Česká společnost uživatelů otevřených systémů EurOpen.CZ
Czech Open System Users' Group
www.europen.cz

40. konference

Sborník příspěvků

Velké Bílovice – sklepy
Hotel Mádl
13.–16. května 2012

Sborník příspěvků z 40. konference EurOpen.CZ, 13.–16. května 2012

Plzeň 2012. První vydání.
Editor: Vladimír Rudolf
Sazba a grafická úprava: Ing. Miloš Brejcha – Vydavatelský servis, Plzeň
e-mail: servis@vydavatelskyservis.cz

Tisk: Typos, tiskařské závody, s. r. o.
Podnikatelská 1160/14, Plzeň

Příspěvky neprošly redakční ani jazykovou úpravou.

ISBN 978-80-86583-23-5

Obsah

Tutorial: Jak se stát neviditelným

Pavol Lupták

E-mail: pavol.luptak@nethemba.com

Abstrakt

Cieľom workshopu bude vysvetliť princípy anonymizujúceho smerovania (Onion routing), sfunkčnenie anonymizujúcej Tor siete v štandardnom webovom prehliadači, anonymizáciu hlavičiek HTTP spojení (privoxy a Torbutton) a sprevádzkovanie anonymnej služby (Tor hidden service) - anonymného blogu a webového servera.

Autor příspěvek nedodal.

IT bezpečnost v měnícím se světě Internetu

Jan Müller

E-mail: jan.muller@i.cz

Za dobu existence Internetu jsme mohli pozorovat pronikání Internetu, Internetových technologií a služeb do všech možných oblastí lidských činností. Od první poloviny devadesátých let, kdy se objevily první weby, až do dnešní doby jsou tyto systémy stále všudypřítomnější a Internetové služby používáme stále běžněji v denním životě pro stále důležitější věci. Způsob užívání těchto služeb se ale, zejména v posledních letech, zásadně mění, a to má podstatné dopady i na bezpečnost.

Kromě oblastí, kde Internet slouží spíš jako prostředek k realizaci kriminálního jednání, zůstává těžiště bezpečnostní problematiky v tradičních oblastech jako je oblíbený DoS, Denial-of-Service, online fraud, zejména vykrádání bankovních účtů, a průmyslová a vládní špionáž. Zde všude vidíme nárůst v závažnosti, v objemech a systémovější přístupu, kde je zvýšená motivace daná možností vyšších zisků, ale také se objevují nové metody a postupy, dané měnícími se postoji k Internetu.

Denial-of-Service

Mezi novinářsky nejoblíbenější patří útokyDoS, které bývají velmi razantní a viditelné. Obecně se jedná o vyčerpání zdrojů cílového systému, v některých případech i sestřelení systému (starší útoky jako Teardrop, Land nebo ping-of-death). Nyní obvykle vidíme buďto masivní distribuované DDoS, který zahltí Internetové připojení cílového systému (často až 40Gb/sec) anebo sofistikované vyčerpání jiných systémových zdrojů jako statických tabulek apod. (někdy i ve vyšších vrstvách jako SSL nebo HTTP). Dříve to byl např. SYN flood (vyčerpání tabulek TCP množstvím polootevřených spojení), teď jsou nebezpečnější pomalé útoky LDoS (Low-Rate DoS), které dosahují stejného efektu s výrazně nižším zatížením Internetového připojení (např. Slowloris). Mění se také důvody k vlastnímu útoku DoS; dříve se jednalo spíš o předvádění a poměřování se, nyní již mívají takové útoky konkrétní, obvykle politický (hacktivismus) nebo ekonomický cíl. Skupina Anonymous útočila nástroji LOIC a Slowloris na RIAA/MPAA, Bílý dům, VISA, Irán,Sony atd., později kvůli penězům i na WikiLeaks!, dále jsme viděli další útoky v Iránu, poměrně masivní DDoS útok na Estonsko v roce 2007

anebo i útoky motivované finančně, např. útoky na cestovní kanceláře nebo útok ruského payment processoru ChronoPay na konkurenční ASSIST. Zatímco většina těchto útoků má za cíl poškodit konkurenci, v loňském roce byl realizován útok DDoS na burzu v Hong-Kongu s cílem narušit výměnu informací tak, aby útočník vydělal na transakci.

