 30
3.2.2 Vytvoření a testování instalačního balíčku 30
3.2.3 Testování 30
3.2.4 Vytvoření plánu a příprava pro instalaci 30
3.2.5 Instalace 31
3.2.6 Ověření instalace 31
3.2.7 Vyhodnocení a uzavření instalace 31
3.2.8 Metriky procesu 31
3.2.9 Modely distribuce služeb 31
4 Nástroje společnosti Microsoft pro správu sítí 33
4.1 Active Directory 34
4.2 Windows Server Update Services 35
5 Microsoft System Center Essentials 36
5.1.1 Licencování 37
5.1.2 Nároky na hardware 38
5.1.3 Nároky na software 38
5.1.4 Nároky na obsluhu 39
5.2 Instalace a identifikace prvků 39
5.3 Správa počítačů 41
5.4 Monitorování 42
5.4.1 Balíčky pro správu 46
5.4.2 Možnosti customizace monitorování 49
5.5 Distribuce software 52
5.6 Distribuce aktualizací 53
5.7 Reporting 55
5.8 Příklad řešení některých úkolů v SCE 56
6 Podpora procesů ITIL aplikací SCE 58
6.1 Správa událostí, incidentů a problémů 59
6.1.1 Správa událostí 59
6.1.2 Metriky správy událostí 62
6.1.3 Správa incidentů a problémů 63
6.1.4 Metriky procesu 65
6.2 Správa konfigurací 66
6.3 Distribuce služeb 70
Závěr 73
Seznam literatury 75
Seznam obrázků 79
Seznam tabulek 80
Terminologický slovník 81
Přílohy 83

Úvod

IT infrastruktura[1] je jedním ze základních pilířů informačního systému. Veškeré služby poskytované v rámci informační systému jsou závislé na jejím fungování. V dnešní době je mnoho firemních procesů již částečně nebo plně automatizováno, a využívání informačních technologií již není pouze konkurenční výhodou, ale přímo jeden z předpokladů udržení si konkurenceschopnosti na trhu. Podle studie společnosti Dimension Data Czech Republic celých 97 % firem uvádí, že jsou provozně závislé na své síťové infrastruktuře [1]. Návrh a především bezvadný provoz síťové infrastruktury jsou pro moderní podnik jedním z klíčových faktorů. Z průzkumů společnosti Gartner vyplývá, že 50% – 70% výdajů z IT rozpočtu[2] připadá na provoz a údržbu síťové infrastruktury a stávajících podpůrných procesů [2]. Ačkoliv se podíl se může zdát na první pohled vysoký, zejména pokud vezmu v úvahu fakt, že jednotková cena hardwaru neustále klesá, je však nutné si uvědomit značný nárůst komplexity síťové infrastruktury v posledních letech.

Síťová infrastruktura by měla firmě přinášet přidanou hodnotu při podpoře podnikání a výše nákladů na její provoz a správu nesmí překročit její přínos. Jak dalece je tato skutečnost naplňována měří například model zralosti CMMI[3]. Pro dosažení nejvyššího stupně zralosti se předpokládají následující kompetence [2]:

- efektivní provozování IT,
- inovace a neustálé zlepšování procesů a produktivity zaměstnanců.

V mé práci se budu zabývat právě první z uvedených kompetencí. Firma může provozovat IT buď sama, nebo může provoz IT přenést na jiný subjekt, tj. outsourcovat. Při outsourcingu jsou definovány pouze parametry služby, v jaké kvalitě bude poskytována, procesy správy a způsob zajištění služeb jsou však přenechány jinému subjektu.

Při vlastním provozu IT jsou však procesy správy, činnosti a nástroje v režii firmy. Firmy pak musí řešit jak procesy správně nastavit, jaké nástroje zvolit a jaké činnosti provádět aby IT odpovídaly potřebám firmy a jejich provoz nebyl neúměrně finančně nákladný. Je třeba si klást otázky jako například:

- Jak dlouho může trvat výpadek služby a je tato doba pro firmu únosná?

[1] ICT prostředky pro vývoj a provoz aplikací a pro uložení a přenosy dat. [24, s. 24]
[2] Konkrétně cca 50 % na servery, WAN, hlasové služby, service desk, podporu koncových uživatelů; 20 % na provoz a podporu existujících aplikací. [28]
[3] CMMI – Capability Maturity Model Integration: model optimalizace vývoje software a jeho adaptace na podnikové procesy. Více na http://www.sei.cmu.edu/cmmi/.

- Zaznamenávají se při provozu sítě opravdu všechny analytické údaje potřebné k rozhodování o dalším rozvoji infrastruktury?

Většina požadavků na provoz IT vyplývá z podnikových procesů. U těch zbylých mohou do značné míry napomoci tzv. „best practices“ tj. nejlepší praktiky k řízení podnikové informatiky.

Aplikování těchto metodik zatím není v České republice příliš rozšířené. Podle průzkumu společnosti Dimension Data Czech Republic řídí své procesy dle nejpoužívanější metodiky ITIL (IT Infrastructure Library) přibližně pouhých 10 % procent firem [3]. Ostatní firmy své procesy řídí buď dle jiné metodiky anebo, v drtivé většině, neřídí vůbec. Neřízení IT procesů má za následek, že mnohé firmy nejsou schopny změřit kvalitu svých IT služeb a určit na jaké úrovni se jejich IT infrastruktura nachází a podniknout případné další kroky k jejímu zlepšení.

Vzhledem ke své popularitě jsem zvolil právě metodiku ITIL k validaci síťových nástrojů dostupných na trhu. Po jejím prvotním uvedení v roce 1989 se ITIL rychle rozšířil a dnes patří mezi nejuznávanější metodiky. Poslední verze 3 pochází z roku 2007 a právě s touto verzí bude srovnání softwarových nástrojů pro správu IT infrastruktury provedeno. Ačkoliv převládají pozitivní ohlasy na ITIL, mezi ty negativní patří malá konkrétnost v některých případech a změna terminologie mezi verzemi 2 a 3 [4]. Při přebírání „best practices“ si je však třeba uvědomit univerzálnost informace. Pro každý obchodní model má IT různý význam. Nelze tedy brát uvedené informace dogmaticky a vždy je třeba správně vyhodnotit reálnou situaci.

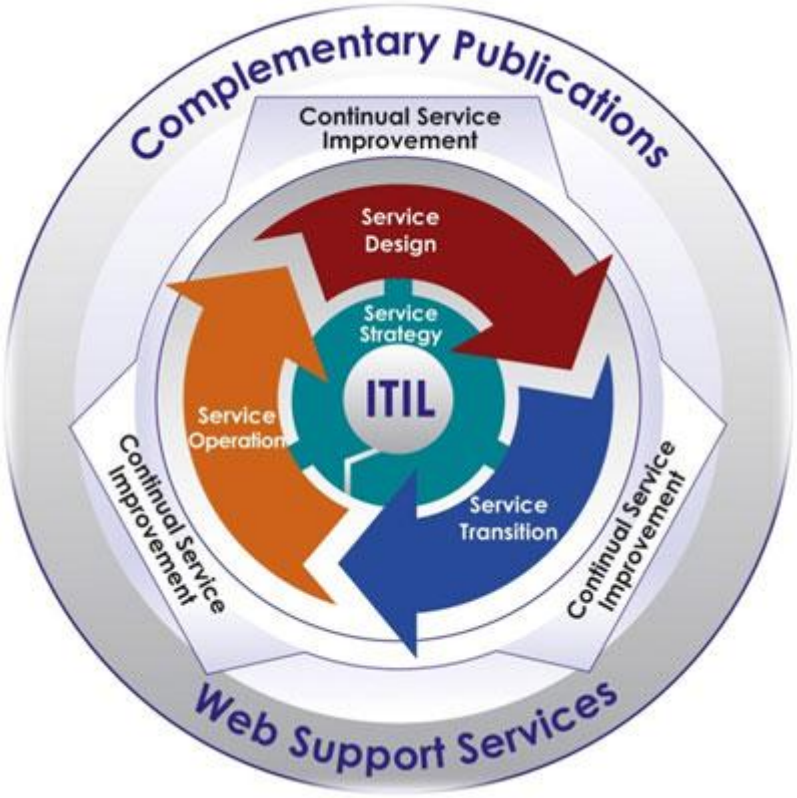
V současné době si společnost Microsoft drží první příčku na trhu s nástroji pro správu počítačové infrastruktury [5][6]. Většina firem používá adresářové služby Active Directory, pracovní stanice s operačním systémem Windows. Volbu tohoto řešení argumentují zpravidla nižšími náklady oproti jiným řešením. Sítě Microsoft se tak staly určitým standardem. Svým produktem System Center Essentials přibližuje nástroje pro monitorování IT infrastrukturu a správu konfigurací středním a menším firmám. System Center Essentials patří do rodiny produktů System Center, která se zaměřuje právě na správu síťové infrastruktury.

Společnost Microsoft v prezentacích svých produktů uvádí, že v sobě obsahují „best practises“. Jsou tyto „best practises“ shodné s obecně uznávanými praktikami metodiky ITIL v. 3? Jak dalece podporují produkty na správu IT infrastruktury procesy dle ITIL? Tyto otázky a další jsou předmětem této práce.

1 ITIL

Za touto zkratkou se nachází pojem IT Infrastructure Library, tedy knihovna IT infrastruktury. Celá knihovna tvoří rámec, ve kterém jsou popisovány procesy, aktéři, technologie a vazby mezi těmito jednotlivými prvky v řízení podnikové informatiky. Na rozdíl od standardů jako je ISO/EIC 20000, ITIL neobsahuje pouze cíle, ale i prostředky, návody a znalosti – tzv. „best practices“, jak těchto cílů dosáhnout.

ITIL tvoří několik svazků publikací, které pokrývají jednotlivé fáze životního cyklu služby (viz Obrázek 1).



Obrázek 1 Rozdělení ITIL v3 (zdroj: [7])

Celý cyklus by měl být v souladu se **Service Strategy**, tedy informační strategií podniku. Svazek Service Strategy popisuje jak vytvářet informační strategii tak, aby byla co nejlépe sladěna s obchodními cíli společnosti. Popisuje definování požadavků na portfolio služeb, složení portfolia služeb a vazeb mezi nimi i implementování strategie v průběhu životního cyklu služby.

Service Design neboli návrh služeb je první etapou z výše uvedeného životního cyklu služby. Popisuje návrh jednotlivých služeb a procesů IT a řízení IT tak, aby zapadaly co nejlépe do celkového

portfolia služeb a zároveň podporovaly strategické cíle. Praktiky Service Design nejsou vyhraněny jen pro nové služby, ale i pro úpravy stávajících služeb.

Service Transition pojednává o implementaci nových či úpravě stávajících služeb, jak byly navrženy ve fázi Service Design, do produkčního prostředí. Úpravami stávajících služeb se rozumí i změna konfigurací prvků IT infrastruktury. Obsahuje procesy jako distribuce služeb nebo řízení rizik. Cílem těchto procesů je eliminace rizik, které s implementací služeb souvisí.

Service Operation popisuje procesy a principy řízení provozu IT. Hlavními procesy v Service Operation jsou řízení problémů a incidentů či vyřizování požadavků. Cílem je udržení dostupnosti IT a umožnění škálovatelnosti služeb.

Continual Service Improvement zmiňuje principy udržitelnosti a rozvoje služeb. Cílem je schopnost rozeznat podněty ke zlepšení služeb během celého životního cyklu služby.

Přehled podpory jednotlivých fází životního cyklu ITIL produkty společnosti Microsoft je uveden v kapitole 6.

Podle ITIL v. 3 je IT provozováno prostřednictvím služeb. Služba je zde definována jako prostředek přinášející hodnotu pro uživatele (popř. zákazníka). Umožňuje uživateli snadněji dosáhnout jeho cílů, aniž by nesl specifická rizika spojená s touto službou či přímé náklady na ni.

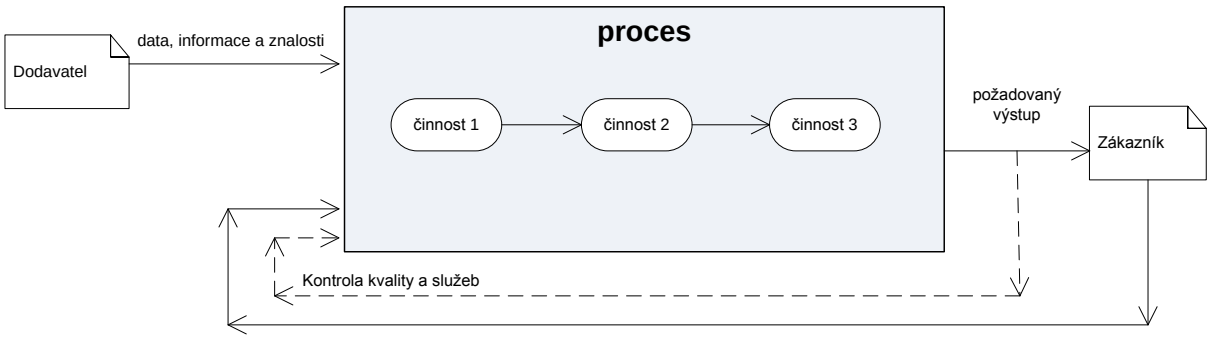
Služby jsou poskytovány skrze procesy a funkce[4].

Funkce je specifická činnost s určitými vyhrazenými prostředky vykonávaná za určitým cílem.

Proces je definován jako transformace v systému, která

- má určitý cíl,
- je měřitelná,
- má své uživatele,
- je aktivována určitou událostí.

[4] Funkce bývají někdy zaměňovány za procesy. V některých modelech však může být činnost funkcí a v jiných procesem. Záleží na návrhu modelu.



Obrázek 2 Proces (zdroj: ITIL v3 – Service Operation [8, s. 13])

Obrázek 2 znázorňuje rozklad procesu. Z grafiky je patrné, že se proces skládá z po sobě jdoucích činností, případně funkcí. Měření výkonu procesu se provádí pomocí metrik (například dostupnost služby). Pomocí indikátorů se pak označují prahové hodnoty metrik, při kterých se výkon procesu dostává do nežádoucího stavu.
Funkce na rozdíl od procesu může existovat i sama o sobě.

Procesy a činnosti, které jsou uplatněny při správě IT infrastruktury, jsou popsány ve svazcích Service Operation a Service Transition. Service Operation se zaměřuje na každodenní činnosti jako je například monitorování sítě, Service Transition pak popisuje činnosti spojené se změnami v IT infrastruktuře jako je například instalace software či aktualizací.

2 Provoz služeb

Provoz služeb je velmi důležitou fází v cyklu života informačního systému. Bez správného řízení a správy procesů pro provoz služeb roste riziko nedostupnosti služeb. Důsledky nedostupných služeb mohou v některých případech představovat i vážné ohrožení firmy. Během provozu dochází také ke generování informací nezbytných pro ostatní fáze života informačního systému, kterými jsou například Service Transition či Service Design. Pokud tyto informace chybí nebo jsou neúplné, nelze řízení IT infrastruktury zcela optimalizovat.

Při provozu služeb se lze setkat s:

Událostí	Událost je definována jako rozpoznatelný stav, který má význam pro správu IT infrastruktury či provozování služeb. *Příklad: informace o úspěšném dokončení zálohování.*
Problémy	Problém je příčinou jednoho či více incidentů. *Příklad: Problém může být například porucha síťové karty. Incident je následná nedostupnost serveru. Incident je tedy důsledkem.*
Incidenty	Za incident se považuje neplánované přerušení nebo degradace IT služeb. Incidentem je i výpadek komponenty konfigurace, který neovlivnil uživatele. *Příklad: porucha disku v diskovém poli se zrcadlením.*
Požadavky uživatelů	Za požadavek jsou považovány žádosti uživatelů vůči IT oddělení. *Příklad: Žádost o nastavení hesla k uživatelskému účtu, nastavení počítače, instalace software apod.*

Tabulka 1 Přehled

Service operation obsahují tyto čtyři hlavní procesy:

- správa událostí,
- správa incidentů a problémů,
- správa požadavků uživatelů,
- řízení přístupu.

Správa událostí vyhodnocuje události, které mohou nastat, a určuje, jak budou identifikovány a dále zpracovávány. V případě nežádoucího stavu jsou iniciovány kroky k nápravě.

Správa incidentů a problémů se zaměřuje na řešení problémů, poruch hardware a chyb software. Tento proces se dělí na dva podprocesy řízení problémů a řízení incidentů, které budou rovněž popsány v další části této kapitoly.

Správa požadavků. Požadavky, zpravidla od uživatelů, jsou přijímány na jediném místě a tím je service desk. Požadavek může být například na re-konfiguraci aplikace, přidání periferního zařízení. Vždy tak dochází ke změně konfigurace (CI[5]). Tento proces definuje, jak budou požadavky uživatelů vyřizovány.

Řízení přístupu. Tento proces určuje, na základě čeho budou přidělována přístupová práva uživatelům služeb a systémů.

Procesy vyřizování požadavků a řízení přístupu nejsou podporovány popisovanou aplikací, a proto nebudou dále podrobněji rozebírány.

Hlavní **funkce** v provozu služeb jsou:

- service desk,
- technický management,
- technická podpora (onsite support),
- správa aplikací,
- rozhraní k ostatním fázím cyklu života služeb.

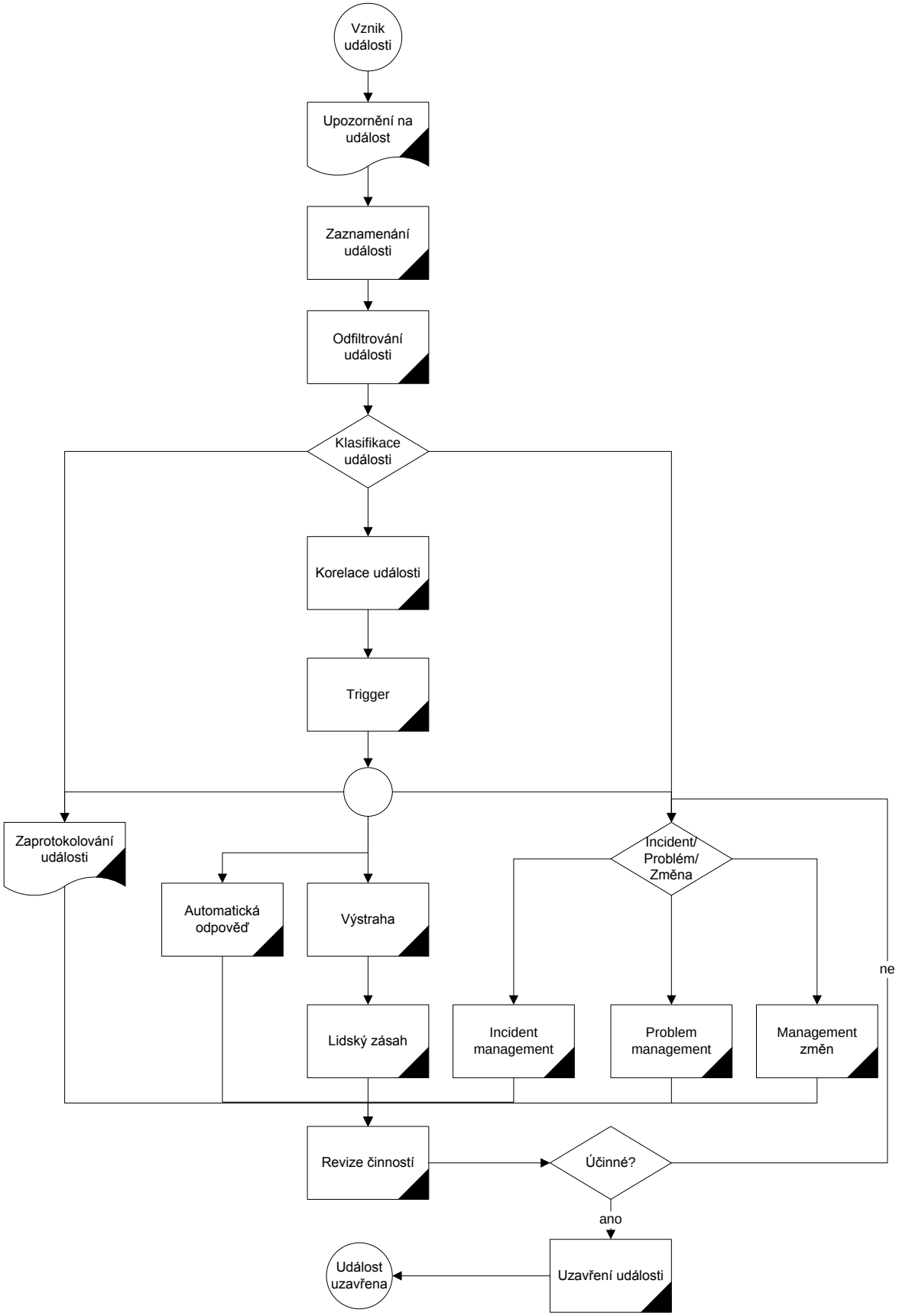
Tyto funkce mohou figurovat i ve více procesech či mohou být částečně konsolidovány. Konkrétní podoba implementace záleží na řízení IT a návrhu procesů.