Důvod, proč jsou útoky DoS tak úspěšné, spočívá právě v tom, že zneužívají a blokují služby, na kterých jsme stále závislejší. Problém je o to horší, že si jednak své závislosti nejsme vědomi a považujeme dostupnost síťových služeb za automatickou, a jednak tím, že si neuvědomujeme složité řetězce a závislostí v neprůhledných systémech a možné kaskádové efekty.

Americké ministerstvo obrany DoD se neuvědomovalo, že letitý problém průniků do jejich neutajované sítě NIPRNet může způsobit DoS útok na utajovanou síť SIPRNet, která je přes ni často tunelována. Toto spoléhání na dostupnost přenosových sítí je vidět v bankovních systémech, obchodních komunikacích, mezilidských vztazích nebo třeba i v bojových operacích, např. ve vyhodnocování dat z bezpilotních průzkumných letadel v Iráku, kde se senzorová data přenášejí prakticky v reálném čase na velké vzdálenosti (vyhodnocovací střediska MCE jsou v USA). Podobně až do útoku v roce 2007 bylo Estonsko hrdé na to, že jsou „the most wired society in Europe“.

V mnoha ohledech byla u nás situace ještě horší, protože zejména v oblasti utajovaných informací se potřeba dostupnosti vůbec neuvažovala. Např. vyhláška 523/2005 Sb. o bezpečnosti informačních a komunikačních systémů praví: „Při přenosu utajované informace komunikačním kanálem musí být zajištěna ochrana její důvěrnosti a integrity“, přičemž „dostupnost“ v §10 vyhlášky znamená řešení havárie serveru a plánování kapacit. Situace se zlepšuje až v současném návrhu zákona o kybernetické bezpečnosti, kde věcný záměr hovoří o „zvýšení bezpečnosti kybernetického prostoru“ a „zajištění kybernetické bezpečnosti kritické infrastruktury a ISVS“. Na druhé straně se zde zanedbává hrozba APT (viz dále) a zřetelně hrozí formální přístup k IT bezpečnosti, ze kterého se teprve nyní vzpamatovávají Spojené státy.

Zločin a podvody na Internetu

I think the next big Internet security trend is going to be crime. Not the viruses and Trojans and DDoS attacks for fun and bragging rights. Real crime. On the Internet.

Criminals tend to lag behind technology by five to ten years, but eventually they figure it out. Just as Willie Sutton robbed banks because „that‘s where the money is“, modern criminals will attack computer networks. Increasingly, value is online instead of in a vault.

Bruce Schneier
Cryptogram 15. 12. 2002

Zločin na Internetu má tisíce podob, v tomto kontextu se zabýváme pouze těmi postupy, které skutečně závisejí na Internetových technologiích, a které je využívají k podvodnému získání peněz (fraud). Víceméně stranou tedy zůstávají různé oblasti jako copyright, cyberstalking/harrassment, dětské porno, využívání Internetu k šíření nenávisti a návodů na výrobu bomb, kšeftování se zbraněmi a drogami atd. Některé z těchto útoků by bez Internetu nebyly možné (šíření spamu), jiné jsou jen z papírové pošty přesunuté do mailu, např. známý scam 419 (jsem Pepa Nobongogongo z Nigérie, otec zemřel při havárii letadla – viz foto – a zůstalo po něm $10M, fakt potřebuji Vaši pomoc).

I samotné Internetové podvody jsou velmi různé, obvykle jen varianty nesíťových podvodů které cílí na fyzické osoby, např. zprostředkování práce nebo viza do USA, vyhrál-jste-v-loterii, nabídky výhodných koupí, variace sňatkových podvodníků, prodej falešného zboží nebo nedodání po platbě apod. Jiné operace cílí na burzy a využívají Internet k šíření fám o trendech cenných papírů za účelem ziskového nákupu nebo prodeje (např. pump-and-dump scheme). V některých případech vznikají celá nová odvětví, např. cyber-extortion, kdy útočník pronikne do cílového počítače, zašifruje data a požaduje peníze za dešifrování (nedávno útočník v Irsku dokonce zneškodnil zálohovací sw firmy několik týdnů před vlastním útokem).

Je třeba si uvědomit, že podvodníci jsou mimořádně vynalézaví a kdekoliv se objeví nějaká možnost, okamžitě ji využijí – např. po hurikánu Katrina se objevily desítky falešných webů, které sbíraly peníze. Letos mě zaujalo, když si aktivisté z Anonymous, kteří po uzavření Megauploadu útočili na DoJ, whitehouse.gov apod. pomocí nástroje slowloris, infikovali své vlastní systémy právě modifikovanou verzí slowlorisu. Některý podvodník uviděl příležitost k šíření trojského koně, a tak do slowlorisu zabudoval oblíbený virus Zeus, který pak standardně očesal uživatelům hesla, bankovní credentials a poslal je do svého řídícího centra.

Nejzávažnější Internetové podvody se tedy vyznačují použitím malware, který už neslouží jen samoúčelnému poškození nebo ovládnutí cílového počítače, ale slouží finančnímu zisku. Nejnebezpečnější a nejpropracovanější typy podvodů jsou založeny na krádeži identity, a přestože podle statistik IC3 je identity theft asi jen 10 % ze všech síťových podvodů, představuje největší ztráty (např. jen ve Velké Británii přes 3 mld. liber ročně). Samotné technologie, procesy a systémy se stále vyvíjejí, a jak ty starší, tak ty nově vznikající mají mnoho společného s útoky APT (Advanced Persistent Threat) s tím, že při standardní krádeži identity je cílem přístup na konto oběti, kdežto v APT je to obvykle jen předehra. V některých případech se síťoví loupežníci z APT poučili a útoky jsou cíleně pod prahem vnímání (low profile, stealth). Předloni např. FTC (Federal Trade Commission) odhalila skupinu, která vydělala okolo $10 mil. tím, že si z každé karty strhla 20 centů až 10 dolarů (jenom jednou) – 90 % majitelů si ničeho nevšimlo!

Moderní doba ale přinesla neuvěřitelný pokrok i mimo vlastní technologie, a to v obchodní oblasti, kde vznikly rozsáhlé sofistikované ekosystémy. Partičky hackerů byly nahrazeny profesionálními obchodními společnostmi, které mají standardní procesy jako product management, payment processing, customer support, marketing, inzerci atd. a kde vládne ostrý konkurenční boj. Některé typy malware vymazávají konkurenční viry na napadeném počítači, je běžný systém slev pro starší produkty nebo větší objemy zakázek, a ceny údajů o účtech s PINy klesají díky konkurenci. Svět hackerů se rozdělil na výrobce, obchodníky/dealery/integrátory a koncové uživatele, prosté dělníky zločinu. Již před 5 lety napsal Don Jackson, když analyzoval trojana Gozi:

„. . . full-fledged e-commerce operation. It was slick and accessible, with comprehensive product offerings and a strong customer focus. . . Gozi represents the shift taking place in Internet crime, from software-based attacks to a service-based economy".

Koncový uživatel-zloděj si může pronajmout sadu infikovaných počítačů, typicky na měsíc (platební cyklus) a doufá, že během té doby získá autentizační údaje oběti. Dealer naopak vidí obchodní příležitost v celkové podpoře zákazníka: „profit is not only in the kit, but in selling value added services like exploitation, compromised servers/accounts, database configuration, and customization of the interface". Tento service-oriented přístup MaaS (Malware-as-a-Service) vede až ke kuriozním řešením – D. M. Naskovec byl odsouzen za konspiraci,protože poskytoval jazykovou podporu těmto podvodům: „. . . offered the services of German and English speakers who would call the bank from which the thief was attempting to steal the funds and pretend to be the account holder."

Výsledkem tohoto vývoje je nyní situace, kdy prakticky nelze na Internetu svou identitu ochránit (když ji neukradnou vám, ukradnou ji z databáze obchodníka) a tolik propagovaný e-banking (a e-cokoliv) je ve skutečnosti tak nebezpečný, že můžeme pouze doufat v omezení ztrát omezením hotovosti na účtu.