[5] z anglického Configuration Item

2.1 Správa událostí

Události vypovídají o stavu IT infrastruktury a jsou tedy důležité pro její správu. Zároveň jsou často východiskem pro řadu procesů operativního řízení (např. incident management apod.). V případě nežádoucího stavu (poruchy) může být událost předána kompetentnímu týmu, aby se předešlo významnějšímu vlivu výpadku služby či aby bylo spuštěno automatické korekční opatření. Dále může událost pomoci při diagnostice příčin problému.

Obrázek 3 znázorňuje proces správy událostí dle ITIL verze 3.



Obrázek 3 Správa událostí (zdroj: ITIL v. 3 – Service Operation [8, s. 38])

2.1.1 Vznik události

Události vznikají při provozu IT infrastruktury soustavně. Ne všechny jsou však zaznamenány a ne všechny události, které mohou být zaznamenávány, mají význam pro řízení IT. Je tedy důležité při návrhu služeb určit, jaké události mají být zaznamenávány.

2.1.2 Upozornění na události

Na události bývá upozorňováno během činnosti, která se nazývá monitorování.

ITIL v3 definuje Monitorování jako činnost sledování situace během vymezeného časového úseku za účelem identifikace změn, které se za tento časový úsek odehrály.

Monitorování zahrnuje následující činnosti:

- sledování stavu prvku IT infrastruktury pomocí patřičných nástrojů,
- kontrola, že jsou splněny podmínky pro provoz (např. dostupnost síťového prvku),
- kontrola, že sledované hodnoty jsou v normálním stavu[6] a pokud tomu tak není, dojde k nahlášení incidentu,
- identifikace neobvyklých činností zařízení (např. pokus o narušení zabezpečení),
- identifikace neoprávněných zásahů do systému,
- kontrola dodržování zásad informační politiky organizace,
- kontrola dodržování licenční politiky,
- sledování kvality výstupů,
- sledování výkonu klíčových prvků.

Na základě hodnot z monitorování jsou pak vytvářeny reporty. Ačkoliv monitorování slouží primárně pro dohled nad provozem infrastruktury, jsou generované údaje, zejména v podobě reportů, důležitým vstupem pro koncepce zlepšování služeb (například vytížení současných kapacit IT infrastruktury). Je tedy důležité, aby monitorování bylo prováděno i s ohledem na tyto činnosti.

[6] tj. v předem stanovených hodnotách

Druhy monitorování

ITIL v. 3 popisuje níže uvedené druhy monitorování. Každý z uvedených druhů monitorování je vhodný do jiných podmínek.

Aktivní monitorování

Při tomto monitorování se vznáší požadavek na určité zařízení nebo systém (například pro zjištění, zda vzdálený systém odpovídá). Na základě zjištěného stavu mohou být generovány události. Každé dotazování však vyžaduje systémové prostředky. To může v konečném důsledku negativně ovlivnit výkon aplikací či služeb. Proto se doporučuje tuto metodu omezit na kritické systémy nebo na provádění diagnostiky při řešení problémů.

Pasívní monitorování

V tomto případě zařízení či systém vygeneruje událost a předá ji monitorovacímu systému. Při této metodě je klíčové nadefinovat správně události, které mají být předávány, aby nedošlo například k situaci, kdy chybová událost vyřadí zařízení z provozu a monitorovací centrum se o této chybě neobdrží hlášení.

Reaktivní monitorování

Při reaktivním monitorování se spouští reakce na určitou událost. Například pokud není v systému spuštěna určitá služba, systém ji automaticky spustí (či restartuje). Nemusí se však vždy jednat jen o chybové hlášky či varování, reakce může být spuštěna i na základě informativní události jako je úspěšné dokončení zálohování apod.

Proaktivní monitorování

Proaktivní monitorování identifikuje tendence v chování systému na základě vícero událostí. Obsahuje předdefinované události na základě předchozích zkušeností, které vedou k určitému problému (např. kolaps služby nebo systému).

Průběžné monitorování

Průběžné monitorování sleduje systémy a služby v reálném čase. Používá se tak například na měření dostupnosti serverů. Průběžné monitorování je oproti aktivnímu monitorování nepřetržité. Vzhledem k systémovým prostředkům, které jsou pro zajištění monitorování nezbytné, je monitorování často omezeno na krátké intervaly (např. každých 15 vteřin).

Mimořádné monitorování

Mimořádné monitorování je spuštěno na základě nějaké mimořádné události. To je výhodné z hlediska systémových prostředků a nákladů. Může to však zvýšit dobu potřebnou pro řešení problému. V některých situacích je možné použít pouze Mimořádné monitorování. Mezi takové situace patří například ověření parametrů tisku.

2.1.3 Detekování události

V této fázi procesu jsou události detekovány pro další interpretaci. Zpravidla tuto činnost zajišťuje software (nazývaný též „agent“), který předává události aplikaci pro správu a dohled.

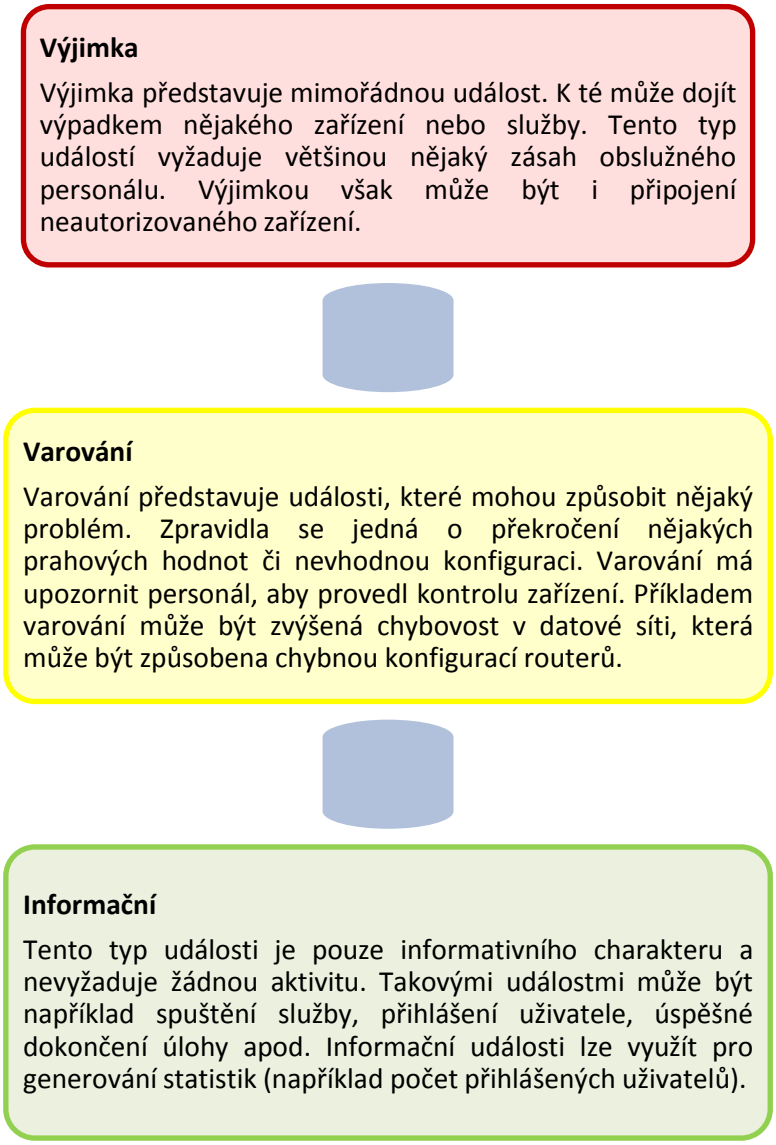
2.1.4 Odfiltrování událostí

Při filtrování událostí dochází k výběru událostí, které budou předány nástroji pro správu a dohled. Tuto činnost zpravidla zajišťuje, stejně jako detekování události, software (agent). Zde může rovněž docházet k první části interpretace událostí (např. dle jejich typu). Interpretované události umožňují dynamičtější reakci a tedy i rychlejší nápravu.

Události, které nejsou předány nástroji pro správu a dohled, zůstávají správcům IT infrastruktury nadále k dispozici v protokolech zařízení/služby.

2.1.5 Klasifikace událostí

Klasifikace událostí je na uvážení firmy. ITIL verze 3 doporučuje implementovat minimálně následující 3 kategorie:



Od kategorie události se dále odvíjí její zpracování.

2.1.6 Korelace událostí

Pokud se jedná o významnější událost ve smyslu možného narušení služeb, je zapotřebí nalézt rychlé řešení.

Korelace událostí vyhodnocuje události dle daných kritérii a určí tím míru dopadu na chod businessu. Při korelaci lze uvažovat například tyto kritéria:

- počet podobných událostí,
- počet CI generující stejnou podobnou událost,
- zdali událost vyžaduje specifickou činnost,
- zdali se jedná o výjimku,

- zda-li v dané době nedošlo zároveň k degradaci výkonu CI,
- zda-li jsou potřeba další údaje k řešení incidentu,
- kategorizace události,
- přiřazení priority k události.

Specifikace korelačního nástroje vychází z návrhu služeb (publikace Service Design).

2.1.7 Trigger

Na základě výsledků korelace události je zahájena další činnost. Tou může být:

- zaznamenání události jako incidentu,
- generování žádosti o změnu,
- spuštěním skriptu s nápravným opatřením,
- upozornění kompetentní osoby,
- úprava přístupu k databázi služby[7].

[7] Např. za účelem zachování integrity dat.

2.1.8 Reakce na událost

Reakcí na událost může být celá řada a vzhledem k události je lze různě kombinovat.

Tabulka 2 popisuje reakce na události dle ITIL v. 3:

Zaprotokolování události Vždy je vhodné událost zaprotokolovat. I když v daném případě nemusí být potřeba žádná další akce, může událost pomoci při korelaci událostí či při řešení problému a incidentů.	**Automatická odpověď** Automatická odpověď na událost představuje spuštění korekčního skriptu. Ten může například restartovat zařízení/službu, změnit její parametry apod.
Lidský zásah Pokud událost vyžaduje lidskou intervenci (např. při chybě), je důležité, aby se událost co nejrychleji dostala ke kompetentní osobě.	**Přechod do řízení incidentů, problémů a změn** Některé události by měly být řešeny v procesu řízení incidentů/problémů/změn a v některých případech (např. selhání hardware v serveru) dokonce kombinací těchto procesů.

Tabulka 2 Reakce na události

2.1.9 Revize činností

Revize činností se provádí při událostech, které narušily chod IT infrastruktury či degradovaly její výkon[8]. Cílem tohoto kroku je ověření, že událost byla korektně zpracována.

2.1.10 Uzavření události

Události, které iniciovaly proces řízení incidentů/problémů/změn jsou zakončeny tímto procesem. Informační události jsou uzavřeny změnou stavu síťového prvku či služby.

[8] Vzhledem k značnému množství událostí nelze revidovat provedené činnosti u všech událostí.

2.1.11 Metriky procesu

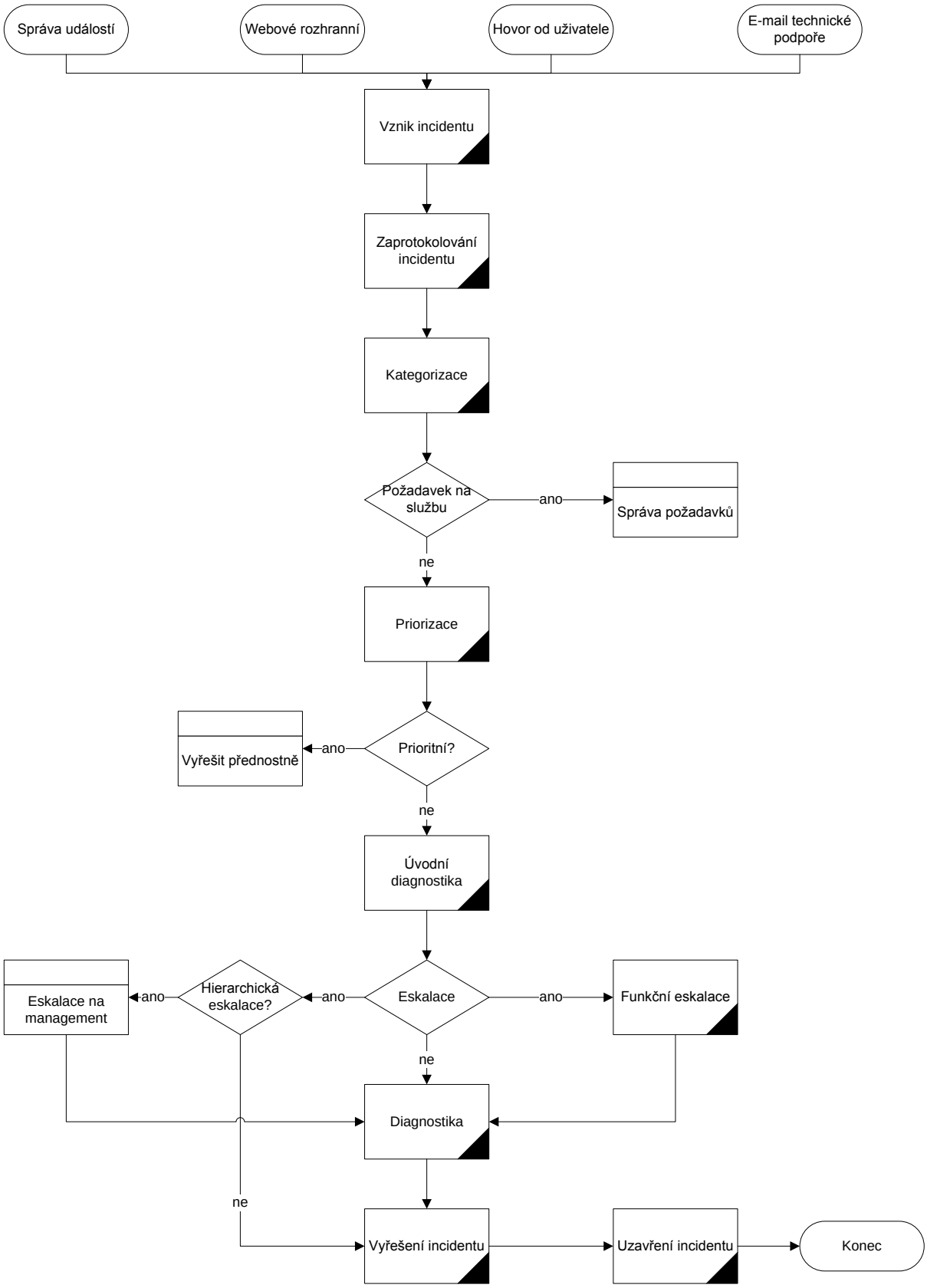
ITIL v. 3 doporučuje uplatnit následující metriky pro sledování výkonu procesu řízení událostí:

- počet událostí v určité kategorii či určitého typu celkem a dle jednotlivých služeb či platforem,
- počet a procento událostí, které vyžadovaly lidský zásah,
- počet a procento událostí, které byly identifikovány jako incident/změna,
- počet a procento událostí, které byly zaviněny známou chybou,
- počet a procento událostí, které
    - se opakují,
    - poukazují degradaci výkonu služby,
    - poukazují na dostupnost služby.

2.2 Správa incidentů

Správa incidentů se snaží minimalizovat důsledky incidentů tím, že incidenty vyhodnocuje podle předem stanovených kritérií. Vyhodnocení incidentů usnadňuje interpretaci incidentů a může urychlit jejich vyřešení. V ideálním případě ještě dříve než stačí postihnout uživatele. Vyhodnocování incidentů se často provádí obdobně jako u problémů. Činnosti jako je kategorizace či priorizace jsou sdílené oběma procesy. Často jsou proto zahrnuty v jediném nástroji pro správu a dohled nad sítí.

Průběh procesu znázorňuje Obrázek 4 Správa incidentů.



Obrázek 4 Správa incidentů (zdroj: ITIL v3 – Service Operation [8, s. 48])

2.2.1 Vznik incidentu

Incident může být zaznamenán buď správou sítě (technikem či aplikací monitorující síť) nebo uživatelem.

2.2.2 Zaprotokolování incidentu

Incident musí být řádně zaprotokolován. V záznamu o incidentu by neměl chybět:

- jednoznačný identifikátor,
- kategorie incidentu,
- důležitost,
- osoba nahlašující incident včetně kontaktních údajů,
- popis problému,
- stav incidentu,
- prvky konfigurace (CI), kterých se incident týká,
- řešící tým a postupy vedoucí k řešení problému,
- datum vyřešení problému.

2.2.3 Kategorizace

Kategorizace je vhodná pro snazší identifikaci incidentu. Každá společnost si může definovat své kategorie. Obvykle jsou kategorie vytvářeny hierarchicky (např. Hardware – Server – Základní deska – Chyba síťové karty).

Pokud z incidentu vyplývá i požadavek na změnu (například při selhání hardwaru), je iniciován proces správy změn.

2.2.4 Priorizace

V této fázi se určí priorita incidentu. Vyhodnocování priorit lze určit pomocí tabulek, kdy se počítá naléhavost a míra dopadu incidentu na uživatele. Dalším aspektem při priorizaci je závažnost, která bere v potaz finanční náklady a lidské zdroje potřebné pro odstranění incidentu.

Existují však i případy, kdy je potřeba vyhodnocovat priority individuálně (např. reputace firmy).

2.2.5 Úvodní diagnostika

Tato činnost se provádí zejména v případě, kdy byl incident nahlášen přes Service Desk. Cílem je získat od uživatele co nejvíce informací o chybovém stavu a snaha jej s uživatelem vyřešit. Pokud je incident složitější a nelze jej vyřešit, je předán dál k řešení.

2.2.6 Eskalace

V závislosti na povaze problému může incident eskalovat horizontálně, přes úrovně správy IT infrastruktury až k samotnému dodavateli služby/software, či vertikálně na vyšší management.