APT, špionáž a cyberwarfare

Kromě útoků na bankovní účty vidíme v posledních letech nárůst profesionálních útoků a špionáže ve velkém měřítku jak vládní, tak i průmyslové; současně se také státy připravují na možnosti kybernetického konfliktu. Termínem APT, Advanced Persistent Threat, se obvykle rozumí hrozba, která se vyznačuje profesionalitou, vytrvalostí a odbornou zdatností; klíčová je ale schopnost dlouhodobého systematického pronásledování, která je daná jednak vysokou hodnotou cíle, dále vysokými technickými schopnostmi a finančními možnostmi útočníků, a v řadě případů i systematickým operačním provedením, který připomíná modus operandi tajných služeb. Za typickým útokem APT stojí tedy organizace, která disponuje mimořádnými zdroji, a mnohdy nelze odlišit, zda se jedná o stát,

bohatou průmyslovou skupinu nebo bohatý zločinecký syndikát. Mezi první proslulé útoky typu klasické špionáže patří bezesporu operace Titan Rain, kde od roku 2003 neznámá entita (= Čína) stáhla během několika let desítky terabytů citlivých informací. Útok byl vystopován až ke 20 stanicím a 3 směrovačům v Číně v provincii Guangdong; útočníci si ukradené dokumenty dočasně ukládali na zombie systému v Korei, kde byly objeveny velmi citlivé materiály jako např. detailní schémata pohonných systémů NASA, SW pro řízení bojových helikoptér apod.

Po útoku se ozvaly i další země jako Nový Zéland, Francie, Německo, že byly napadeny ze strany Číny (Čína to popřela a tvrdila naopak, že ona byla napadena). Kromě těchto a mnoha dalších případů „státní“ špionáže se ovšem množí špionáž industriální; tak například útok Nitro proti chemickým a obranných firmám v r. 2011 stahoval výrobní postupy a formule, zatímco Night dragon v letech 2008–2010 pronikl mj. do společností Shell, Exxcon Mobil a BP a šel po informacích o naftovém průzkumu, po finančních informacích, nabídkách apod.

Kromě technické dokonalosti (viz např. Stuxnet) se útoky APT vyznačují i systematickou volbou postupných cílů. Tak např. loňský útok na RSA Security, kdy se útočníci zmocnili materiálů k SecurID, byl zřejmě jen předstupeň k útoku na klíčové firmy amerického obranného průmyslu jako Lockheed Martin nebo Northrup Grumann. Zajímavou variantu předvedli útočníci při průniku do certifikačních autorit Comodo a DigiNotar, kdy bylo cílem získat certifikáty podepsané kořenovým klíčem, nepochybně pro další účely. O podobnou věc šlo zřejmě i v útoku Aurora v r. 2010, kdy byly napadeny firmy Google a Adobe, a útočník se snažil modifikovat zdrojové kódy jejich programů.

Není jisté, zda útoky jako Titan Rain nebo Aurora byly skutečně vládní akce ČLR nebo jen akce čínských hackerů (případně na vládní objednávku), každopádně vzhledem k rozsahu, provedení a cílům (včetně aktivistů lidských práv) jsou odborníci přesvědčeni, že za útoky je Čína, která již v roce 2007 zřídila armádní jednotky pro ofenzívní vedení kyberválky. Na takovou možnost se ale v současné době připravuje většina států, mění odpovídajícím způsobem své vojenské doktríny a např. USA v r. 2009 zřídily Cyber Command jako součást strategického velení US STRATCOM. V řadě případů je ale přístup poněkud zmatený, vyznačuje se tendencí bojovat minulé války a pojímat cyberwarfare jako tradiční válčení – při útoku na Estonsko v roce 2007 se dokonce jednalo o možnost aplikace článku V smlouvy NATO o kolektivní sebeobraně. Do jisté míry ale kyberkonflikty zuří už teď – při útoku Ruska na Jižní Osetii byla napadena gruzínská internetová infrastruktura, a v současné době probíhají vzájemné útoky mezi Spojenými Emiráty a Izraelem.

Změny vnímání Internetu a dopady na bezpečnost

. . . organizations are vulnerable to cyberattack only to the extent they want to be . . .
M. C. Libicki: Cyberdeterrence and Cyberwar, RAND
A to se týká i lidí. . .

Bouřlivé změny se netýkají jen cílů a způsobů provedení útoků, ale i samotné techniky. Zde vidíme přesun z nižších vrstev systému jako cíle do vyšších vrstev na úroveň prohlížeče a webových interakcí. Stále se používá velké množství technik, od nedostatečné kontroly vstupu (XSS) přes triky s DNS (DNSchanger, Kaminskeho cache poisoning) až po specifické exploity na nové zranitelnosti (zero day exploity ve Stuxnetu a Auroře), nicméně zdaleka nejoblíbenější jsou díry v prohlížečích a pluginech. Současně se mění klasický push model infekce na pull, kde se jako primární vektor používá buďto sociální inženýrství (phishing) nebo automatické downloady (drive-by-downloads), obvykle pomocí iframe, což je vynikající fičura HTML4 jako stvořená pro infekci.

Co ale umožňuje nasazení všech těchto technik? Internetové služby jsou všudypřítomné, jsme na nich závislí a používáme je denně i pro kritické činnosti. V postojích uživatelů k Internetu se dále objevují nové trendy, které otevírají nové zranitelnosti.

Bruce Schneier některé z nich pojmenovává krásnými termíny:

- Deperimeterization: interní sítě se rozplizávají a stírá se rozdíl mezi vnitřkem a vnějškem
- Comsumerization: zaměstnanci chtějí své cool hračky jako různé iPady používat i v práci (BYOD)
- Decentralization: data se ztrácejí někde v cloudu, počítač je jen dočasný nástroj pro přístup
- Deconcentration: univerzální počítač vymírá, je nahrazován specializovaným HW a SW pod kontrolou poskytovatelů obsahu
- Decustomerization: většina služeb na Internetu je tzv. free (platíme za ně tím, že do nás hrnou reklamy) – „we are not Google‘s customers; we are Google‘s product that they sell to their customers“.
- Depersonization: uživatel je vzdalován od interakce s počítačem a sofwaroví agenti za něj rozhodují, co se mu líbí a co chce vidět nebo dělat.

Není asi nutno rozebírat bezpečnostní aspekty ztráty bezpečného perimetru ve firmě nebo používání vlastního (nepatchovaného) HW a SW ve firmě. Skutečně zajímavý sociologický jev ale je, co všechno si uživatel nechá líbit výměnou za „free“ službu. Nejenže se musí smířit s neuvěřitelným množstvím reklamního balastu, ale jeho software má speciální vlastnosti, které to umožňují (navíc musí být nějak ne-bezpečně nakonfigurován). Loni na podzim Adobe opravoval chybu v Adobe Flash (clickjacking – umožňovala špehovat uživatele webovou kamerou). SANS: „this attack exploits a control on the client side that was placed there for the benefit of the advertisers who buy Flash.“

Mimochodem, citát z Adobe Licence Agreement:
Connectivity and Privacy. You acknowledge and agree to the following ... your Computer may connect to a website operated by Adobe, an advertiser, or other third party. Your Internet Protocol address („IP Address“) is sent when this happens. The party hosting the site may use technology to send (or „serve“) advertising or other electronic content that appears in or near the opened PDF file. The website operator may also use JavaScript, web beacons (also known as action tags or single-pixel gifs), and other technologies... Adobe may not have access to or control over features that a third party may use, and the information practices of third party websites are not covered by the Adobe Online Privacy Policy.

Jinými slovy uživatel souhlasí s tím, že mu kterákoliv třetí strana může kdykoliv poslat na počítač jakýkoliv content, za který ale Adobe neručí...

Celá kultura současného Internetu tzv. free služeb vytváří hektickou atmosféru, kdy uživateli někdo něco neustále podstrkává, inzerenti reklamy, kamarádi odkazy na veselá videa, kolegové odkazy na dokumenty, certifikační autorita výzvu k obnovení čehosi atd. atd., a uživatel kliká. Kromě toho je možné si stáhnout spoustu cool aplikací třeba z Android Marketu, a vše se vyřídí po Internetu, ani nemusí chodit do banky. Sám tomu moc nerozumí, ale je to bezpečné, říkal to ten pán v bance, a ostatní lumíci také klikají. Pán v bance ale nikdy neslyšel o MitB (Man-in-the-Browser), který žije mezi HTTPS a uživatelem, nebo o ZitMo (Zeus in the Mobile), který žije v mobilu a odchytává autorizační SMS z banky a posílá je domů. Co je horší, výrobce SW má zcela jiné priority, produkt musí být cool, rychle na trhu a umožnit reklamy, bezpečnost není důležitá a často jí ani nerozumí. To se může stát i renomovaným firmám, např. Microsoft v CE Windows „šifroval“ hesla tak, že je zXORoval se slovem PEGASUS psaným pozpátku, po leta nechápal, že streamové šifry jako RC4 musí mít náhodný unikátní IV, nepoužíval salt, zato používal v NTLM samotné hashe hesel pro autentizaci (!), nebo v LEAP MS CHAPv.2 šikovně snížili entropii (i přes použití DES). Jiní výrobci jsou na tom podobně, i Cisco mělo ve svém materiálu o bezpečnosti v 802.11 roztomilé povídání o tom, kterak ECB šifra vzniká tak, že se vygeneruje stream key a ten se zXORuje s plaintextem :-o). I samozvaní mistři bývají často mimo mísu, skupina Hackers Choice např. útočí na PKI proto,