2.2.7 Řešení incidentu

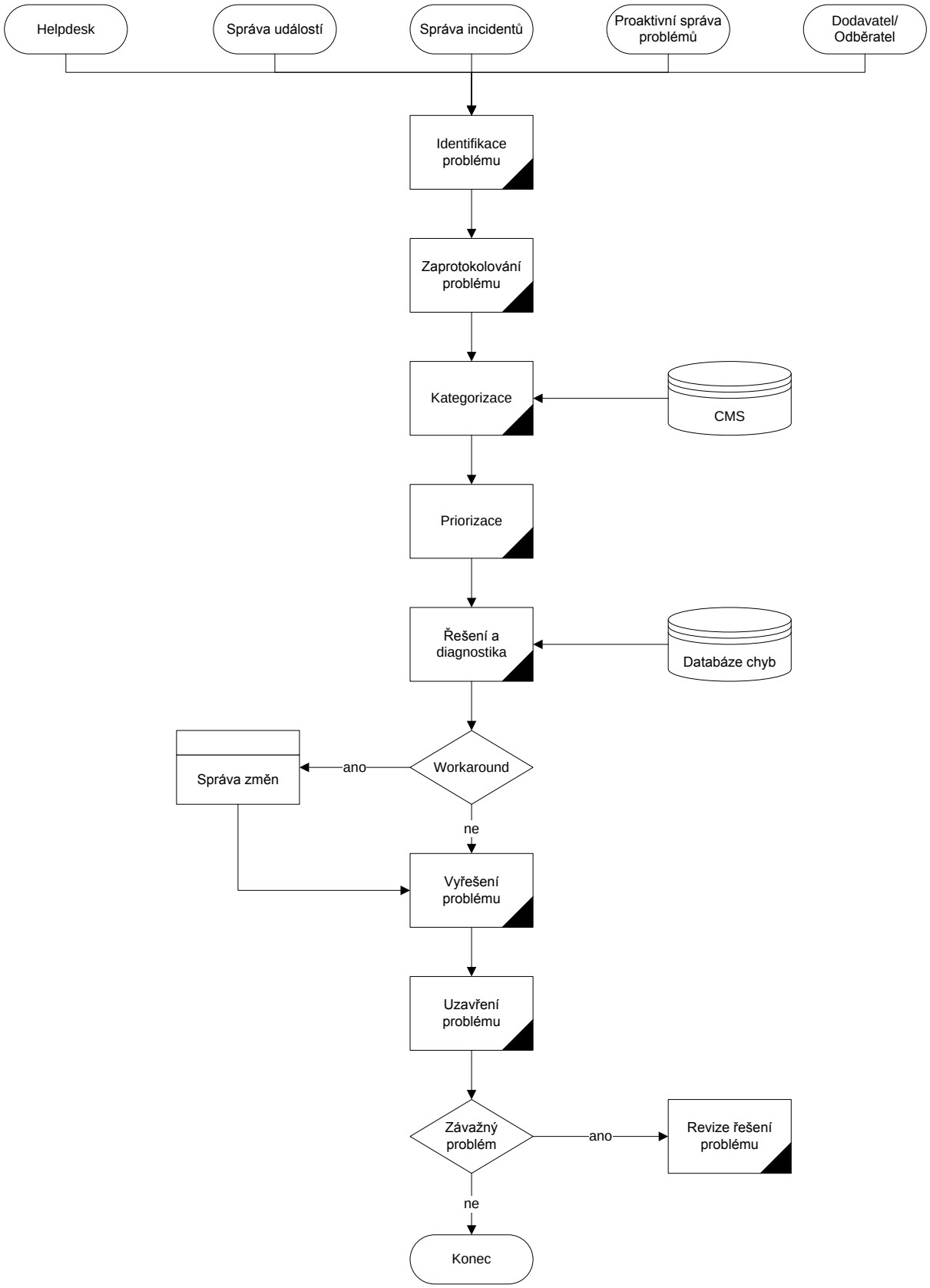
V případě, že bylo nalezeno řešení a důkladně otestováno, provedou se korekční opatření. Do této fáze může být zapojen jak uživatel, tak i řešící tým.

2.3 Správa problémů

Správa problémů je proces, který se snaží problémům předcházet a tím minimalizovat jejich vliv na uživatele a chod businessu. To, pokud je řízení problémů efektivní, zvyšuje produktivitu uživatelů a pomáhá snižovat výdaje na řešení incidentů. Existují dva typy procesů, které reprezentují řízení procesů:

- **reaktivní**, kdy problém je řešen na provozní úrovni,
- **proaktivní**, kdy problém je iniciován v Service Operation avšak pak je postoupen do Continual Service Improvement.

Obrázek 5 znázorňuje průběh reaktivního procesu.



Obrázek 5 Proces správy problémů (zdroj: ITIL v3 – Service Operation [8, s. 60])

2.3.1 Identifikace problému

Jak již napovídá Obrázek 5, problém může být detekován několika způsoby. Těmi jsou:

- identifikace problému v rámci řešeného incidentu,
- automatická detekce problému nástroji pro správu a dohled IT infrastruktury,
- upozornění na problém dodavatelem/odběratelem (například v případě stažení výrobku z trhu).

2.3.2 Zaprotokolování problému

Každý problém by měl být zaprotokolován, a pokud se váže k nějakému incidentu, doporučuje se tuto vazbu rovněž zmínit. Zápis by vedle popisu problému měl obsahovat i zmínku o uživateli, zasaženém CI a o čase, kdy problém nastal.

2.3.3 Kategorizace

viz 2.2.3 Kategorizace

2.3.4 Priorizace

viz 2.2.4 Priorizace

2.3.5 Řešení problému a diagnostika

Při odstraňování problému je vhodné určit i hlavní příčinu problému. To může pomoci při opakovaném řešení problému či řešení podobného problému.

Důležitým zdrojem informací při řešení problémů a diagnostice je systém pro správu a dohled nad sítí.

ITIL v. 3 uvádí například tyto techniky pro podporu řešení problémů:

a) **Chronologická analýza** sleduje sled událostí, jak nastaly, a umožňuje tak odhalit souvislosti mezi nimi.
b) **Analýza způsobených škod** kalkuluje dopad na uživatele a ztráty způsobené výpadkem služeb.
c) **Brainstorming** umožňuje diskutovat různé nápady a návrhy na řešení problémů.

2.3.6 Workaround

V některých případech lze uplatnit tzv. workaround. Workaround neboli dočasné řešení umožňuje zajistit částečnou či plnou obnovu služby na jiném systému a v mezičase odstranit problém na zařízení/službě původní. Po celou tuto dobu zůstává problém otevřený.

2.3.7 Zařazení mezi „Známé problémy“

Popsaný problém by měl být za-archivován mezi známé problémy. To umožňuje rychleji řešit shodné či obdobné problémy.

2.3.8 Popis řešení problému

Jakmile je nalezeno spolehlivé řešení problému, postup pro řešení problému by měl být zaznamenán.

2.3.9 Uzavření problému

Pokud byly všechny změny provedeny a řešení problému bylo aplikováno a zaznamenáno, může být problém formálně uzavřen.

2.3.10 Revize závažných problémů

V případě, že se jednalo o zásadní problém, je důležité provést revizi řešení a vyhodnotit, co bylo vykonáno dobře či špatně a co lze do budoucna zlepšit případně, zda je možné opakování problému zamezit.

2.3.11 Metriky procesu

ITIL v. 3 doporučuje použít následující metriky pro sledování výkonu tohoto procesu:

- počet problémů za dané období,
- procento problémů vyřešených do doby stanovené SLA,
- procento problémů, které překročilo svůj vyhraněný čas k řešení,
- procento zásadních problémů, jejich tendence, a zda byly dokončeny včas,
- průměrné náklady na řešení problému.

2.4 Dohled nad síťovou infrastrukturou

Procesy uvedené v předchozích kapitolách úzce souvisí s činností nazývanou dohled nad síťovou infrastrukturou.

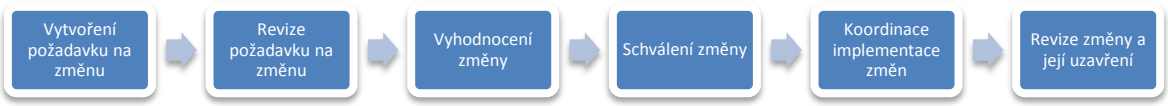
Náplní této činnosti je dohled nad IT infrastrukturou (tj. servery, stanice, aplikační software, apod.) a to z jediného místa. Prvky na které je dohlíženo se přitom mohou nacházet i na odlehlých místech. V případě incidentů je právě na dohledovém centru, aby zajistilo řešení problému ať už vzdálenou správou nebo upozornilo na problém odpovědné servisní týmy.

Dohled nad síťovou infrastrukturou bývá někdy spojený s funkcí service desku, kam uživatelé hlásí své problémy nebo požadavky na změnu. V menších organizacích však může být dohled omezen pouze na vzdálenou správu.

3 Service Transition

Dnešní IT prostředí je značně dynamické. Ať už dochází k výměně pracovníků, požadavkům na nová zařízení či úpravy stávajících aplikací (aktualizace, re-konfigurace apod.), vždy se jedná o zásah do IT infrastruktury. Vzhledem ke komplexnosti[9] systémů je potřeba zásahy mapovat a plánovat aby byla zachována integrita systémů a služeb. ITIL v. 3 shrnuje procesy a činnosti související se zmiňovanými zásahy do IT infrastruktury do publikace s názvem Service Transition. Service Transition probíhá tedy například při upgradu síťové infrastruktury, implementaci nových služeb, může ale být i důsledkem nějakého incidentu (např. výměna poškozeného hardwaru) nebo požadavku uživatele (např. instalace software).

Pro jednotlivé typy změn služeb a prvků infrastruktury existují konkrétní procesy. Průběh těchto procesů je definován ve fázi Service Design. Část procesů ze Service Transition spadají hlavně do této fáze (např. Service Validation and Testing) a druhá část procesů (např. Release and Deployment Management) se prolíná s Service Operation. Právě druhou skupinou procesů se budu dále zabývat v mé práci.



Obrázek 6 Standardní proces změny

Obrázek 6 znázorňuje průběh standardního procesu změny. Od toho jsou odvozované konkrétní procesy (např. správa distribuce software). Standardní proces může být upraven tak, aby byl připraven i na nestandardní situace (např. havarijní stavy, kdy je třeba provést změny co nejrychleji).

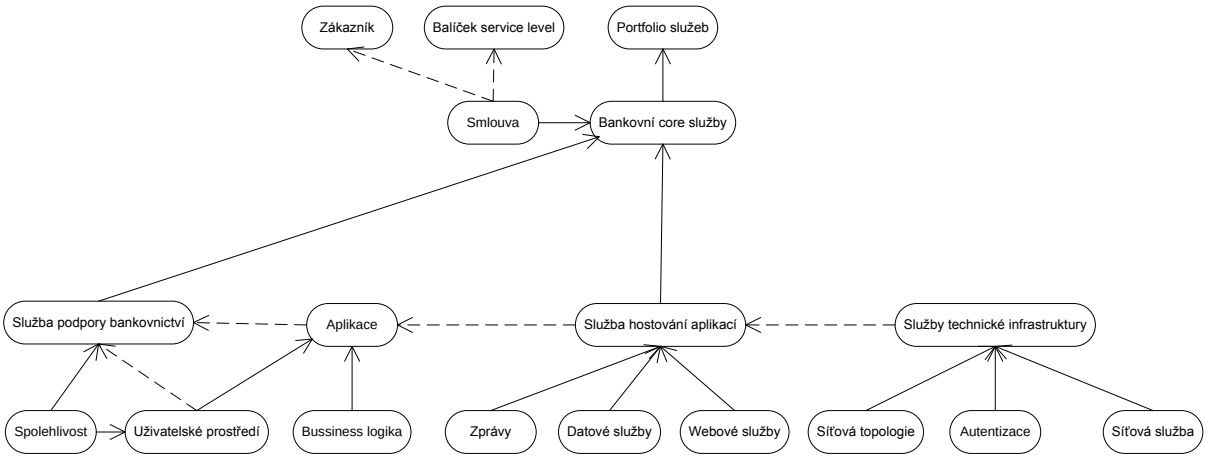
3.1 Správa konfigurací

Správa konfigurací je nezbytnou činností pro správu větších IT infrastruktur a služeb a provádí se zpravidla pomocí dedikovaného software tzv. Configuration Management System (CMS). CMS uchovává veškeré konfigurace včetně jejich podrobné specifikace a vazeb mezi nimi. Pokud jsou správně definovány vazby, lze v případě incidentu určit další problémy, které mohou vzniknout.

[9] služby v řadě případů používají společné prostředky

Konfigurací (CI) dle ITIL v. 3 může být aktivum (tj. pracovní stanice, server, apod.), komponenta služby či schopnosti (procesy, znalosti, apod.). Vzhledem ke značné rozmanitosti bývají CI seskupovány do kategorií a konfigurace jsou pokud možno co nejvíce homogenní. Vedle kategorií jako je řízení CI, CI rozhranní služeb s poskytovateli, je kategorie CI služeb, pod kterou spadá i IT infrastruktura. V mé práci se zaměřím pouze na evidenci CI IT infrastruktury.

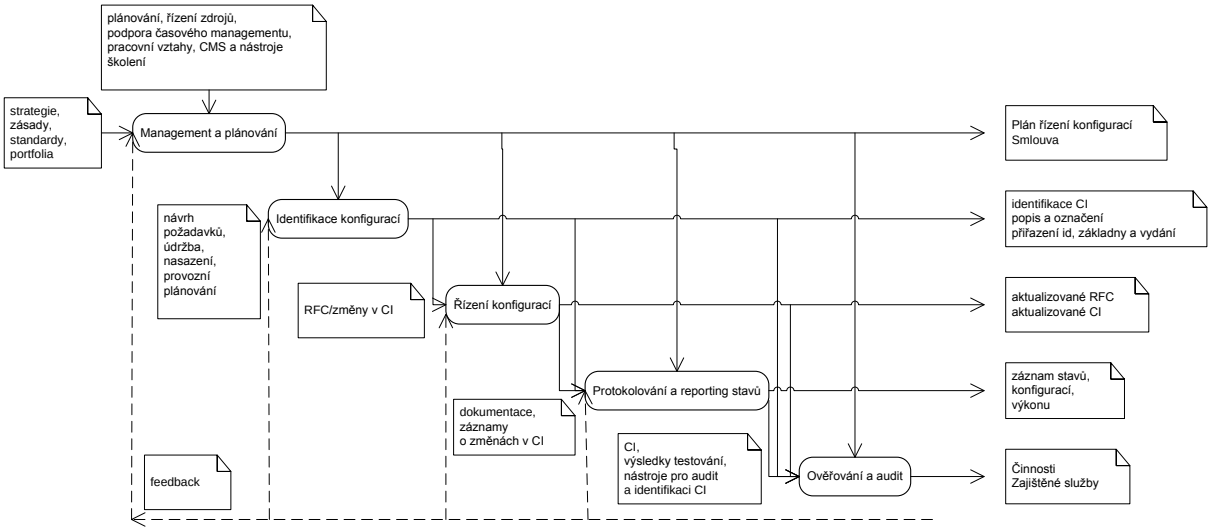
Konfigurace a vazby mezi nimi tvoří model konfigurací.



Obrázek 7 Model konfigurace (zdroj: ITIL v. 3 – Service Transition [9, s. 67])

Obrázek 7 demonstruje příklad modelu konfigurace elektronické bankovní služby (e-banking). Tato služba je součástí portfolia služeb nabízeného bankou a má smluvně garantované parametry (SLA). Dále je podporována službou pro hostování aplikací, která využívá služeb technické infrastruktury. Technická infrastruktura má určitou topologii, síťové služby a dochází v ní k autentizaci přístupů. Z příkladu je patrné, že čím níže se výpadek v hierarchii nachází, tím větší může být jeho dopad na ostatní CI.

Proces správy konfigurací popisuje Obrázek 8.



Obrázek 8 Proces správy konfigurací (zdroj: ITIL v. 3 – Service Transition [9, s. 71])

Z modelu procesu je patrné, že každá fáze může být zpětnou vazbou pro ostatní fáze. To je důležité pro optimalizaci systému a proces zlepšování služeb. Vlevo od činnosti jsou uvedeny vstupní informace (resp. dokumenty) a vpravo pak výstupy jednotlivých činností v procesu.

3.1.1 Management a plánování

Nejprve dochází k vypracování plánu pro řízení konfigurací. Součástí tohoto plánování je i stanovení konfiguračních prvků, které se budou evidovat, z čeho se budou skládat a případně jak se budou seskupovat.

3.1.2 Identifikace konfigurací

V této fázi se identifikují a označují konfigurace. Vyberou se komponenty, které tvoří konfiguraci, a konfigurace se označí jednoznačným identifikátorem. Jednoznačný identifikátor by měl být odvozen od předem definovaných jmenných konvencí. Jmenné konvence by měly obsahovat nejen sériové číslo (odlišující i různé verze), ale vyjadřovat i hierarchii v modelu konfigurací. Konfiguraci se přiřadí relevantní atributy. Doporučené atributy CI jsou:

- jednoznačný identifikátor,
- typ CI,
- název (popř. i popisek),
- verze (sestavení),
- umístění,
- datum dodání,

- informace o licenci (např. ukončení její platnosti),
- vlastník (popř. odpovědná osoba),
- stav,
- dodavatel,
- přiřazené dokumenty,
- přiřazený software,
- vazební typ (k ostatním CI),
- SLA (pokud se na CI vztahuje).

Vzhledem k rozsáhlosti a komplexitě dat je vhodné, aby v případě IT infrastruktury byla tato činnost prováděna automaticky pomocí CMS software a následně pak ve fázi auditu porovnával aktuální konfigurace s databází.

3.1.3 Správa konfigurací

Ve třetí fázi se informace aktualizují, aby odpovídaly reálnému stavu. Děje se tak vždy, když je CI přidána, změněna, nahrazena či odstraněna. Sleduje se:

- licencování,
- změnový management (tj. k jaké změně došlo),
- správa verzí,
- správa přístupu.

Tato činnost může být rovněž iniciována např. požadavkem od uživatele či selháním hw/sw komponenty.

3.1.4 Protokolování a reporting

Pří této činnosti je protokolován stav CI v jeho životním cyklu. Tím může být například:

- koncept (draft/development),
- schváleno (approved),
- nainstalováno (installed),
- vyřazeno (withdrawn).

Každý záznam o stavu konfigurace by měl obsahovat identifikační informace o konfiguraci, konfiguraci, nový stav konfigurace, změny, které byly provedeny, a výsledky testování.

Pomocí reportů pak lze sledovat vývoj ve změnách konfigurací (tracking) a jejich přechod mezi stavy.

3.1.5 Ověřování a audit

V poslední fázi dochází k ověření informací a auditu systému. Tím se ověřuje, zda informace v CMS odpovídají realitě. Ověřuje se aktuálnost dokumentace, fyzická dostupnost CI, či zda jsou nainstalovány autorizované verze softwaru (popř. komponent). Veškeré konflikty by měly být zaprotokolovány.

3.1.6 Metriky procesu

Stejně jako u ostatních procesů i zde je potřeba monitorovat efektivitu těchto procesů. Podle ITIL v. 3 by měly být sledovány následující charakteristiky:

a) Procentuální zlepšení v údržbě aktiv. Údržba by neměla být opomíjena ani prováděna příliš často.
b) Vyváženost údržby a podpory businessu. Údržba by neměla být nákladnější než přínos pro business.
c) Rychlost obnovy provozu služby od nahlášení problému či identifikace incidentu.
d) Míra identifikace aktiv, které způsobují výpadky služeb.
e) Důsledky incidentů na jednotlivé CI.
f) Míra znovupoužitelnosti prvků.
g) Adekvátnost záložních řešení vzhledem k potřebám businessu.
h) Míra využití nakoupených licencí.
i) Průměrné náklady na licenci.
j) Míra dodržení naplánovaného rozpočtu.
k) Procentuální snížení vlivu na chod businessu.
l) Zlepšení výsledků auditu.

Většinu z těchto metrik lze měřit pomocí CMS. Výjimku tvoří zpravidla metriky, kde se měří podpora businessu.

3.1.7 Požadavky na CMS

CMS dle ITIL v. 3 by měl obsahovat následující komponenty:

Knihovny a úložiště

V knihovnách se uchovávají informace o skupinách software, konfigurační soubory apod. V úložištích se pak uchovávají veškerá IT aktiva. Dobrá funkčnost úložišť je důležitá pro zajišťování kontinuity provozu IT infrastruktury, aby v případě výpadku byly k dispozici informace o konfiguracích a podařilo se je na základě toho plně obnovit.

Knihovna médií (Definitive Media Library)

Knihovna médií obsahuje veškeré instalační soubory od schváleného softwaru v patřičné verzi odpovídající jeho uplatnění v konfiguraci.

Konfigurační základna

V konfigurační základně jsou obsaženy informace o konfiguraci klíčových služeb. Tyto informace se mohou změnit pouze v rámci životního cyklu dané služby. Jsou rovněž východiskem pro další plánování zlepšování služeb.

Snapshot

Snapshot je zachycení určitého stavu systému. Snapshoty se vytváří například po instalaci systému. V případě problému mohou být pak porovnávány jednotlivé stavy systému pro jednodušší identifikaci incidentu.

3.2 Správa distribuce služeb

I sebemenší změna konfigurace (např. instalace aktualizace[10]) s sebou nese riziko. Minimalizovat toto riziko má za cíl proces správy a distribuce služeb (Release and deployment management). Konkrétní průběh procesu vychází z fáze Service Design. V pozměněné podobě se může vyskytovat pro konkrétní aplikace jako je například distribuce softwarových balíčků nebo distribuce aktualizací.

[10] Jsou známy případy, kdy po instalaci aktualizace server již nenaběhl a skončil chybou zprávou na modré obrazovce. V případě, že tato situace nastane u několika serverů zároveň, jedná se o velmi vážnou situaci.



Obrázek 9 Proces správy distribuce služeb

3.2.1 Plánování

Nejprve dochází k validaci instalačního záměru, zda je v souladu s pravidly stanovenými ve fázi Service Design. Vyhodnocuje se také, jestli nebudou potřeba další specializované týmy či školitelé.

CMS pro tuto fázi poskytuje informace o stavu IT infrastruktury a instalovaných verzí.

3.2.2 Vytvoření a testování instalačního balíčku

Následuje vytvoření instalačního balíčku. Balíček by měl obsahovat veškeré komponenty aplikace, nastavení a měl by být schopen redistribuce. Balíček by měl být patřičně zdokumentován.

Na základě CMS je vhodné porovnat aktuální a plánovanou konfiguraci a identifikovat vazby a vlivy na ostatní konfigurace.

3.2.3 Testování

Testování je velmi důležitou činností. Ověřuje se, zda může být softwarový balíček bez problémů nainstalován a integrován. Ověřují se parametry služby, že běží v plánovaných rozmezích a že případná komunikační rozhranní odpovídají předem definovaným standardům. Testují se i procesy spojené se službou a jejich integrita v životním cyklu služeb.

3.2.4 Vytvoření plánu a příprava pro instalaci

Dochází k vytvoření plánu pro implementaci. Plán by měl zohledňovat lidské a technické zdroje tak, aby při instalaci nedošlo například k zahlcení síťových prostředků. Probíhá školení zaměstnanců.

3.2.5 Instalace

Dochází k nasazení služby včetně hardware, software a lidských zdrojů. Staré verze a redundantní komponenty jsou odstraněny. Instalace probíhá podle jednoho z distribučních modelů popsaných v kapitole 3.2.9.

3.2.6 Ověření instalace

Instalace je ověřena oproti původnímu plánu. Případné nesrovnalosti jsou zaznamenány, aby mohla být provedena korekční opatření.

3.2.7 Vyhodnocení a uzavření instalace

Po vyhodnocení případných problémů, chyb a negativních efektů na konfigurace při instalaci je implementace služby uzavřena.

3.2.8 Metriky procesu

Mezi tvrdé, jednoznačně měřitelné, metriky patří například počet incidentů u dané služby. Mezi ty měkké pak spokojenost uživatelů.

3.2.9 Modely distribuce služeb

Modely distribuce software popisují principy, kterými se instalují softwarové balíčky na pracovní stanice. Každý model má své výhody a nevýhody, které je zapotřebí pro každý případ zvážit.

‚Big Bang' a fázová distribuce

Při distribuci typu „Big Bang" je instalace provedena současně na všech pracovních stanicích. Tento model je vhodné použít, když je potřeba zachovat konzistenci služby.

Fázová distribuce probíhá v několika fázích, tj. vždy určité množiny pracovních stanic jsou aktualizovány. To může být výhodné například s ohledem na kapacity datových linek. Fázová distribuce má i několik variant, kdy:

- implementace probíhá fázově, ale uživatelům je zpřístupněna najednou,
- implementace probíhá dle uživatelských celků (např. jedna firemní divize),
- jednotlivé typy služeb jsou nasazeny postupně (např. nejdřív hw a pak sw),
- se použije kombinace uvedených variant.

Push a pull

Při Push distribuci je instalace vynucena distribučním serverem. Ten současně definuje, kdy bude instalace provedena a uživatel ji nemůže ovlivnit.

Pull distribuce probíhá na základě požadavku klientské pracovní stanice. Uživatel se tak může rozhodnout, kdy bude distribuční balíček nainstalován. Příkladem této distribuce jsou antivirové systémy.

Obě metody mohou být i zkombinovány. Například tím, že uživateli je umožněno v určitém časovém rozmezí update pomocí metody pull. Pokud však update neprovede je distribuován pomocí metody push.

Automatická a manuální

Automatickou distribucí se rozumí distribuce pomocí softwarových nástrojů či skriptů. Příprava a nastavení automatické distribuce je složitější proces. Ne vždy se proto vyplatí a některé balíčky jsou pak distribuovány manuálně.

Manuální distribucí se rozumí, že instalace je obsluhována a provedena technikem ať už vzdáleně nebo na místě. Manuální distribuce s sebou však nese riziko vzniku chyb. Chybou mohou být nesprávně nastavené parametry při instalaci nebo dokonce vynechání některé klientské pracovní stanice.

4 Nástroje společnosti Microsoft pro správu sítí

Společnost Microsoft prošla ve své dlouhé historii důležitými fázemi ve vývoji informačních technologií. Microsoft má všechny předpoklady uplatnit své nejlepší zkušenosti ve svých produktech.

Jeho dominantní pozice, která podle studie společnosti AT Institute, dosahuje téměř 94% [10], na trhu operačních systémů a na trhu kancelářských aplikací mu do značné míry pomohla prosadit i své ostatní produkty. V oblasti adresářových služeb předstihl i známý Novell Netware, který počátkem 90. let tomuto tržnímu segmentu zcela dominoval. [11]

Nedávno představila společnosti Microsoft novou produktovou linii, Microsoft System Center, která je zaměřena na podporu operativních činnosti při provozu IT infrastruktury. Původní System Management Serveru byl v nové verzi označen jako Configuration Manager a do řady System Center přibyly další nové produkty.

V současné době nabízí společnost Microsoft tyto produkty:

System Center Service Manager

System Center Service Manager analyzuje síťová prostředí a na základě dat z ostatních produktů řady System Center, Active Directory a best practices ze znalostní báze Microsoft Operational Framework a ITIL poskytuje návrhy na zlepšení služeb. Vyhodnocuje při tom údaje ze správy incidentů, problémů změn a rizik. Tato aplikace je zatím pouze ve verzi BETA[11]. Její uvedení na trh se předpokládá v první polovině roku 2010. [12]

System Center Configuration Manager

System Center Configuration Manager je nástroj na správu konfigurací. Identifikuje konfigurace a podává informace o jejich hardware a software včetně jejich verzí. Aplikace současně umožňuje tyto konfigurace hlídat, aby splňovaly definované parametry.

Nechybí ani podpora distribuce operačního systému, software a jejich aktualizací na klientské počítače, servery případně mobilní zařízení. [13]

System Center Mobile Device Manager

System Center Mobile Device Manager umožňuje spravovat mobilní zařízení s operačním systémem Windows Mobile. Pomocí této aplikace lze distribuovat nastavení zabezpečení, připojení VPN a dalších funkcí, případně celé aplikace. [14]

[11] BETA verze je verze publikovaná výrobcem za účelem širšího testování před vydáním komerční verze.

System Center Operations Manager

System Center Operations Manager je řešení pro monitorování IT infrastruktury. Umožňuje sledovat aplikace, operační systémy Windows a síťová zařízení s podporou protokolu SNMP. Tzv. balíčky pro správu obsahují sadu metrik a indikátorů pro monitorování určitého produktu dle jeho best practices. Nechybí ani znalostní báze pro řešení případných incidentů. [15]

System Center Data Protection Manager

System Center Data Protection Manager je aplikace pro real-time zálohování aplikací Microsoft s dynamickými datovými úložišti. Těmi jsou Exchange Server, SQL Server a SharePoint Server. [16]

System Center Virtual Machine Manager

System Center Virtual Machine Manager umožňuje spravovat a řídit prostředky virtuálních serverů. Lze tak například jednoduše převádět fyzické servery na virtuální. [17]

System Center Essentials

System Center Essentials (SCE) je komplexní nástroj pro správu IT infrastruktury, který vychází z produktů Configuration Manager a Operations Manager. Funkcionalita obou produktů je zde oproti oběma plnohodnotným produktům částečně omezena (viz příloha). Toto řešení je určeno pro malé a střední firmy.

Důležitou roli ve správě IT infrastruktury tvoří adresářové služby Active Directory a i řada aplikací využívá jejich služeb. Nechybí mezi nimi ani System Center Essentials. O významu Active Directory pojednává stručně následující kapitola.

4.1 Active Directory

Active Directory (AD) je základním stavebním kamenem síťového prostředí Microsoft. Obsahuje informace o všech významnějších síťových objektech a vazbách mezi nimi a slouží jako zdroj pro řadu aplikací. Nejznámějším příkladem je groupwarový systém Microsoft Exchange a dále pak později popisovaný System Center Essentials. [18]

Základními prvky Active Directory jsou:

- adresářové služby a zásady systémové politiky,
- služby DNS,
- služby DHCP.

Služba Active Directory je poskytována prostřednictvím doménových řadičů. Ty obsahují databáze se síťovými objekty a seskupují je pod jeden jmenný prostor (doména). Objekty Active Directory mohou být uživatelé, počítače, různá zařízení apod. Značnou výhodou je možnost rozšiřování schémat objektů o další atributy (vlastnosti). Lze tak uchovávat o objektech téměř jakékoliv informace. Speciálním objektem jsou bezpečnostní skupiny, které mohou obsahovat další uživatele, počítače či celé skupiny. Správci sítí mohou objekty Active Directory, uspořádávat na vertikální i horizontální úrovni.

Hlavní funkcí Active Directory je autentizace a autorizace síťových objektů podle definovaných přístupových pravidel (ACL[12]).

Zásady skupinového zabezpečení (GPO[13]) upravují nastavení a přístup k aplikacím a komponentám operačního systému.

Active Directory využívá službu DNS (Domain Name Service) pro překlad názvů z jmenného prostoru domén na číselné adresy, aby síťové prvky mezi sebou mohli komunikovat přes IP protokol. Active Directory automaticky replikuje zóny[14] DNS na ostatní řadiče v doméně.

Služba DHCP provádí přiřazování číselných adres síťovým prvkům v počítačové síti. Vzhledem k tomu, že se jedná o kritickou službu, jejíž narušení může vážně ohrozit chod počítačové sítě, disponuje Active Directory seznamem autorizovaných DHCP serverů. V počítačové síti pak fungují pouze autorizované DHCP servery.

4.2 Windows Server Update Services

Windows Server Update Services je služba pro distribuci aktualizací pro produkty Microsoft na počítače a servery v lokální síti. Hlavními přednostmi tohoto produktu jsou nižší vytížení internetové konektivity, kdy každá aktualizace je pro všechny počítače stáhnuta jen jednou, a možnost monitorování stavu instalace aktualizací. Tento produkt je volně dostupný a lze jej provozovat spolu s licencí na Microsoft Windows Server. Podrobněji je proces distribuce aktualizací popsán v rámci System Center Essentials jehož jsou WSUS součástí.

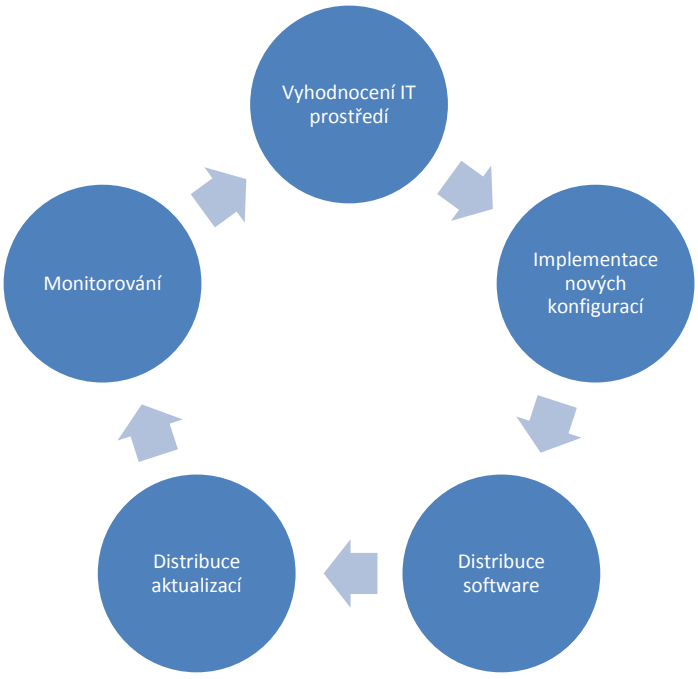
[12] z anglického Access Control List
[13] z anglického Group Policy Object
[14] doménový soubor s DNS záznamy

5 Microsoft System Center Essentials

Microsoft System Center Essentials (SCE) je řešení pro správu a dohled nad IT infrastrukturou. Je určeno pro středně velké organizace s 50 – 500 pracovními stanicemi a maximálně 30ti servery a integruje v sobě nástroje pro monitorování a správu operačních systémů Microsoft Windows, aplikací Microsoft a dalších aplikací[15]. Obsahuje funkce pro:

- distribuci softwarových balíčků,
- distribuci aktualizací,
- proaktivní monitorování IT infrastruktury,
- reporting (inventář hardware, inventář software, statistiky výkonu a incidentů).

Podrobněji budou tyto funkce popsány v dalších kapitolách. V produktu SCE jsou navrženy tak, aby pokrývaly životní cyklus pracovní stanice, jak jej znázorňuje Obrázek 10.



Obrázek 10 Životní cyklus pracovní stanice (zdroj: Microsoft [19])

[15] například Lotus Domino Server, Adobe Photoshop a další (viz [38])

Až na implementaci nových konfigurací pokrývá SCE všechny etapy výše uvedeného životního cyklu. Pod vyhodnocením IT prostředí se rozumí prvotní identifikace konfigurací, která probíhá přes komponentu s názvem Správa počítačů, a při níž se identifikují i další atributy sledovaných objektů. Další komponenty mají shodná jména s činnostmi uvedenými v schématu.

Funkcionalita System Center Essentials je tvořena kombinací aplikací Operations Manager a Configuration Manager. Nejpodstatnějšími rozdíly produktů Operations Manager a Configuration Manager oproti System Center Essentials jsou:

- vyšší škálovatelnost
- podpora replikace
- správa objektů z více domén
- přístupová oprávnění
- vyšší pořizovací náklady

Podrobný přehled rozdílů je uveden v příloze.

I přes výše uvedená omezení, lze SCE značně customizovat a v této oblasti by produkt měl odpovídat požadavkům většiny malých a středně velkých firem [20].

5.1.1 Licencování

Microsoft System Center Essentials podléhá komerční licenci. Licencuje se základní produkt, který dále umožňuje spravovat 50 pracovních stanic s klientským operačním systémem Windows a 10 serverů se serverovým operačním systémem Windows.

Další klientské licence lze dokoupit až do celkového počtu 500 pracovních stanic a 30 serverů. [20]

5.1.2 Nároky na hardware

Výrobce produktu uvádí následující požadavky na hardware pro provoz tohoto produktu:

	Minimální	Doporučené
Essentials 2007 management server	Procesor 1.8 GHz 1 GB RAM 12 GB volného místa na disku (1 GB na systémovém disku)	Procesor 2.8 GHz nebo vyšší 2 GB RAM 20 GB volného místa na disku (1 GB na systémovém disku)
Essentials 2007 konzole pro správu	Procesor 1.0 GHz 512 MB RAM 512 MB volného místa na disku	Procesor 2.8 GHz nebo vyšší 1 GB RAM 512 MB volného místa na disku

Tabulka 3 Přehled systémových požadavků SCE (zdroj: Microsoft [20])

Server, na kterém jsem produkt testoval, odpovídal doporučené konfiguraci. Dle mých praktických zkušeností bych v provozním prostředí nedoporučoval používat SCE na nižší než doporučené konfiguraci. Konkrétní hardwarové nároky se však odvíjejí od velikosti sítě, která má být spravována.

5.1.3 Nároky na software

Serverová aplikace Microsoft System Center Essentials běží výhradně na platformě Windows. Pro svůj provoz si nárokuje alespoň Windows Server 2003. Počítače a servery musí být začleněny do adresářových služeb Active Directory.

Konzole pro správu běží pod serverovými operačními systémy Microsoft Windows 2003 a vyšší a klientskými operačními systémy Microsoft Windows XP[16] a vyšší.

Spravované pracovní stanice musí být výhradně na platformě Windows. V případě serverového i klientského operačního systému je požadována verze 2000 s aktualizací Service Pack 4. Nezbytné je rovněž začlenění pracovní stanice do Active Directory.

Síťové prvky lze monitorovat přes protokol SMNP[17].

[16] Avšak pouze od edice podporující začlenění do Active Directory (tj. Professional/Business či vyšší).
[17] Simple Network Management Protocol – standardizovaný protokol pro správu síťových zařízení.

5.1.4 Nároky na obsluhu

Prostředí pro správu SCE integruje do jednoho místa řadu aplikací a nástrojů pro správu. To značně zjednodušuje obsluhu aplikace. Po spuštění aplikace má správce ihned k dispozici přehled o stavu IT infrastruktury a vyznačené objekty, kde je potřeba servisní zásah. Nechybí ani možnost okamžité notifikace při výskytu kritické události. Správa aplikace je tedy vcelku nenáročná a postačí na ni jeden (popř. více) systémových administrátorů.

Je však potřeba ještě zmínit skutečnost, že SCE neumožňuje řídit přístup ke svým jednotlivým komponentám. Nelze tedy nastavit, že pokud má firma správce databázového serveru, aby měl přístup (pouze) k monitorování databáze. Předpokládá se, že správce SCE spravuje kompletně celou IT infrastrukturu ve firmě.

5.2 Instalace a identifikace prvků

Nasazení System Center Essentials do síťového prostředí není nijak náročné. Instalační průvodce po volbě několika instalačních parametrů provede instalaci všech komponent a nakonfiguruje zásady skupinové politiky (GPO) Active Directory tak, aby klientské stanice získávaly aktualizace a hlásily chybová hlášení přes SCE server. Celý instalační proces trvá dle mých zkušeností v závislosti na výkonu serveru 30 minut až jednu hodinu.

Při instalaci lze využít například již existující instalace produktů Microsoft SQL Server nebo Microsoft Windows Server Update Services (MS WSUS)[18].

Po instalaci je zapotřebí přidat počítače, servery a síťová zařízení, které bude SCE spravovat. Přidávání objektů funguje prostřednictvím průvodce. Vybrat lze automatické vyhledávání objektů či ruční. Oba dva typy využívají informací z Active Directory. Po vyhledání nových objektů proběhne instalace klientské aplikace – agenta, pro monitorování. Automatické vyhledávání a instalace klientů je užitečná zejména v rozsáhlejších sítích, kde dosahuje počet klientů řádů stovek. V této fázi probíhá vyhodnocování IT infrastruktury (viz Obrázek 10)

Agenty pro monitorování je rovněž možné předinstalovat na spravované počítače a po zapojení do počítačové sítě jen schválit jejich správu prostřednictvím SCE.

Po prvotní identifikaci objektů je vhodné je začlenit do skupin. Předdefinovány jsou skupiny pro objekty se serverovým operačním systémem a klientským operačním systémem. Další skupiny lze libovolně vytvářet. Kritéria, podle kterých bývají objekty seskupovány, jsou:

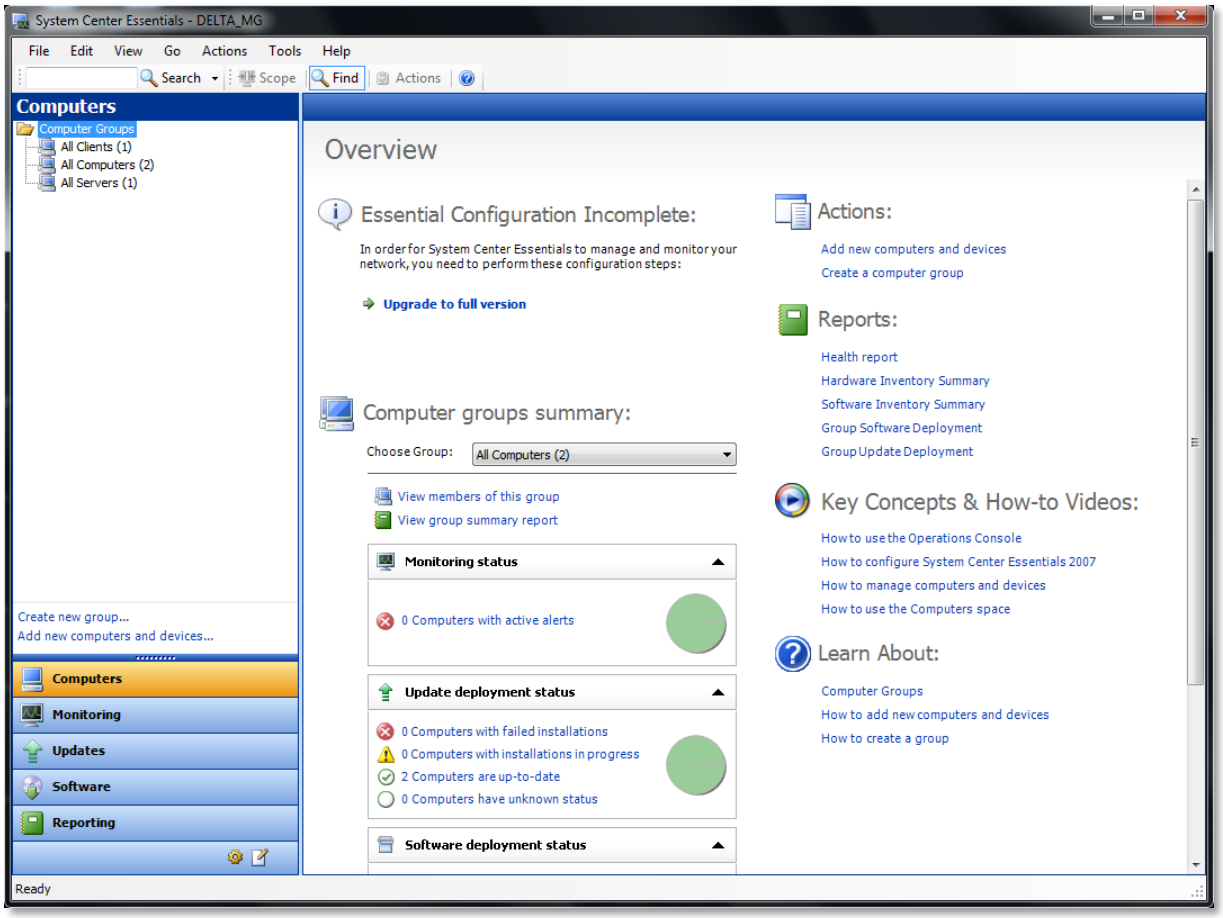
[18] WSUS však musí běžet na stejném serveru, kam bude SCE instalován.