že dává komerčním společnostem (tj. CA) „a master key to ALL SSL traffic“. Často jsou pak problémy nikoliv v samotných šifrách, ale v implementaci a okolí, málokde je vidět snaha po bezpečném programování (OWASPGuide) a ve světě Web 2.0, mashupů a reusabilních kódů se často používají data a SW z různých zdrojů, které vznikly mimo bezpečnostní kontext procesu.

Internet poháněný reklamami pak představuje ideální prostředí pro šíření malwaru, a ve skutečnosti se hranice mezi adware, malvertising a malware často smazává, protože používají stejné metody šíření, chovají se stejně agresivně, nejdou obvykle deinstalovat a malvertising stejným způsobem sbírá a odesílá informace o uživateli. Malware používá k šíření často reklamní sítě a používá také stejné techniky, aby se ve výsledcích hledání posunul na výhodnější místo. Podle odhadu Googlu se na 1,3 % všech dotazů vrací seznam výsledků, obsahující alespoň jedno URL označené jako „malicious“.

IT bezpečnost organizací je spíš mimo rozsah tohoto příspěvku; organizace samozřejmě nemohou zanedbat tradiční hrozby (insider threat), musí mít přehled o svých IT aktivech, procesech a odpovědnostech a alespoň částečně je řídit pomocí standardních mechanizmů jako ISMS (Information Security Management System podle ISO 27002) nebo BCM (Business Continuity Management podle ČSN BS 25999-1). Papírování ale nestačí; USA se teprve letos vzpamatovávají z toho, čemu Vivek Kundra říká culture of compliance. Opatření musí být reálná, musí zahrnovat technická řešení jako aktualizace, testování a trvalé monitorování, oddělení systému pro citlivé informace a také školení uživatelů.

Obecně tedy nejslabším článkem bezpečnosti zůstává člověk – koncový uživatel. Když na samém konci loňského roku Anonymous hákli Stratfor, publikovali skoro milion zašifrovaných hesel (tj. hashí) bezpečnostních specialistů. Tech Herald je cvičně proběhl s nástrojem Hashcat, a během 7 minut měli 25 000 hesel, a o 4 hodiny později dalších 50 000, kde byly takové skvosty jako qwerty, 123456, Robert, atd. Přestože slabá hesla zůstávají oblíbeným útočným vektorem, zejména při APT bývá úvodní útok vícenásobný a jeho součástí je skoro vždy pečlivě vypracovaný phishing (tzv. blended email). Tyto emaily, i když jsou určeny jednotlivému člověku, mohou být jen předstupeň k tomu, aby útočník pronikl nejen do účtu oběti, ale také do citlivých systémů společnosti (např. průnik do RSA byl přes phishing,který využil chybu v Adobe Flash Reader). Nejlepší obrana je přemýšlet, ale to může být obtížné...

Příklady

Když přijde normálnímu člověku následující lákavý mail, tak asi lákání nepodlehne:
Date: Wed, 30 Nov 2011 00:46:53 -0800
From: Albina <detert@dlh.de>

Maybe its error... Who are you??? Who have this e-mail address??
I will be glad, if I will be received answer from man, who wishes dialogue with young blue-eyed girl with name Albina))) you can write to me here: albina-sobolev@rambler.ru
I hope, that my English understood))

Totéž platí, když jde o peníze, tak přesvědčivě nabízené:

From: Juan Rua <juan-rua@comunicaciones.udea.edu.co>
Reply-To: mrsmithraymond01@hotmail.com
To je oficiálne oznámit, že výsledek našeho pocítace cerpat 844 tohoto dne zvolený Vaše jméno a e-mailovou adresu pripojen k vstupenek Císlo 034-22478556 s poradovým císlem 129, které následne vyhrál Velká Británie Lottery velkou udelování cen v 2. category.You mít bylo potvrzeno, že vítez kategorie B ve Spojeném království Lottery vylosuje pocítac remíz. Vaše tvrzení soubor byl rádne predána k tomuto kancelár s pokyny, které jsme se pri manipulaci s prevodem Vaší cenu 1,000000.00 ? GBP. (One Million Velká Británie libra) na Váš úcet nominován. Laskave poslat níže informace o pohledávky.