- shodný typ objektu,
- shodný systémový obraz,
- shodná konfigurace,
- shodná organizační úroveň.

Rovněž je vhodné vzít funkční aspekt aplikace SCE a přizpůsobit skupiny monitorování a distribuci software a aktualizací. Jeden objekt může být i součástí více skupin. Prvotní uspořádání skupin by mělo být definováno v návrhu služby.

5.3 Správa počítačů

Správa Microsft System Center Essentials se provádí přes konzoli pro správu. Zde je možné prakticky z jediného místa řídit všechny komponenty aplikace SCE.



Obrázek 11 Přehled správy SCE serveru

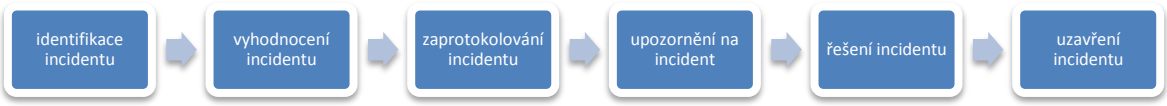
Po spuštění konzole pro správu je obsluze k dispozici agregovaný přehled nad spravovanými objekty dle komponent systému (viz Obrázek 11). Na první pohled je patrné, kolik klientů zaznamenalo nějaký incident, kolik objektů vyžaduje instalaci software či aktualizací nebo kolik klientů již delší dobu nekomunikovalo se serverem SCE.

V navigační části se nachází skupiny se spravovanými objekty. Po vybrání objektu lze v podokně procházet jeho hardwarový a softwarový inventář.

Nabízí se zde i přidání dalších nových objektů.

5.4 Monitorování

Monitorování je stěžejní funkcí Microsoft System Center Essentials. Cílem je identifikovat incidenty a co nejpřehledněji prezentovat a poskytovat relevantní informace pro rychlé rozhodování pro jejich vyřešení. Obrázek 12 znázorňuje proces správy incidentů v SCE.



Obrázek 12 Proces správy incidentů v SCE

První čtyři činnosti jsou v SCE částečně či plně automatizovány.

Identifikace incidentu

První z činností je identifikace problému. SCE monitoruje především dostupnost a výkon hardware a software. Monitorování probíhá pro-aktivně. Na klientských stanicích je nainstalována klientská aplikace[19] - agent, který vyhodnocuje události a výkon systému. Počet metrik se však v systémech Microsoft Windows a dalších aplikacích Microsoft pohybuje v řádech stovek. Důležitou otázkou monitorování tedy zůstává: „co měřit?“. S touto problematikou souvisí nejen volba vhodných metrik, ale i nastavení indikátorů. SCE přichází v tomto směru se značným zjednodušením v podobě tzv. balíčků pro správu. Podrobněji jsou balíčky pro správu popsány v následující kapitole. Prvky v počítačové síti jsou pak monitorovány podle těchto balíčků. Vyhodnocené údaje pak předává SCE serveru.

Vyhodnocení incidentu

V omezené míře lze monitorovat i pracovní stanice a servery bez nainstalovaného agenta. SCE zde využívá komponentu operačního systému Windows: Windows Error Reporting. Windows Error

[19] Klientská aplikace je shodná jako pro System Center Operations Manager.

Reporting shromažďuje informace při kritických chybách systému a běžících aplikací a posílá je dál na SCE server k dalšímu zpracování.

Po identifikaci incidentu je incident klasifikován dle nastavení balíčku pro správu.

Zaprotokolování incidentu

Vyhodnocený incident je zaprotokolován do databáze a je upozorněna obsluha SCE serveru.

Upozornění na incident

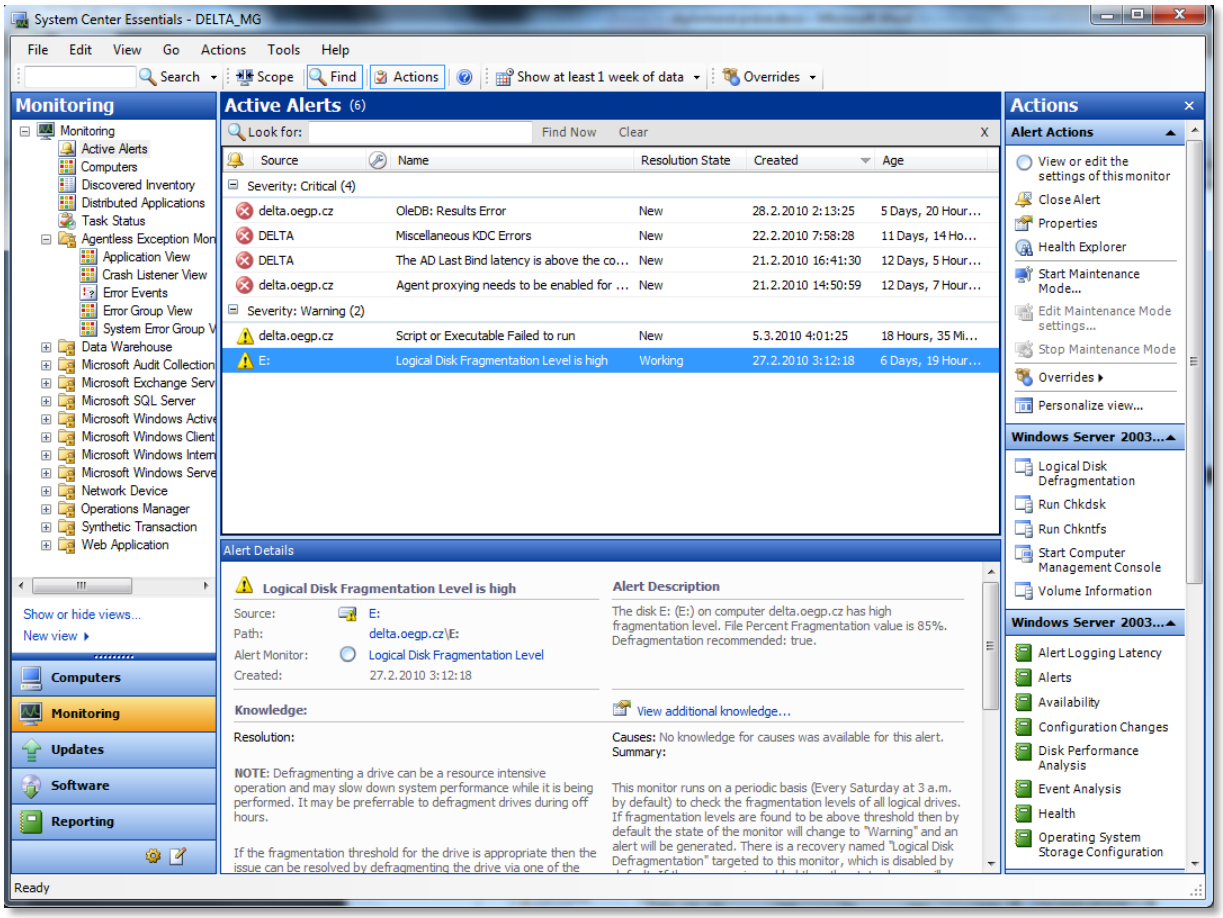
Zpravidla je obsluha SCE serveru upozorněna na nové incidenty prostřednictvím konzole pro správu. Lze však použít i další komunikační kanály (viz Tabulka 4). Pro jednotlivé komunikační kanály lze definovat i parametry incidentu, které budou ve zprávě posílány (např. čas vzniku incidentu, zasažená služba, atd.).

Přehled komunikačních kanálů pro notifikaci v SCE:	
E-mail	Standardní zpráva elektronické pošty přes SMTP protokol.
Rychlé zprávy	Odešle rychlou zprávu přes SIP[20] protokol.
SMS	Krátká textová zpráva na mobilní telefon.
Příkazová řádka	Spustí příkaz příkazové řádky s definovanými parametry.

Tabulka 4 Přehled komunikačních kanálů v SCE

[20] Session Iniciated Protocol

Obrázek 13 zobrazuje přehled aktuálních incidentů.



Obrázek 13 Přehled aktuálních incidentů

Incidenty jsou řazeny dle závažnosti a dále pak dle stáří incidentu.

V podokně s podrobnostmi o incidentu má obsluha k dispozici:

- informace o zdroji incidentu a časovém údaji jeho výskytu,
- informace o příčině incidentu,
- stručné vysvětlení incidentu,
- možnosti řešení incidentu,
- odkaz na zobrazení dalších znalostí (Produktových a Podnikových).

Složitější incidenty bývají někdy popsány zjednodušeně, aby je obsluha mohla rychle vyhodnotit i bez podrobných znalostí zasaženého systému.

Ve vlastnostech incidentu může obsluha SCE specifikovat:

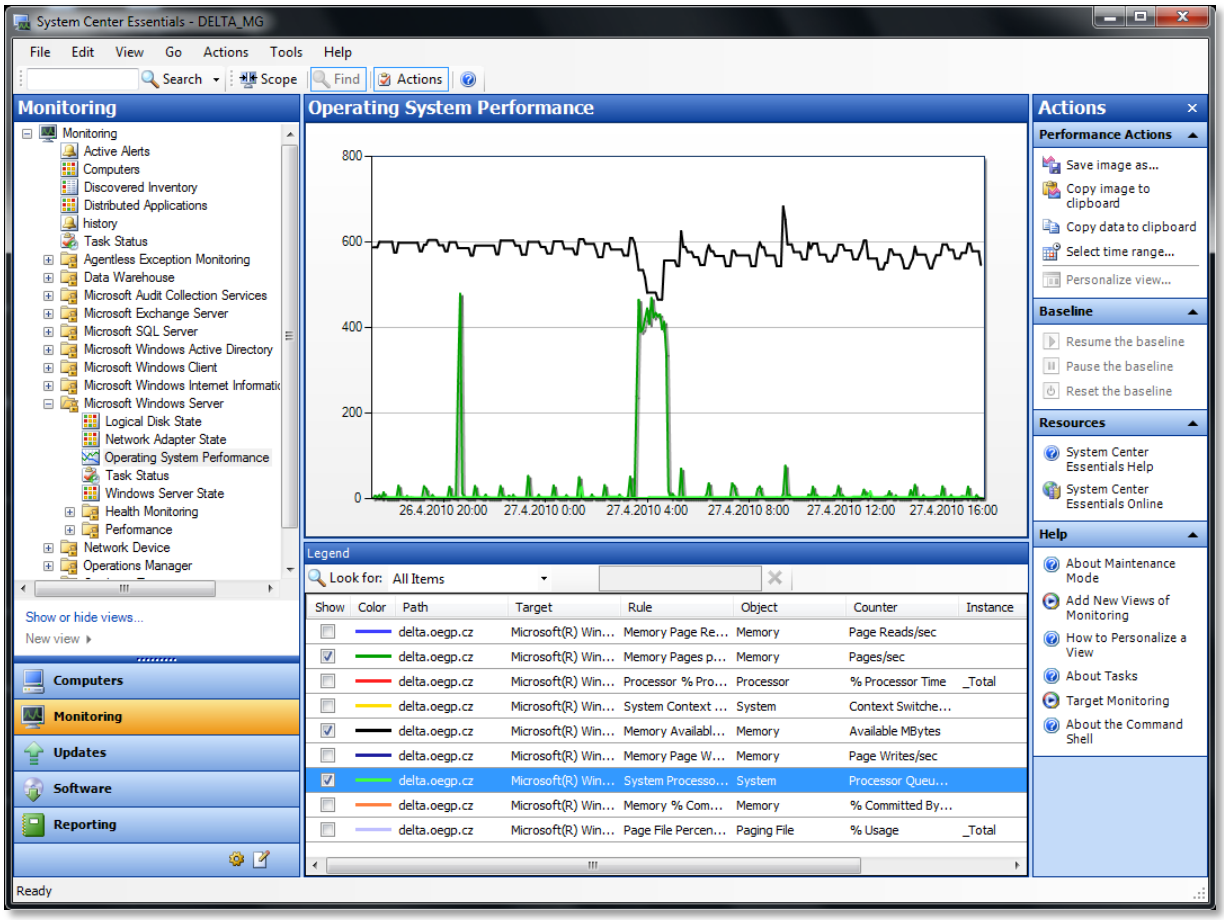
- vlastníka, tedy osobu, která se bude incidentem zabývat,
- identifikační číslo ticketu,
- stav (nový, customizovaný, uzavřený),
- podnikové znalosti k incidentu,
- další customizovaná pole.

Řešení incidentu

V pravé části jsou k dispozici vybrané diagnostické nástroje a nástroje pro vzdálenou správu s ohledem na zdroj incidentu a balíček pro správu. Následují reporty pro objekt, na kterém se incident vyskytuje. Pokud se na počítači či serveru budou při řešení incidentu provádět úpravy na konfiguraci, je možné aktivovat tzv. „režim údržba“. U objektů v tomto režimu nejsou vyhodnocována chybová hlášení ani degradace výkonu.

Po vyřešení incidentu se změní jeho stav na „uzavřený“ a tím incident zmizí z okna aktuálních incidentů.

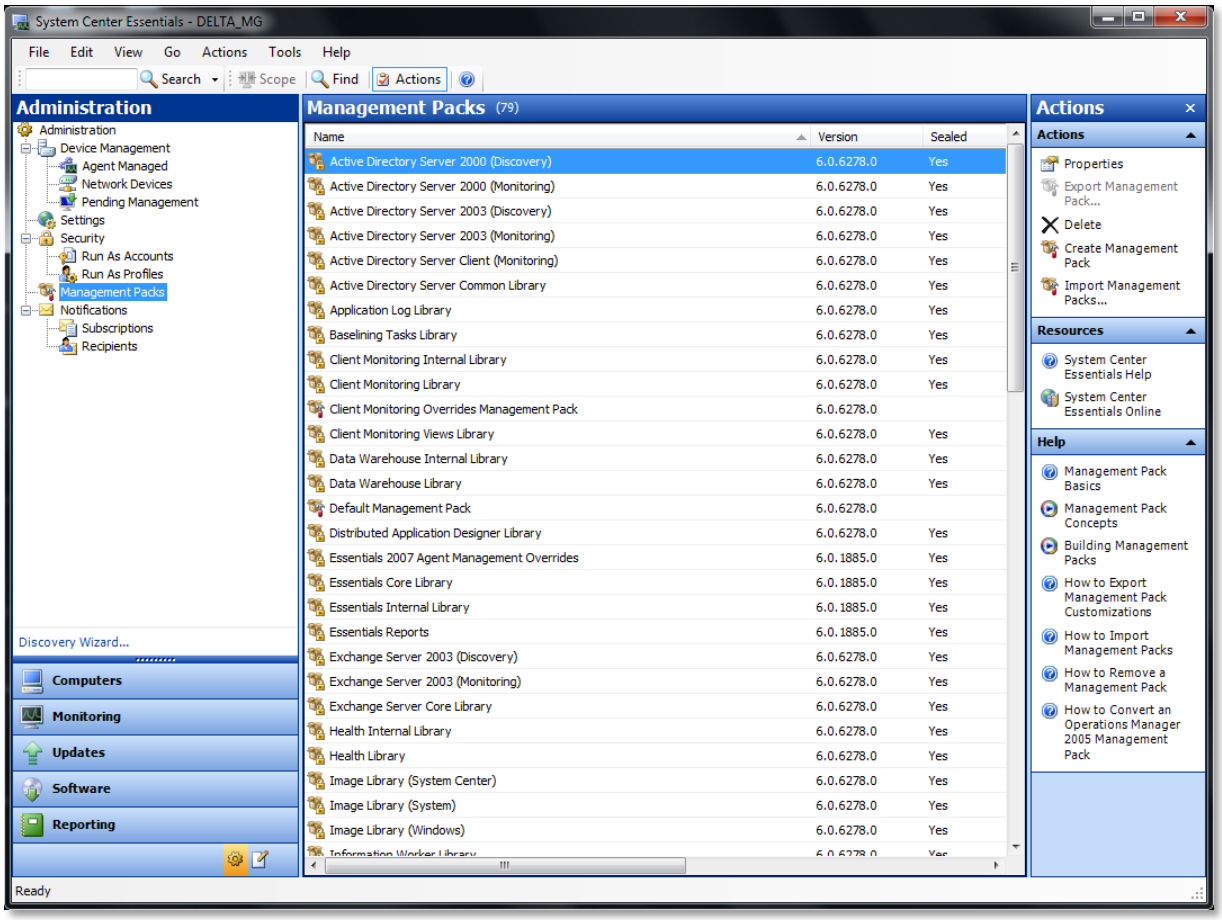
Další náhledy umožňují zobrazit stav (žádoucí/nežádoucí) sledovaných komponent jednotlivých objektů. Nabízí se i možnost sledování využití hardwarových prostředků serverů resp. pracovních stanic (viz Obrázek 14) či počty transakcí v relačních databázích.



Obrázek 14 Monitorování výkonu v SCE

5.4.1 Balíčky pro správu

Balíčky pro správu (Management Packs) obsahují přednastavené metriky a indikátory zpravidla pro určitý softwarový produkt. Jsou navrženy jako best practises pro zajištění spolehlivého provozu systémů. Zároveň obsahují databáze znalostí (expertízy) jak řešit případné problémy.



Obrázek 15 Balíčky pro správu v SCE

SCE je dodáván s přeinstalovanými balíčky pro správu pro nejběžnější produkty Microsoft, kterými jsou:

- Windows,
- Office,
- Exchange Server,
- SQL Server,
- SharePoint a další.

Další balíčky pro správu nebo aktualizované verze těch předinstalovaných lze stáhnout z webových stránek společnosti Microsoft. V případě, že mají být monitorovány novější verze operačních systémů jako je Windows Vista a Windows 7, je doinstalování patřičného balíčku pro správu nezbytné. V portfoliu se nabízí i balíčky pro správu produktů a zařízení jiných než od společnosti Microsoft. Některé balíčky jsou placené. Balíčky jsou rovněž kompatibilní se systémem Microsoft Operations Manager.

Balíčky pro správu v sobě obsahují znalostní bázi ke všem chybám, které jsou schopny identifikovat. Tato báze je v SCE označována jako Produktová znalost. Do Balíčku pro správu lze přidat i tzv. Podnikovou znalost (company knowledge), která se váže k chybě v daném podnikovém prostředí. Do Podnikové znalosti lze uvést například pracovní postup, který vedl k vyřešení incidentu, pokud incident v minulosti již nastal.

Balíčky pro správu se zpravidla skládají z dalších menších balíčků pro správu, které se zaměřují na konkrétní oblasti produktu a ošetřují odlišnosti různých verzí. Například balíček s označením „Windows Client Operating System Management Pack for Operations Manager 2007“ lze dekomponovat na (zjednodušené schéma):

- Windows Client
    - Windows Vista Client
    - Windows 7 Client
        - Windows 7 business critical operating systems
        - Windows 7 (agregátní)
        - Windows 7 (monitoring)
            - Monitorování výkonu
            - Monitorování stavu systému (health)

Za povšimnutí ve výše uvedeném schématu stojí balíček s přívlastkem „business critical operating systems“. Tento balíček obsahuje přísnější nastavení indikátorů nežádoucích stavů systému.

Následující tabulka uvádí přehled, co vše balíček pro správu obsahuje:

Metriky	Vymezení, co bude monitorováno.
Indikátory	Indikátory představují prahové hodnoty, které když jsou překročeny, představují incident
Znalostní báze	Znalostní báze obsahuje postup pro řešení známých problémů.
Reporty	Definice pro vytváření statistik monitorovaných metrik.

Tabulka 5 Přehled obsahu balíčku pro správu

Balíčky pro správu dokážou identifikovat většinu chyb, které se mohou na serveru či pracovní stanici vyskytnout. Z vlastní zkušenosti mohu potvrdit, že ne všechna chybová hlášení jsou přeposílána na SCE server:

Příklad:

U jednoho ze spravovaných serverů selhal záložní zdroj napájení (UPS) a chybně komunikoval se serverem. Důsledek tohoto incidentu byl, že se na serveru v intervalu přibližně jednou za 24 hodin objevila tzv. „modrá obrazovka smrti" (BSOD) a server se restartoval. V protokolu událostí byla zaznamenána kritická chyba jádra systému (Kernel Power Manager). V konzoli pro správu SCE se však zobrazilo pouze, že server byl na okamžik nedostupný.

Případy, kdy balíček pro správu nepokrývá určité mimořádné stavy systému, lze ošetřit customizací monitoringu (viz kapitola customizace) či doinstalováním patřičných balíčků pro správu.

5.4.2 Možnosti customizace monitorování

Monitorování lze přizpůsobovat pro potřeby organizace. Možnosti customizace shrnuje následující přehled.

SCE umožňuje upravovat:	
Indikátory	Prahové hodnoty, od kterých se systém resp. aplikace nachází v nežádoucím stavu.
Monitorování	Komponenty systému resp. aplikace, které budou monitorovány.
Incidenty	Události, které budou považovány za incidenty.

Tabulka 6 Přehled customizace monitorování v SCE

5.4.2.1 Úpravy prahových hodnot

V některých situacích je žádoucí upravit prahové hodnoty pro vyhodnocování dat z monitorování. Pokud se jedná o kritické systémy, mohou být prahové hodnoty přísnější v opačných případech třeba benevolentnější.

Příklad:

Firma vlastní detašované pracoviště, malou kancelář, s deseti pracovníky na druhém konci republiky. Každý z pracovníků má vlastní počítač. Lokální počítačová síť je propojena tunelovým připojením přes Internet s hlavní počítačovou sítí firmy. To však značně zvyšuje síťovou odezvu[21]*. Aby nedocházelo k poplašným alarmům, například při větším vytížení sítě, je vhodné posunout prahovou hodnotu vypršení odpovědi o přiměřenou hodnotu.*

5.4.2.2 Aktivace a deaktivace monitorování objektů

Proces monitorování vyžaduje i sám pro sebe systémové prostředky. Vypnutím monitorování objektů, které nejsou pro firmu příliš relevantní, lze optimalizovat výkon systému.

V jiných případech je žádoucí monitorování některých objektů aktivovat. Těmi mohou být diagnostika systému (mimořádné monitorování) nebo dodatečné monitorování pro vyšší zajištění služeb.

5.4.2.3 Vytvoření nového monitorování objektu

SCE umožňuje definovat nové monitorování objektu. Monitorovat lze:

- připojení k databázi přes rozhraní OLE[22],
- TCP port,
- webovou službu,
- služba systému Microsoft Windows.

Připojení k databázi přes rozhraní OLE

Tato funkce umožňuje monitorovat dostupnost databází prostřednictvím rozhranní OLE. V průvodci se stačí specifikovat pouze OLE připojení a parametry jak často má být připojení k databázi monitorováno[23].

[21] ICMP echo request
[22] Object Linking and Embedding
[23] Standardní hodnota je 2 minuty.

TCP port

Tato funkce umožňuje monitorovat, zda je na vzdáleném počítači otevřený specifikovaný TCP port. Dle stavu TCP portu lze určit funkčnost síťové rozhraní služby.

Webová služba

Funkce monitorování webové služby umožňuje monitorovat v stav a částečně i výkon webových služeb. Základem je specifikování odkazu na webovou službu, která má být monitorována. Testy jsou opakovány v pravidelných intervalech a zahrnují sledování:

- stavového kódu HTTP odpovědi serveru,
- odezvy serveru,
- shody obsahu.

Další sledovatelné parametry lze nastavit v rozšířených možnostech. Monitorovat lze převážnou většinou webových služeb a uplatnění této funkce je široké.

Služba systému Microsoft Windows

Tato funkce umožňuje sledovat službu Windows, zda služba běží či neběží.

K výše uvedeným monitorováním lze přidat atributy služby, které mají být dodržovány. V opačném případě SCE hlásí chybnou konfiguraci či následuje další zpracování incidentů.

Příklad:

Firma používá pro ochranu svých počítačů a serverů před počítačovými viry, adware a rootkity řešení od společnosti AVG Technologies. Součástí tohoto řešení je serverová aplikace AVG DataCentre, která spravuje klientské stanice. Firma by ráda prostřednictvím SCE monitorovala dostupnost a výkon AVG DataCentre.

AVG DataCentre se skládá ze serverové aplikace, která běží jako služba v operačním systému a SQL databáze (v tomto případě například Microsoft SQL Server Express Edition). S klienty komunikuje prostřednictvím portu TCP 4158.

Řešení monitorování této aplikace by v SCE vypadalo následovně: Do nově vytvořeného balíčku pro správu se vytvoří objekty monitorování pro jednotlivé komponenty systémy. První objekt

monitorování bude sledovat protokol TCP, zda je port 4158 na serveru dostupný a otevřen pro připojení klientů. Druhý objekt monitorování bude sledovat připojení SQL databáze, zda je k dispozici. Poslední objekt monitorování bude sledovat službu AVG DataCentre, zda běží. Vytvořený balíček lze doplnit o znalosti pro řešení problémů z dokumentace software.

5.4.2.4 Úprava zobrazení incidentů

Konzoli SCE lze doplnit o customizovaná zobrazení incidentů, událostí, stavů, výkonnostních ukazatelů apod. Balíčky pro správu sice mnoho zobrazení (views) obsahují, ale v závislosti na procesech řízení IT ve firmě, v nich mohou některé informace chybět. Pokud firma využívá například systém ticketů pro řešení incidentů a problémů, bude například pro obsluhu potřeba, aby měla k dispozici u každého incidentu i číslo ticketu v hlavním přehledu incidentů.

Pomocí customizovaných zobrazení lze zobrazit i uzavřené incidenty, které přes standardně implementovaná zobrazení nejsou přístupná.

5.5 Distribuce software

SCE umožňuje distribuovat software na klientské pracovní stanice a servery. Proces distribuce software dle SCE znázorňuje Obrázek 16.



Obrázek 16 Proces distribuce software (zdroj: Microsoft [19])

Software je na klientské stanice distribuován prostřednictví tzv. instalačního balíčku. Instalační balíček obsahuje instalační soubory, nastavení instalátoru (pokud je potřeba) a v některých případech i přednastavení instalované aplikace[24].

Vytváření instalačních balíčků probíhá prostřednictvím průvodce. Podporovány jsou instalátory ve formátu EXE a MSI. Do balíčku je možno zahrnout i více souborů, pokud je instalátor vyžaduje. [21]

Hotové instalační balíčky jsou přiřazeny ke skupině či skupinám počítačů a po jeho schválení je balíček instalován na pracovní stanice. Distribuční skupiny často kopírují skupiny, ve kterých jsou počítače spravovány. Pokud je však potřeba vytvořit dodatečné skupiny například kvůli instalaci odlišných verzí, lze tak učinit jak bylo uvedeno v kapitole Správa počítačů.

Ačkoliv schéma společnosti Microsoft tuto činnost neuvádí, domnívám se, že je vhodné vzdálenou instalaci nejdříve odzkoušet v testovacím prostředí. Z vlastní zkušenosti vím, že některé balíčky MSI nepodporují plně vzdálenou instalaci. Testováním se rovněž ověří, zda je instalovaný software kompatibilní s vyžadovanými systémovými komponentami a ostatním software.

Instalace probíhá automaticky a obsluha serveru je nemůže ovlivnit. Klient kontroluje dostupnost nových softwarových balíčků přibližně každých 22 hodin, a pokud jsou nové balíčky k dispozici, sám si instalační balíček ze serveru stáhne a nainstaluje.

Prostřednictvím reportů pak obsluha získává statistiky o provedených instalacích a jejich stavech.

5.6 Distribuce aktualizací

Proces instalace aktualizací probíhá v prostředí SCE podobně jako v případě instalace software (viz Obrázek 17).

[24] např. Microsoft Office lze takto přednastavit



Obrázek 17 Proces distribuce aktualizací (zdroj: Microsoft [19])

Aktualizace jsou však již vytvořené a jsou přejímány ze serverů služby Microsoft Update. Kontrolu dostupnosti aktualizací doporučuje společnost Microsoft provádět v nočních hodinách, kdy datové linky nebývají tolik vytíženy. Aktualizace lze ukládat na SCE server a klienti si je pak stahují přímo z SCE serveru, což snižuje zátěž firemní konektivity do Internetu.

Nové aktualizace jsou zařazeny ke schválení. V ideálním případě jsou aktualizace otestovány v testovacím prostředí, a pokud jsou shledány v pořádku, jsou schváleny k instalaci do produkčního prostředí. Schvalovat lze aktualizace pro všechny skupiny i pro jednotlivé skupiny zvlášť. V SCE je dále k dispozici automatické schvalování aktualizací k instalaci. To je vhodné například pro počítače testovacího prostředí.

Dle mých zkušeností z praxe si některé menší firmy nemohou dovolit dodatečné pracovní stanice a servery pro testovací prostředí. Jako alternativa jsou aktualizace testovány v tzv. pilotním testování. Aktualizace jsou nejdříve nainstalovány na vybrané vzorky pracovních stanic (zpravidla méně důležité pro chod společnosti) a až po té do produkčního prostředí.

Aktualizace získávají klienti automaticky, podobně jako je tomu u služby Microsoft Update. Na SCE serveru se pak uchovávají výsledky instalací aktualizací. Je tak možné zjistit kteří klienti nejsou aktualizovaní či kde instalace aktualizací selhala.

Proces distribuce aktualizací je částečně automatizován už v operačních systémech klientů. Díky SCE však lze určit, jaké aktualizace budou instalovány a stav aktualizací monitorovat. Navíc lze takto distribuovat nové opravné balíčky (service pack) a nové verze některých komponent systému Windows (např. Internet Explorer), které přes Microsoft Update nejsou automaticky instalovány a vyžadují pro instalaci schválení správce systému a přijmutí licenčního ujednání.

Distribuce aktualizací v SCE je prakticky shodná s produktem Microsoft Windows Server Update Services (MS WSUS). SCE je však koncipován jako jediný server pro distribuci aktualizací v síti a proto SCE neumožňují replikaci databáze aktualizací jako tomu je u WSUS. Oproti WSUS však umí

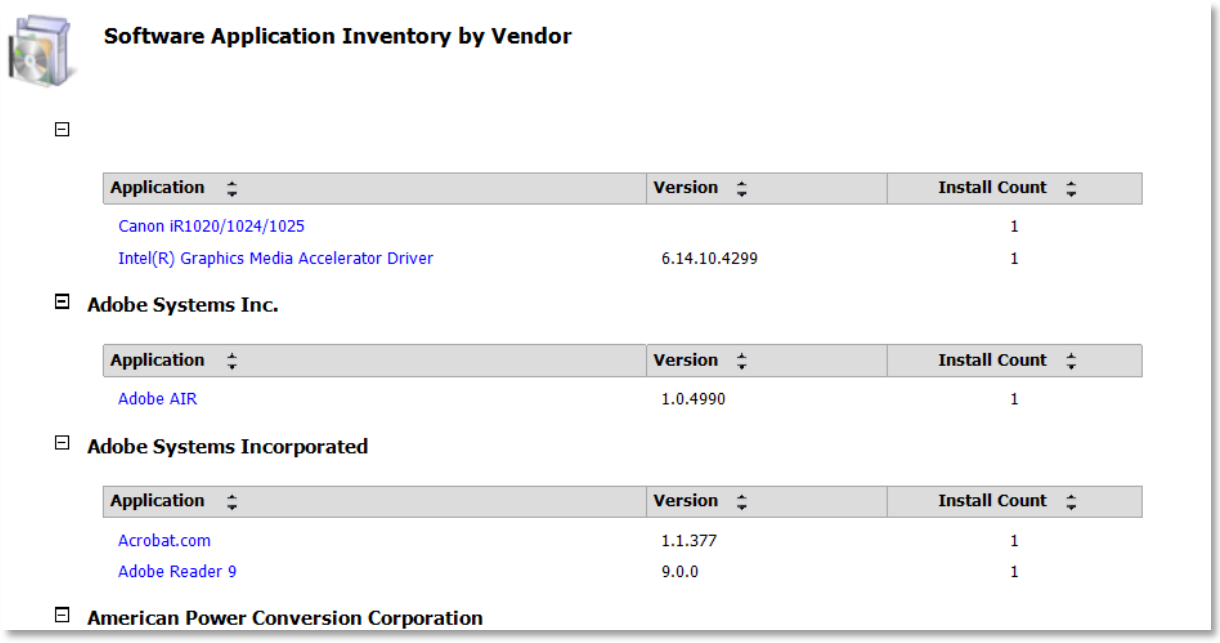
vytvářet aktualizace produktů třetích stran. Proces distribuce aktualizací třetích stran je shodný jako u aktualizací společnosti Microsoft.

5.7 Reporting

Reporting umožňuje správcům System Center Essentials generovat agregované statistiky za určité období pro zvolené objekty monitorování. Analyzované proměnné jsou dané šablonou reportu. Reporty se mohou uplatnit nejen z hlediska dlouhodobého sledování výkonu systémů, ale i jako podklad pro další procesy řízení IT ve firmě.

Šablony pro reporty jsou součástí balíčků pro správu. Balíček pro správu klientů Windows tak umožňuje vytvářet statistiky například pro využití pevných disků či dobu startování (bootování) operačního systému. Balíčky pro správu obsahují reporty z převážné většiny jako statistiku využití prostředků. Statistika obsahuje zpravidla extrémní hodnoty, průměrnou hodnotu a běžnou odchylku.

Reporty v SCE již zahrnuté umožňují generovat hardwarový a softwarový inventář. Inventáře jsou k dispozici buď pro jednotlivé počítače, nebo pro celé skupiny (viz Obrázek 18).



Obrázek 18 Ukázka softwarového inventáře v SCE

Pro vyhodnocování splňování SLA či OLA[25] se může hodit report se statistikou dostupnosti. Dále jsou k dispozici například reporty vyhodnocující četnost incidentů. Některé reporty pro hodnocení výkonu procesu (například „doba řešení incidentu“) SCE neobsahuje.

System Center neumožňuje vytvářet customizované reporty a ukládá veškerá data po dobu nejvýše 40 dnů. Obě tyto skutečnosti představují poměrně značné omezení při vyhodnocování nasbíraných dat.

5.8 Příklad řešení některých úkolů v SCE

Tato kapitola popisuje řešení některých typických situací, které mohou nastat při správě IT infrastruktury.

Změna komponent počítače

Pokud se na žádost uživatele či v důsledku incidentu například vymění síťová karta v počítači, System Center Essentials tuto změnu neprotokoluje. V inventáři hardware je nový hardware uveden, ale ve změnách v konfiguraci záznam o změně chybí.

Změnu nelze ani zaprotokolovat ručně. Pokud by se vyskytnul incident v souvislosti například již zmíněné síťové karty, správa IT infrastruktury by neměla z SCE informaci, že na počítači byla karta měněna.

Re-instalace počítače

V některých případech (například při neopravitelné poškození operačního systému či po výměně pevného disku) musí být počítač re-instalován.

Důsledkem re-instalace se zpravidla zruší vazba mezi klientem a server SCE. Pro obnovení vazby lze v SCE použít nástroj na opravu instalace agenta popřípadě počítač z SCE odebrat a následně znovu přidat.

Pokud název počítače po re-instalaci zůstane shodný jako před instalací, lze navázat na již prováděné monitorování. Do statistik se tak započítávají údaje před i po re-instalaci.

[25] z anglického Operational Level Agreement

Přenosné počítače

Přenosné počítače vyžadují speciální pozornost při začlenění do SCE. Oproti stolním počítačům se notebooky často používají v různých počítačových sítích, kde prostředky domácí počítačové sítě nemusí být dostupné. Tyto situace generují zpravidla chybné události o nedostupnosti služeb[26].

Standardně tyto události nejsou vyhodnocovány jako incidenty dle balíčků pro správu dodávaných s SCE.

Pokud by bylo vyhodnocování těchto událostí jako incidentů standardně zapnuto, je možné pro přenosné počítače vyhradit speciální skupinu, kde bude protokolování těchto incidentů vypnuto. Nevýhodou tohoto opatření je, že pokud by se vyskytl relevantní incident v domácí síti, nebyl by zaprotokolován.

[26] většinou se jedná o služby související s Active Directory, dostupností řadičů domény, stahování zásad zabezpečení apod.

6 Podpora procesů ITIL aplikací SCE

Z předchozí kapitoly je patrné, že společnost Microsoft vyvíjí své produkty tak, aby v sobě obsahovaly nejlepší zkušenosti při správě služeb. O tom jak dalece nejlepší zkušenosti společnosti Microsoft odpovídají praktikám ITIL pojednává tato kapitola.

Na začátek uvádím přehled pokrytí jednotlivých fází rámce ITIL (kapitola 1) aplikacemi pro správu společnosti Microsoft (kapitola 3).

ITIL	Aplikace Microsoft
Service Strategy	-
Service Design	-
Service Transition	System Center Configuration Manager, System Center Mobile Device Manager, System Center Essentials
Service Operation	System Center Operations Manager, System Center Data Protection Manager, System Center Service Manager, System Center Essentials
Continual Service Improvement	System Center Service Manager

Tabulka 7 Přehled podpory jednotlivých částí ITIL produkty Microsoft

První dvě fáze nejsou přímo podporovány žádným ze softwarových nástrojů. Informační strategie a služby by měly být navrhovány specificky podle obchodní strategie firmy. Při návrhu služeb však lze využít některé informace z aplikací System Center, zejména v agregované podobě z reportů.

Fázi Service Transition podporují produkty Confirguration Manager, Mobile Device Manager a Essentials nástroji pro inventarizaci síťových prvků a distribucí software a aktualizací.

Service Operation lze podpořit produkty Operations Manager a Essentials pro monitorování sítě a zpracování událostí z jednotlivých konfigurací. Data Protection Manager zastává funkci real-time zálohování dat.

Pro Continual Service Improvement umožňuje System Center Service Manager ukládat potřebná data z ostatních aplikací řady System Center.

6.1 Správa událostí, incidentů a problémů

Z kapitoly 5.4 je patrné, že monitorování v SCE se do značné míry podobá procesům dle ITIL v. 3. Nyní se zaměřím na jednotlivé činnosti ITIL a popíši, jak jsou podporovány v SCE.

6.1.1 Správa událostí

ITIL v. 3	System Center Essentials
vznik události	
Události vznikají soustavně. U každé služby lze nadefinovat, které události budou zaznamenány	Události, které jsou zaznamenávány (např. v protokolu událostí operačního systému), nelze pomocí SCE ovlivnit. Ty jsou dány buď výrobcem, nebo je lze nastavit u dané aplikace/služby.
upozornění na události	
K upozornění na události dochází během monitoringu. **Typy monitoringu uvádí kapitola 2.1.2.**	V typických případech provádí SCE proaktivní monitorování prostřednictvím softwarového agenta, který je nainstalován na klientské stanici. Pasivní monitorování lze použít pro monitorování bez agenta. V tomto případě odešle komponenta Windows Error Reporting chybovou zprávu na SCE server. Přes aktivní monitorování jsou sledovány v SCE webové služby a dostupnost datových zdrojů[27]. Na monitorování výkonu služeb je použito průběžné monitorování.

[27] Konkrétně databáze SQL přes platformu ODBC.