Co ale, když přijde takovýhle mail?

Date: Sun, 18 Mar 2012 17:48:45 -0400
From: Adobe <newsletter@response.adobesystemsinc.com>
Subject: 2012 Release - New PDF Reader/Creator Upgrade
Get The New PDF Reader/Creator Release
Adobe is pleased to announce new version upgrades for Adobe Acrobat Reader
http://www.2012-adobe-online-update.com [www.2012-adobe-online-update.com]
New Version Features :
...
To upgrade and enhance your work productivity today, go to:
http://www.2012-adobe-online-update.com [www.2012-adobe-online-update.com]
Our whole team has been working hard to satisfy your product needs.
Start downloading the update right now and let us know what you think about it.
We‘re working on making Adobe Acrobat Reader better all the time!
Copyright 2012 Adobe Systems Incorporated. All rights reserved.
Adobe Systems Incorporated
343 Preston Street
Ottawa, ON K1S 1N4
Canada

Jedna z možností je si ten mail trochu rozebrat.

```
envelope-from="BakerCommunications@en25.com"; helo=e214.en25.com;
client-ip=209.167.231.214
```

Ukáže se, že hlavičky jsou přepsány, že mail přišel přes SMTP z e214.en25.com, že response.adobesystemsinc.com neexistuje, zato existuje 2012-adobe-online-

update.com, a surprise surprise, je to registrováno v Rusku a bylo to registrováno ten den, kdy přišel přislušný mail:

```
Domain Name: 2012-ADOBE-ONLINE-UPDATE.COM
  Registrar: REGIONAL NETWORK INFORMATION CENTER, JSC DBA RU-CENTER
  Name Server: NS3.NIC.RU
  Creation Date: 18-mar-2012
```

S trochou práce je tedy zřejmé, že mi to asi nepíše Adobe ;-).

Nicméně, co když tu práci do toho někdo dát neumí? Každý uživatel by měl tedy vědět, že nemá klikat na kdejaké URL, které mu přijde, a měl by se umět zamyslet, proč právě teď Adobe pocítilo nezkrotnou touhu mu něco tak zásadního sdělit (když to nikdy před tím neudělali). Tady se ukazuje, že při práci s Internetem, stejně jako s motorovou pilou, je zapotřebí být opatrný a především MYSLET!

Kryptoanarchia – 20 rokov od napisania kryptoanarchistickeho manifesta

Pavol Lupták

E-mail: pavol.luptak@nethemba.com

Abstrakt

Anonymná kryptomena Bitcoin sa aj napriek nedávnym fluktuáciám špekulantov stabilizovala a je nenahraditeľná v Internetovom undergrounde. Vzniká nový anonymný kompletne neregulovateľný voľný trh. „Escrow“ služby ako ClearCoin, či Silk Road a reputačné systémy ako Bitcoin OTC sa stávajú čím ďalej, tým populárnejšie v eliminácii rizika anonymných obchodov – a to všetko bez potreby akejkoľvek centrálnej autority. Kryptoanarchia predpovedaná pred 20 rokmi vizionárom Timothy C. Mayom sa stáva krutou realitou.

Autor příspěvek nedodal.

Základní registry

Jiří Gallas

E-mail: jiri.gallas@i.cz

1 Úvod

Od 1. 7. 2010 vešel v platnost zákon 111/2009 Sb. O základních registrech a zákon 227/2009 Sb. O změně některé zákonů v souvislosti s přijetím zákona o základních registrech, tak zvaný „tusťoch“ (mění 194 zákonů).