Detekování události	
Probíhá detekování události pro její případné další zpracování.	Tato činnost je prováděna automaticky: přes softwarového agenta Windows Error Reporting SCE serverem při aktivním monitorování

Odfiltrování události	
Vyberou se události, které budou dále zpracovávány nástrojem pro správu a dohled nad sítí	SCE filtruje události prostřednictvím balíčků pro správu.

Klasifikace událostí	
Události jsou klasifikovány podle toho, zda s sebou nesou riziko nedostupnosti služeb.	V SCE jsou události klasifikovány plně v souladu s metodikou ITIL v. 3 tedy jako: výjimka, varování, informace.

Korelace událostí	
Korelace událostí vyhodnocuje události dle daných kritérií a určí tím míru dopadu na chod businessu.	Korelace událostí je v SCE částečně podporována. Opakované události se seskupují a v přehledu událostí je vidět pouze datum posledního výskytu. U události je pak uveden celkový počet výskytů. Pokud však nastanou dvě kritické události, SCE nedokáže vyhodnotit, která z nich je závažnější a měla by být řešena prioritně popřípadě, zda spolu tyto události nesouvisí.

Příklad: V důsledku chyby ve skriptu zůstává procesor databázového serveru vytížen na 100%. To samozřejmě ovlivní i výkon aplikací, které na něm běží. System Center Essential, které server monitorují, identifikují incidenty „Výkon procesoru je trvale na 100%“ a „Databázový server má dlouhou odezvu“. Bohužel však nedokáže určit, že ta dlouhá odezva je způsobena vytížením procesoru.

Trigger a Reakce na událost	
Na základě korelace události je zahájena další činnost: **zaznamenání incidentu/problému** **žádost o změnu** **spuštění skriptu** **kontaktování osoby** **úprava přístupu k databázi**	V závislosti na vyhodnocení události, může SCE automaticky podniknout určitá opatření. Informativní události jsou zpravidla zaprotokolovány na spravovaném objektu. V případě sledované služby pak i na SCE. Výjimkou je například změna stavu spravované služby. Problémy a incidenty (tj. v SCE události klasifikované jako varování či výjimka) jsou automaticky zobrazeny obsluze SCE v konzoli pro správu. Dále může být automaticky spuštěn definovaný skript či upozorněna kontaktní osoba jedním z notifikačních kanálů (viz kapitola 5.4). Omezení přístupu k databázovým zdrojům není možné. SCE spravuje problémy a incidenty v jednom procesu. To vede k určitým omezením, která jsou patrná z následující kapitoly. Zaznamenávání žádostí o změnu SCE nepodporuje vůbec. To lze však zajistit pomocí aplikace System Center Service Manager.

Revize činností	
Řešení vážnějších událostí, které nějakým způsobem narušily chod IT infrastruktury, by mělo být revidováno.	U incidentů se předpokládá revize lidským faktorem. Pokud by se například jako důsledek události špatně provedl korekční skript, skončí celá záležitost pravděpodobně incidentem, který je nutno opět řešit.

Uzavření události	
Formální uzavření události.	Incidenty jsou v SCE uzavřeny při jejich uzavření v procesu správy incidentů. Informativní události jsou uzavřeny změnou stavu služby.

6.1.2 Metriky správy událostí

Pro sledování výkonu tohoto procesu jsou definovány metriky (viz kapitola 2.1.11).

Jak již bylo zmíněno, SCE umožňuje generovat agregované výstupy pomocí funkce Reporting. Reporty jsou však definované balíčky pro správu a nelze je dále upravovat.

Důležitým aspektem je, že SCE umožňují vyhodnocení reportingem pouze varování a výjimky. Informativní události nejsou předmětem vyhodnocení.

Následující tabulka uvádí metriky procesu správy událostí a jejich podporu prostřednictvím reportů v SCE.

Počet událostí v určité kategorii či určitého typu celkem a dle jednotlivých platforem	SCE umožňuje vytvořit reporty s těmito informacemi prostřednictvím balíčku „Generic Reports Library“.
Počet a procento událostí, které vyžadovaly lidský zásah.	Tento údaj nelze v SCE určit. I incidenty, které se „samy vyřešily“ (například restartováním aplikace/služby) jsou zaprotokolovány. Obsluha SCE by měla ověřit, zda aplikace po tomto automatickém opatření běží správně. Prakticky tedy všechny incidenty v SCE vyžadují lidský zásah.
Počet a procento událostí, které byly identifikovány jako incident/změna	Tento údaj není v SCE přímo k dispozici. Lze však určit počet událostí, které byly informativního, varovného či chybového typu. Správu změn SCE nepodporuje.
Počet a procento událostí, které byly zaviněny známou chybou	SCE neumožňuje správu známých problémů. Tato informace je však dostupná uživatelům aplikace System Center Service Manager. [12]
Počet a procento událostí, které: **se opakují,** **poukazují na degradaci výkonu služby,** **poukazují na dostupnost služby.**	V SCE jsou prostřednictvím reportů k dispozici počty opakujících se událostí. Ačkoliv nelze zobrazit přímo počty událostí související s dostupností, lze sestavit graf s dostupností ve zvoleném časovém intervalu. Události související přímo s degradací výkonu služby taktéž nelze zobrazit. Lze však podobně, jako je tomu u dostupnosti, zobrazit graf výkonu ve zvoleném časovém intervalu.

Ze srovnání vyplývá, že SCE neposkytuje dostatek údajů pro vyhodnocování požadovaných metrik. K tomu je třeba zvážit skutečnost, že data k vyhodnocování jsou v SCE ukládána maximálně po dobu 40 dní.

6.1.3 Správa incidentů a problémů

Pokud je událost klasifikována jako varování nebo výjimka, přechází do správy incidentů respektive správy problémů. V System Center Essentials je proces správy problémů a incidentů konsolidován do jednoho procesu (viz kapitola 5.4). To s sebou přináší i jistá omezení, kterými je postižen především proces správy incidentů. Konkrétní omezení jsou patrné z následujícího srovnání.

Vznik incidentu/problému	
Incident/problém může být zaznamenán správou sítě nebo uživatelem (resp. dodavatelem).	SCE umožňuje spravovat pouze incidenty, které byly vygenerovány při monitorování. Nelze tedy ručně přidávat vlastní incidenty nahlášené např. technikem nebo uživatelem. Vlastní incidenty lze protokolovat přes System Center Service Manager. [12]

Zaprotokolování incidentu/problému	
Incident/problému by měl být zaprotokolován s doporučenými[28] atributy.	SCE protokoluje automaticky všechny incidenty do databáze. Atributy odpovídají požadavkům ITIL v. 3. Další atributy je možné definovat customizací.

Kategorizace	
Kategorizace je vhodná pro snazší identifikaci	Kategorie incidentů jsou v SCE definovány balíčky pro správu. Balíčky pro správu se zpravidla zaměřují na komponenty systému. Kategorie pak většinou odpovídají komponentám systému (např. síťový adaptér, monitorovací agent, Microsoft Office Excel 2003)

[28] Viz kapitola 2.2.2

Priorizace	
Priorizace určuje, s jakou předností bude incident řešen.	SCE vyhodnocuje prioritu incidentů na základě balíčků pro správu. Takto vyhodnocené incidenty však určují pouze míru závažnosti incidentu. Neuvažují, jak uvádí ITIL, například počet ovlivněných uživatelů či lidské zdroje. Proces priorizace nelze ani nijak ovlivnit.

Úvodní diagnostika	
Provádí se v případě, že byl incident nahlášen uživatelem přes Service Desk.	(žádná podpora)

Eskalace	
V závislosti na povaze problému může incident eskalovat horizontálně či vertikálně.	Vzhledem k tomu, že SCE neumožňuje řízení přístupů ke svým komponentám, postrádá delegování incidentů v tomto případě smysl. System Center Operations Manager tuto funkci umožňuje. [15]

Řešení	
V případě, že bylo nalezeno řešení a důkladně otestováno, provedou se korekční opatření.	Při řešení incidentů disponují SCE produktovými a firemními znalostmi. Na základě balíčků pro správu má obsluha k dispozici některé diagnostické nástroje. V průběhu řešení lze měnit stav incidentu či přidávat poznámky o průběhu řešení.

Workaround	
Dočasné řešení umožňující částečnou či plnou obnovu služby	V případě použití dočasného řešení, zůstává v SCE incident nadále otevřený. Obsluha SCE může do historie řešení zpracování

	uvést, že bylo aplikováno dočasné řešení. Nabízí se i vytvoření vlastního stavu[29] například s označením „workaround“.

Známé problémy	
Problém by měl být zaznamenán jako známý problém	SCE neobsahuje databázi známých problémů. Pokud se incident opakuje, není to v SCE nijak zohledněno. Pokud byl incident v minulosti již řešen a bylo zaznamenáno jeho řešení jako podniková znalost, má obsluha SCE tyto informace ihned k dispozici. Nevýhodou tohoto řešení je, že ověření neprobíhá automaticky a obsluha SCE musí ručně ověřit, zda se jedná o opakující se problém.

Popis řešení problému	
Spolehlivé řešení problému by mělo být zaznamenáno.	Popis řešení problému je možné zaznamenat v SCE jako podnikovou znalost. Obsluze bude pak k dispozici pokaždé, kdy se incident shodného typu objeví.

Uzavření incidentu	
Formální uzavření incidentu	Stav incidentu se změní na „uzavřeno“.

6.1.4 Metriky procesu

Pro sledování výkonu tohoto procesu jsou doporučeny tyto metriky:

Počet problémů za dané období	Počet incidentů/problémů za vybrané[30] období lze v SCE zobrazit.
Procento problémů vyřešených do doby stanovené SLA	SCE neumožňuje zobrazit reporty incidentů, jejichž doba řešení přesáhla určitou dobu.

[29] prostřednictvím customizace
[30] nanejvýše však za posledních 40 dní

	Tuto funkcionalitu lze využít v System Center Operations Manager
Procento problémů, které překročilo svůj vyhraněný čas k řešení.	SCE neumožňuje zobrazit reporty incidentů, jejichž doba řešení přesáhla určitou dobu. Tuto funkcionalitu lze využít v System Center Operations Manager
Procento zásadních problémů, jejich tendence, a zda byly dokončeny včas.	SCE neumožňuje zobrazit reporty incidentů, jejichž doba řešení přesáhla určitou dobu. Dále SCE nerozlišuje mezi zásadními problémy a ostatními problémy. Ačkoliv by se toto rozlišení dalo nastavit pomocí customizace, stále by chyběly reporty, které by údaj ve statistikách zohlednily. Tuto funkcionalitu lze využít v System Center Operations Manager
Průměrné náklady na řešení problému	Nelze pomocí SCE určit.

6.2 Správa konfigurací

Z popisu System Center Essentials v předchozích kapitolách vyplývá, že jeho pojetí jako nástroje pro správu konfigurací je trochu odlišné od pojetí Configuration Management System (CMS) v ITIL v. 3 (viz kapitola 3.1.7).

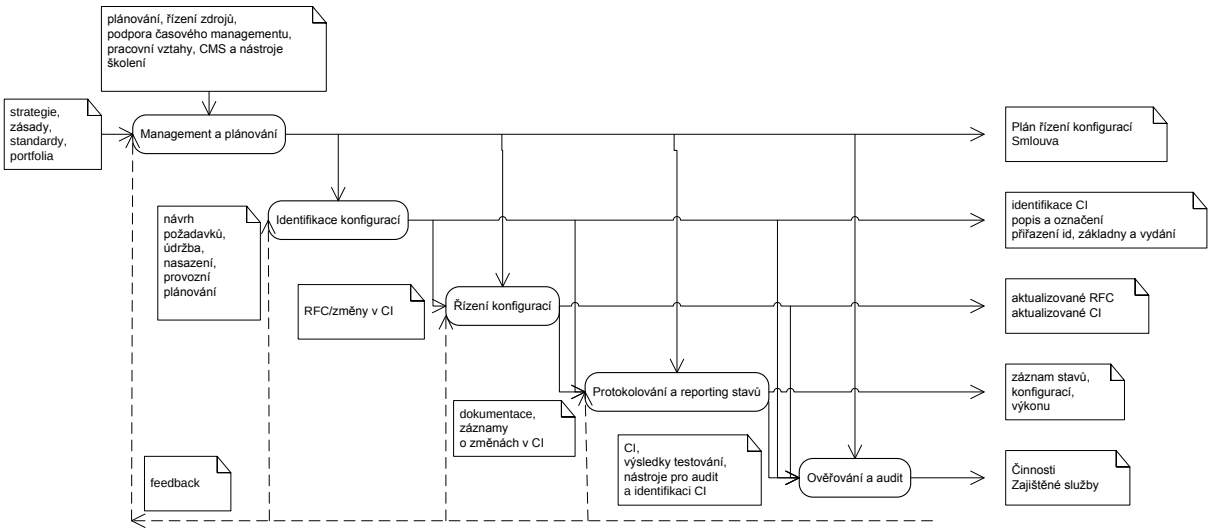
SCE **splňuje** funkci knihovny a datového úložiště, kde obsahuje informace o veškerých významnějších síťových prvcích a může distribuovat schválené aplikace ať už skrze automatickou instalaci nebo iniciovanou uživatelem. Podrobněji bude funkcionalita srovnána v průběhu popisu procesu správy konfigurací.

Naopak v SCE **chybí** konfigurační základna a možnost vytváření Snapshotu. Konfigurační základna je k dispozici ve vyšší verzi System Center Configurations Manager. Nástroj pro centrální vytváření snapshotů od společnosti Microsoft není. Částečně mohou tuto funkcionalitu zastat nástroj System Center Data Protection Manager, který průběžně vytváří zálohy důležitých systémů, nebo Windows Backup and Recovery, který je součástí operačního systému Windows a od verze 7 resp. Server 2008 R2 umožňuje vytvářet obrazy systému. V případě Windows Backup and Recovery se však nejedná o centrálně spravované řešení.

	Podpora v SCE	Alternativa
Knihovna prvků	ANO	
Datové úložiště	ANO	
Konfigurační základna	NE	System Center Configurations Manager
Snapshot	NE	SystemCenter Data Protection Manager

Tabulka 8 Přehled komponent SCE vzhledem k požadavkům ITIL na CMS

Nyní k samotnému procesu správy konfigurací. Pro lepší přehled uvádím ještě jednou schéma procesu správy konfigurací.



Tabulka 9 Proces správy konfigurací dle ITIL (zdroj: [9])

Management a plánování

Tato činnost je strategická a definuje koncept služby správy konfigurací a další průběh procesu. V této fázi je však důležité si uvědomit trochu rozdílné pojetí pojmu prvek konfigurace (CI) v terminologii ITIL v. 3 a v aplikaci System Center Essentials. Zatímco ITIL v. 3 používá prvky konfigurací různého typu různě v sobě obsažených (viz kapitola 3.1), u SCE se pojem CI takřka nevyskytuje. Základní jednotkou je zde „počítač“, přičemž počítač může být jak stolní počítač, přenosný počítač, tak i síťový server. K počítači se váže veškerý v něm obsažený hardware a software, který na něm běží. Služby

(resp. konfigurace služeb), které využívají více počítačů tak již nejsou zohledněny. To může zkomplikovat některé úpravy konfigurací jako je distribuce softwaru a distribuce aktualizací.

Příklad: Služba Microsoft Exchange Server využívá jeden počítač s aplikací Microsoft Exchange Server a databází s poštovními schránkami, jeden počítač s webovým serverem pro komponentu Outlook Anywhere a dva počítače s doménovými řadiči a globálními katalogy (databáze uživatelů a jejich nastavení). Pokud by se například na Exchange Server měl nainstalovat servisní balíček, který vyžaduje webový server pro Outlook Anywhere s určitou aktualizací a tato aktualizace by nebyla na webovém serveru nainstalována, pak SCE nedokáže vyhodnotit tyto závislosti a upozornit na nutnost instalace aktualizace na webovém serveru. Snaha o instalaci servisního balíčku by tak skončila chybou.

Důsledkem tohoto rozdílu je, že nelze automaticky vytvořit mapu závislostí mezi prvky konfigurace, tak jak ji například znázorňuje Obrázek 7.

Identifikace konfigurací

Identifikace konfigurací probíhá v aplikaci System Center Essentials buď automaticky, nebo na základě volby prvků, které mají být identifikovány. Při volbě prvků se vychází z informací obsažených v Active Directory.

Jak již bylo zmíněno v předchozí části, SCE uchovává jako prvky hlavní prvky konfigurace pouze počítače. Tomu odpovídají i atributy, které jsou o prvcích uchovávány.

Označení prvků odpovídá jejich pojmenování v síťovém prostředí (Active Directory). Nezohledňuje se zde verzování jak doporučuje ITIL v. 3.

Podporu dalších doporučených atributů znázorňuje tabulka:

	Podpora v SCE 2007	Alternativní řešení
typ CI	Ano (server/klient/síťové zařízení[31])	
Název (resp. popisek)	Ano (podle AD)	
Verze	Ne	
Umístění	Ne	Tato informace je uvedena v AD
Datum dodání	Ne	O tento údaj lze například rozšířit schéma Active Directory.
Informace o licenci	Ne	
Vlastník (popř. odpovědná osoba)	Ne	Tato informace je uvedena v AD
Stav	Ano (stav monitorování, stav instalací software a aktualizací)	
Dodavatel	Ne	O tento údaj lze například rozšířit schéma Active Directory.
Přiřazené dokumenty	Ne	
Přiřazený software	Ano (seznam nainstalovaného software)	
Vazba k ostatním CI	Ne	Tuto funkcionalitu podle dostupných informací nenabízí ani System Center Configuration Manager.
SLA	Ne	

[31] Spravováno přes SNMP

Správa konfigurací

Tato činnost není v System Center Essentials podporována. Jak již bylo uvedeno v kapitole 5.8, pokud musí být počítač např. re-instalován, není to v SCE uvedeno. Počítač je de facto znovu zařazen do SCE jako kdyby šlo o nový počítač. Také v případě, že jsou v konfiguraci změněny komponenty, není to nikde zaznamenáno. Licencování lze ověřit pouze ručně. Ověřování přístupů probíhá přes Active Directory.

Protokolování a reporting

System Center Essentials neumožňuje protokolovat CI v jejich životním cyklu a podle dostupných informací ani System Center Configuration Manager toto neumožňuje.

Ověřování a audit

Pro tuto činnost nemá SCE žádné podpůrné prostředky. Vyšší verze, System Center Configuration Manager, však tuto funkcionalitu obsahuje.

Metriky procesu

System Center Essentials neumožňuje získat informace o výkonu tohoto procesu, tak jak je vyžaduje ITIL v. 3 (viz kapitola 3.1.6). Výjimku zde tvoří akorát míra využití licencí, kdy lze pomocí SCE zjistit celkový počet instalací daného produktu a podle toho určit míru využití zakoupených licencí.

6.3 Distribuce služeb

Proces Distribuce software a aktualizací je v System Center Essentials dobře podpořen. Již při prvotním srovnání činností v procesech dle ITIL (horní schéma následující grafiky) a SCE (dolní schéma následující grafiky) je patrné, že jsou procesy vcelku sladěny. Vzhledem k tomu, že proces distribuce aktualizací v SCE je téměř shodný[32] s procesem distribuce software, zmíním pouze tento proces.

[32] Jedinou odlišností je, že v procesu distribuce aktualizací jsou aktualizační balíčky od společnosti Microsoft již hotové a nemusí se vytvářet.





Nyní podrobněji k jednotlivým činnostem v procesu.

Plánování

Plánování nasazení software nebo aktualizace vychází ze strategických plánů firmy. System Center Essentials zde může podpořit analýzu stávající situace například tím, že dokáže poskytnout informace o nainstalovaných verzích software (resp. o nainstalovaných aktualizacích).

Vytvoření instalačního balíčku

Instalační balíček je vytvořen v SCE pomocí průvodce. V případě aktualizací společnosti Microsoft, jsou instalační balíčky stahovány automaticky ze serverů služby Microsoft Update.

Jak již bylo zmíněno v kapitole 6.2, SCE neumožňuje ověřovat závislosti služby na více počítačích. To by mělo být v tomto případě ověřeno alespoň ručně.

Testování

Testování může být v SCE podpořeno například vytvořením skupiny pro správu testovacích počítačů. Lze tak kompletně simulovat a sledovat proces distribuce softwaru či aktualizace na počítače před jejich nasazením do produkčního prostředí.

Vytvoření plánu a příprava pro instalaci

SCE může tuto činnost podpořit například poskytnutím informací o využití diskových kapacit počítačů; tedy zda je na počítačích dostatek místa pro instalaci.

Pokud je potřeba v rámci distribučního plánu vytvořit distribuční skupiny, vytváří se zpravidla v této fázi procesu.

Instalace

Instalace software a aktualizací probíhá v SCE automaticky a nelze ji příliš ovlivnit. Podle distribučních modelů ITIL v. 3 lze v případě SCE hovořit o automatické „pull“ instalaci. Klientské počítače automaticky v definovaných časových intervalech ověřují dostupnost nového softwaru a aktualizací k instalaci.

Díky možnosti vytvoření distribučních skupin lze distribuci software a aktualizací provádět i fázově.

SCE nepodporuje „push“ instalace. To může vést k situacím, kdy různí uživatelé pracují s různými verzemi konfigurací.

Ověření instalace

Instalace by měla být ověřena oproti původnímu plánu. System Center Essentials automaticky ověřuje, zda byla instalace provedena bezchybně. V případě nesrovnalostí se incident zobrazí obsluze aplikace, aby mohla být podniknuta korekční opatření.

Vyhodnocení a uzavření instalace

Pro vyhodnocení chyb jsou v System Center Essentials k dispozici statistiky s celkovým počtem úspěšných (resp. nezdařených) instalací.

Metriky

Pomocí softwarových nástrojů lze poskytnout údaje pouze pro tvrdé metriky. ITIL v. 3 definuje jako metriku počty incidentů vzniklých při distribuci softwaru či aktualizací.

SCE poskytuje pouze informace o nezdařených instalacích. Pokud vznikne incident například v důsledku nekompatibility s jinou komponentou konfigurace, SCE tuto vazbu nedokáže identifikovat.

Závěr

Z výsledků srovnání vyplývá, že aplikace řady System Center od společnosti Microsoft ve své kombinaci pokrývají tři z pěti fází životního cyklu služby. Popisované System Center Essentials pak do určité míry dvě z těchto fází.

Ve fázi Service Operation figuruje System Center Essentials spíše jako nástroj pro automatický dohled. Tomu odpovídá i výše popisovaná podpora činností v jednotlivých procesech. V případě, že se spravovaný síťový prvek dostane do nežádoucího stavu, je automaticky vygenerován incident. Takto automaticky vygenerované incidenty lze spravovat dle doporučení ITIL v. 3. Podpora incidentů identifikovanými vlastními silami v SCE chybí. Funkce jako například Service Desk nelze touto aplikací podpořit.
Dalším problémem jsou pak metriky procesů. Mnoho metrik nelze pomocí SCE stanovit, nebo je nelze stanovit přímo a musí se dopočítávat. Pro metriky, které lze měřit pomocí SCE platí omezení analýzy údajů nanejvýše za posledních 40 dní. Neméně významnou roli hraje i skutečnost, že SCE takto vyhodnocuje pouze své automaticky vygenerované incidenty a incidenty identifikované jinými způsoby neumožňuje zahrnout.
Lepší podporu nabízí produkt System Center Operations Manager, který je určen spíše pro větší organizace. Oproti SCE jde dál v možnostech vytváření vlastních statistik, které by odpovídaly metrikám ITIL v. 3. Dále umožňuje monitorovat události vycházející z bezpečnostního auditu. Podporu lze ještě dále vylepšit pomocí nově připravovaného produktu System Center Service Manager, který ve fázi Service Operations umožňuje i oddělenou správu problémů.

Ve fázi Service Transition je možné SCE využít spíše jako nástroj pro distribuci softwaru a aktualizací než jako Configuration Management System. Za CMS lze považovat až vyšší verzi System Center Configurations Manager.
Situace v oblasti metrik je podobná, jako tomu je v případě podpory činností. Údaje pro metriky jsou k dispozici pro procesy distribucí softwaru a aktualizací. Naopak pro proces správy konfigurací jsou údaje metrik téměř nedostupné.

System Center Essentials většinu procesů podporuje, avšak s jistými omezeními (viz kapitola 6). Lepší podporu lze získat použitím pokročilejších nástrojů (System Center Operations Manager a System Center Configuration Manager). Úplné sladění by měl přinést produkt System Center Service Manager, který doplňuje podporu některých procesů, které SCOM a SCCM pokryty nebyly.

Podpora procesů softwarovými nástroji je však pouze jedna strana mince. Druhou je, jak jsou procesy ve firmě implementovány. Je nutné si uvědomit, že ITIL v. 3 poskytuje pouze univerzální doporučení,

jak by měly procesy probíhat. Po přizpůsobení procesů konkrétním podmínkám firmy tak mohou vypadnout některé činnosti nebo mohou být prováděny v omezené míře. Například se může firma rozhodnout, že nebude zaznamenávat změny v konfiguracích desktopů, protože by zde náklady převyšovaly přínosy. Tento fakt může zamíchat s mírou přínosů aplikace v daných podmínkách. Vždy je proto potřeba posoudit konkrétní situaci při volbě řešení.

Popularita metodiky ITIL roste a nabírá na významu. Je tedy pravděpodobné, že se podpora procesů dle ITIL bude s novými verzemi produktů Microsoft nadále zlepšovat.

Přínos mé práce spatřuji nejen v samotném nezávislém srovnání, ale i v možnosti jejího využití v různých podmínkách díky popisu procesů po jednotlivých činnostech. Firma, která má například naimplementovány jen některé činnosti z procesů dle ITIL, stále může vyhodnotit jejich podporu aplikací System Center Essentials.

Seznam literatury

1. **Dimension Data Czech Republic.** How Do You Manage? [Online] 2009. [Citace: 20. 09 2009.] http://www.dimensiondata.com/NR/rdonlyres/0DB88E37-0E7B-48ED-AC13-9C81A7B96C9F/11201/HDYMReport1.pdf.

2. **CIO Business World.** IT infrastruktura v moderní organizaci. *CIO Business World.* [Online] 4. 12 2007. [Citace: 20. 09 2009.] http://businessworld.cz/reseni-a-realizace/it-infrastruktura-v-moderni-organizaci-2534.

3. **Khudhur, Patrik.** 97 % firem potvrzuje závislost na síťové infrastruktuře. *CIO Business World.* [Online] 16. 6 2009. [Citace: 20. 9 2009.] http://businessworld.cz/aktuality/97-procent-firem-potvrzuje-zavislost-na-sitove-infrastrukture-4735.

4. **CIO Business World.** ITIL v3 Není kam spěchat. *CIO Business World.* [Online] 03. 07 2009. [Citace: 18. 10 2009.] http://businessworld.cz/it-strategie/ITIL-v3-Neni-kam-spechat-4746.

5. **IDC.** Server Market Deceleration Continues in Second Quarter, But Signs of Stabilization Emerge, According to IDC . *IDC.* [Online] 02. 09 2009. [Citace: 20. 10 2009.] http://www.idc.com/getdoc.jsp?containerId=prUS21989209.

6. **NetIQ.** NetIQ No. 1 in Market Share for Microsoft Active Directory. *NetIQ.* [Online] 14. 07 2003. [Citace: 20. 10 2009.] http://www.netiq.com/news/releases/release.asp?cid=20030714141048BYXM.

7. **Excel Networks.** ITIL. *Excel Networks.* [Online] 2008. [Citace: 22. 03 2010.] http://www.excel-networks.co.uk/excel/itil_iso/ITIL_%28IT_Infrastructure_Library%29_.html.

8. **Office of Government Commerce.** *ITIL - Service Operation.* místo neznámé : TSO, 2007. 978-0-11-331046-3.

9. —. *ITIL - Service Transition.* místo neznámé : TSO, 2007. 978-0-11-331048-7.

10. **AT Institute.** The Windows 7 beta 1 version remains very confidential. *AT Institute.* [Online] 22. 3 2009. [Citace: 13. 1 2010.] http://www.atinternet-institute.com/en-us/internet-users-equipment/operating-systems-february-2009/index-1-2-7-165.html.

11. **Computerworld.** NetWare Stalwarts Remain Loyal Despite Dwindling Market Share. *Computerworld.* [Online] 14. 4 2003. [Citace: 13. 1 2010.] http://www.computerworld.com/s/article/80264/NetWare_Stalwarts_Remain_Loyal_Despite_Dwindling_Market_Share.

12. **Microsoft Corporation.** System Manager. *Microsoft System Center*. [Online] [Citace: 07. 04 2010.] http://www.microsoft.com/systemcenter/en/us/service-manager.aspx.

13. —. Configuration Manager: Overview. *Microsoft System Center.* [Online] [Citace: 07. 04 2010.] http://www.microsoft.com/systemcenter/en/us/configuration-manager/cm-overview.aspx.

14. —. Mobile Device Manager 2008 SP1. *System Center*. [Online] [Citace: 07. 04 2010.] http://www.microsoft.com/systemcenter/mobile/default.mspx.

15. —. Operations Manager. *System Center*. [Online] http://www.microsoft.com/systemcenter/en/us/operations-manager/om-overview.aspx.

16. —. Data Protection Manager. *System Center.* [Online] [Citace: 07. 04 2010.] http://www.microsoft.com/systemcenter/en/us/data-protection-manager/dpm-overview.aspx.

17. —. Virtual Machine Manager. *System Center.* [Online] [Citace: 07. 04 2010.] http://www.microsoft.com/systemcenter/en/us/virtual-machine-manager/vmm-overview.aspx.

18. —. Active Directory. *Microsoft TechNet.* [Online] [Citace: 2010. 1 14.] http://technet.microsoft.com/en-us/library/bb742424.aspx.

19. —. Desktop Lifecycle Management with System Center Essentials 2007. [Online] 04 2007. http://go.microsoft.com/fwlink/?LinkID=89188.

20. —. System Center Essentials. *System Center.* [Online] [Citace: 30. 03 2010.] http://www.microsoft.com/systemcenter/en/us/essentials.aspx.

21. —. About software deployment in System Center Essentials. *Microsoft TechNet.* [Online] [Citace: 28. 02 2010.] http://technet.microsoft.com/en-us/library/bb422798.aspx.

22. —. Windows Server 2003 R2. *Microsoft.* [Online] [Citace: 16. 1 2010.] http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx.

23. **Ziff Davis Publishing Holdings Inc.** Encyclopedia. *PCMAG.* [Online] http://www.pcmag.com/encyclopedia/.

24. **Voříšek, Jiří.** *Principy a modely řízení podnikové informatiky.* Praha : Nakladatelství Oeconomica, 2008. ISBN 978-80-245-1440-6.

25. **Microsoft Corporation.** Compare Product. *Microsoft System Center.* [Online] [Citace: 28. 02 2010.] http://www.microsoft.com/systemcenter/essentials/en/us/compare-products.aspx.

26. **IT Governance Institute.** *CobiT 4.1.* 2007. 1-933284-72-2.

27. **Microsoft Corporation.** System Management Server 2003 Technical Library. *Microsoft Technet.* [Online] 10 2009. http://technet.microsoft.com/cs-cz/library/bb633760(en-us).aspx.

28. **Radecky, Alexandr.** Dostupná infrastruktura je základem byznysu. *CIO Business World.* [Online] 06. 12 2007. [Citace: 20. 09 2009.] http://businessworld.cz/reseni-a-realizace/dostupna-infrastruktura-je-zakladem-byznysu-2529.

29. **CIO Businessworld.** Historie Microsoft Corporation. *CIO Businessworld.* [Online] 6. 2 2009. [Citace: 13. 1 2010.] http://businessworld.cz/veda-a-historie/Historie-Microsoft-Corporation-4230.

30. **Microsoft Corporation.** Event Logging. *MSDN Developer Center.* [Online] 12. 11 2009. [Citace: 14. 1 2010.] http://msdn.microsoft.com/en-us/library/aa363652%28VS.85%29.aspx.

31. **Northrup, Tony a Mackin, J. C.** *MCITP Self-Paced Training Kit (Exam 70-622): Supporting and Troubleshooting Applications on a Windows VistaB® Client for Enterprise Support Technicians.* místo neznámé : Microsoft Press, 2007. ISBN: 978-0-7356-2408-5.

32. **Desmond, Brian, a další.** *Active Directory O'Reilly Series.* místo neznámé : O'Reilly Media, Inc., 2008. ISBN 059652059X, 9780596520595.

33. **World Wide Web Consortium (W3C).** *World Wide Web Consortium (W3C).* [Online] http://www.w3.org/.

34. **Microsoft Corporation.** Top Ten Benefits. *Microsoft System Center Essentials.* [Online] [Citace: 28. 02 2010.] http://www.microsoft.com/Systemcenter/essentials/en/us/top-ten-benefits.aspx.

35. —. Pricing and Licensing. *Microsoft System Center Essentials.* [Online] [Citace: 28. 02 2010.] http://www.microsoft.com/Systemcenter/essentials/en/us/pricing-licensing.aspx.

36. —. System Requirements and Supported Platforms for System Center Essentials. *Microsoft TechNet.* [Online] [Citace: 28. 02 2010.] http://technet.microsoft.com/en-us/library/bb422876.aspx.

37. **Košec, Petr.** Microsoft System Center Essentials 2010. *SystemOnLine.* [Online] 09 2009. [Citace: 28. 02 2010.] http://www.systemonline.cz/sprava-it/microsoft-system-center-essentials-2010.htm. ISSN 1802-615X.

38. **Microsoft Corporation.** Configuration Manager: Desired Configuration Management. *System Center.* [Online] [Citace: 07. 04 2010.] http://www.microsoft.com/systemcenter/en/us/configuration-manager/cm-desired-configuration-management.aspx.

39. **Ghelani, Ketan.** Overview of Problem Management in Service Manager . *SCSM Engineering Team Blog.* [Online] 02. 11 2009. [Citace: 12. 04 2010.] http://blogs.technet.com/servicemanager/archive/2009/11/02/overview-of-problem-management-in-service-manager.aspx.

40. **Microsoft Corporation.** System Center Management Pack Catalog. *Pinpoint.* [Online] [Citace: 09. 04 2010.] http://pinpoint.microsoft.com/en-US/systemcenter/managementpackcatalog.

41. **Office of Government Commerce.** *ITIL - Continual Service Improvement.* místo neznámé : TCO, 2007. 978-0-11-331049-4.

Seznam obrázků

Obrázek 1 Rozdělení ITIL v3 (zdroj: [7]) 3
Obrázek 2 Proces (zdroj: ITIL v3 – Service Operation [8, s. 13]) 5
Obrázek 3 Správa událostí (zdroj: ITIL v. 3 – Service Operation [8, s. 38]) 9
Obrázek 4 Správa incidentů (zdroj: ITIL v3 – Service Operation [8, s. 48]) 17
Obrázek 5 Proces správy problémů (zdroj: ITIL v3 – Service Operation [8, s. 60]) 20
Obrázek 6 Standardní proces změny 24
Obrázek 7 Model konfigurace (zdroj: ITIL v. 3 – Service Transition [9, s. 67]) 25
Obrázek 8 Proces správy konfigurací (zdroj: ITIL v. 3 – Service Transition [9, s. 71]) 26
Obrázek 9 Proces správy distribuce služeb 30
Obrázek 10 Životní cyklus pracovní stanice (zdroj: Microsoft [19]) 36
Obrázek 11 Přehled správy SCE serveru 41
Obrázek 12 Proces správy incidentů v SCE 42
Obrázek 13 Přehled aktuálních incidentů 44
Obrázek 14 Monitorování výkonu v SCE 46
Obrázek 15 Balíčky pro správu v SCE 47
Obrázek 16 Proces distribuce software (zdroj: Microsoft [19]) 52
Obrázek 17 Proces distribuce aktualizací (zdroj: Microsoft [19]) 54
Obrázek 18 Ukázka softwarového inventáře v SCE 55

Seznam tabulek

Tabulka 1 Přehled 6
Tabulka 2 Reakce na události 15
Tabulka 3 Přehled systémových požadavků SCE (zdroj: Microsoft [20]) 38
Tabulka 4 Přehled komunikačních kanálů v SCE 43
Tabulka 5 Přehled obsahu balíčku pro správu 48
Tabulka 6 Přehled customizace monitorování v SCE 49
Tabulka 7 Přehled podpory jednotlivých částí ITIL produkty Microsoft 58
Tabulka 8 Přehled komponent SCE vzhledem k požadavkům ITIL na CMS 67
Tabulka 9 Proces správy konfigurací dle ITIL (zdroj: [9]) 67

Terminologický slovník

Termín	Zkratka	Význam [zdroj]
Active Directory	AD	Centrální komponenta platformy Windows. Adresářové služby Active Directory poskytují prostředky pro správu identit a vztahů, které vytvářejí síťové prostředí. [22]
Aplication Programming Interface	API	Formát jazyka a zpráv používaný aplikací ke komunikaci s operačním systémem či jiným řídícím programem. API jsou implementována jako volání funkcí. [23]
Configuration Item	CI	Aktivum (tj. pracovní stanice, server, apod.), komponenta služby či schopnosti (procesy, znalosti, apod.). [9]
Dynamic Host Configuration Protocol	DHCP	Funkce software, která umožňuje automatické přiřazení dočasné IP adresy klientům. Eliminuje tak ruční nastavování IP adres. Většinou běží na serveru či routeru. [23]
Domain Name Service	DNS	Služba pro překlad doménových jmen na číselné (IP) adresy a naopak. [autor]
incident		Výjimka v chodu služeb, která vede k jejich degradaci. [8]
IT infrastruktura		ICT prostředky pro vývoj a provoz aplikací a pro uložení a přenosy dat(24)
Operational Level Agreement	OLA	Dohoda mezi poskytovatelem a uživatelem o stanovené kvalitě dodávaných služeb v rámci organizace. [autor]
operační systém	OS	Hlavní řídící program počítače. Je neustále v paměti počítače a řídí hardware a aplikace, které na něm běží. [23]
Personal Digital Assistant	PDA	Kapesní počítač pro osobní organizaci. [23]
Service Desk	SD	Kontaktní místo uživatelů pro nahlášení problémů se službou či konfigurací či předání požadavků na změnu konfigurace svého počítače. [8]
Service Level Agreement	SLA	Dohoda mezi poskytovatelem a uživatelem o stanovené kvalitě dodávaných služeb. [autor]
router		Směrovač. Zařízení, které směruje datové pakety z jedné sítě do druhé na základě směrovací tabulky. [autor]

Univerzální Sériová Sběrnice	USB	Rozhraní pro připojení periferních zařízení k počítači [autor]
Wide Area Network	WAN	Komunikační síť rozkládající se přes více geografických celků. Využívají je telekomunikační operátoři nebo firmy pro připojení vzdálených poboček. [23]

Přílohy

Srovnání System Center Operations Manager 2007 s SCE

Monitorování	System Center Operations Manager 2007	System Center Essentials 2007	Odlišnosti v System Center Essentials 2007
Monitorování serverů, klientů Windows, hardware, software, a služeb	✓	✓	Essentials obsahuje již balíček pro správu síťových zařízení.
Balíčky pro správu s expertními znalostmi	✓	✓	
Agentless Exception Monitoring (AEM)	✓	✓	
Customizace monitorování	✓	✓	
Reporting	✓	✓	Essentials vyhodnocují data nanejvýše 40 dní nazpět bez možnosti customizace.
Monitorování vzdálených poboček	✓	✓	Essentials 2007 neumožňuje interakci více serverů.
Zabezpečení pomocí rolí	✓		V Essentials 2007 server pouze jako lokální správce resp. správce domény.
Framework pro externí konektory	✓		
Nástroje pro audit	✓		
Webová konzole	✓		

Zdroj: [25]

Srovnání System Center Configuration Manager 2007 s SCE

Configuration	System Center Configuration Manager 2007	System Center Essentials 2007	Odlišnosti v System Center Essentials 2007
Distribuce aktualizací (Microsoft a jiné)	✓	✓	
Distribuce software	✓	✓	Essentials umožňuje základní distribuci balíčků MSI a EXE s volitelnými parametry příkazové řádky bez rozšířené funkcionality.
Inventář Hardware a software	✓	✓	Essentials sbírá přes 60 pevně stanovených atributů softwaru a hardwaru. Configuration Manager 2007 umožňuje rozšíření těchto atributů.
Distribuce softwaru a aktualizací vzdáleným pobočkám	✓	✓	Essentials využívají pouze jediný server pomocí BITS 2.0. Replikace nejsou možné.
Distribuce operačních systémů	✓		
Správa preferovaných konfigurací	✓		
Wake on LAN	✓		
Integrace technologie Network Address Protection (NAP)	✓		

Zdroj: [25]