Od 1. 7. 2012 mají být základní registry spuštěny. Jmenované zákony při tom předpokládaly spuštění pilotního provozu k 1. 7. 2010 a ostrého provozu od 1. 7. 2011. Legislativní cestou byl start základních registrů odložen o rok. Všechny projekty jsou financovány prostřednictvím

1.1 Timelineline – trnitá cesta k registrům

1.1.1 Vývoj legislativy

Záměr vybudování registrů základní správy zrál poměrně dlouho a prodělával v některých fázích bouřlivý vývoj a jindy období letargie až hibernace. Po představu uvádím aktivity, které předcházely vydání zákona o základních registrech:

2000–2001	Návrh věcného záměru zákonné úpravy registrů veřejné správy (prošel)
2004	Návrh věcného návrhu zákona o sdílení dat při výkonu veřejné správy (prošel)
2005	Návrh zákona sdílení dat při výkonu veřejné správy (staženo)
2008	Návrh zákona o základních registrech + 4 zákony základních registrů
2008–2009	Zákon o základních registrech (sloučeno z původního návrhu)

Schválení zákona 111/2009 Sb. dne 26. 3. 2009
Schválení zákona 227/2009 Sb. dne 17. 6.2009
. . . a řada novelizací

1.1.2 Původní představy o časování projektů

V čase schválení zákona byla představa o budování základních registrů zhruba tato:

Aktivita	**Termín**
Podpis smlouvy	30. 6. 2009
Analytická příprava jádra	31. 12. 2009
Protokol o převzetí HW + SW	29. 1. 2010
Funkční prototyp jádra	26. 2. 2010
Akceptace pro pilotní provoz	30. 6. 2010
Protokol o převzetí HW + SW	30. 9. 2010
Protokol o přenosu dat	30. 9. 2010
Protokol o zátěžovém testu	30. 11. 2010
Akceptace integračního testu	31. 3. 2011
Akceptace pro ostrý provoz	30. 6. 2011

1.1.3 Reálné termíny

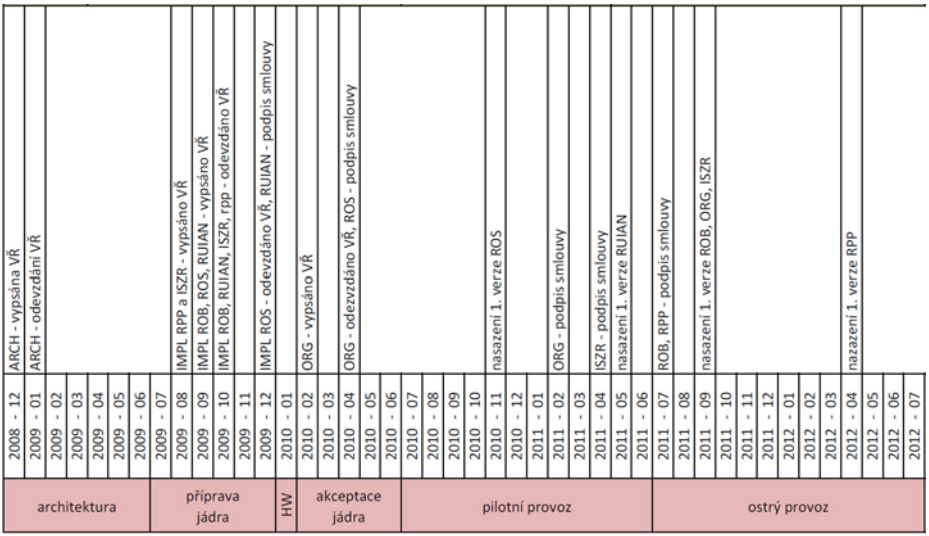
Bylo rozhodnuto o tom, že architekturu jednotlivých registrů navrhnou architekti. Architekturu každé části navrhoval povinně jiný dodavatel, který pak byl vyloučen z výběrových řízení na vlastní realizaci. Dlužno podotknout, že vlastní rámec architektury – tedy rozdělení a obsah částí systému byl dopředu stanoven legislativou a dále upřesněn zadávacími podmínkami pro výběrová řízení architektů. Výjimkou je ORG, který měl jen jedno výběrové řízení na architekturu a realizaci.

Časový start byl relativně shodný, ale jednotlivé registry se z důvodů problémů s výběrovými řízeními a odvoláváním proti výsledku soutěže a dalších neplánovaných zdržení postupně zcela rozfázovaly. Došlo k tomu, že některé části systému již byly v realizaci a jiné stále neměly na realizaci uzavřenou smlouvu.

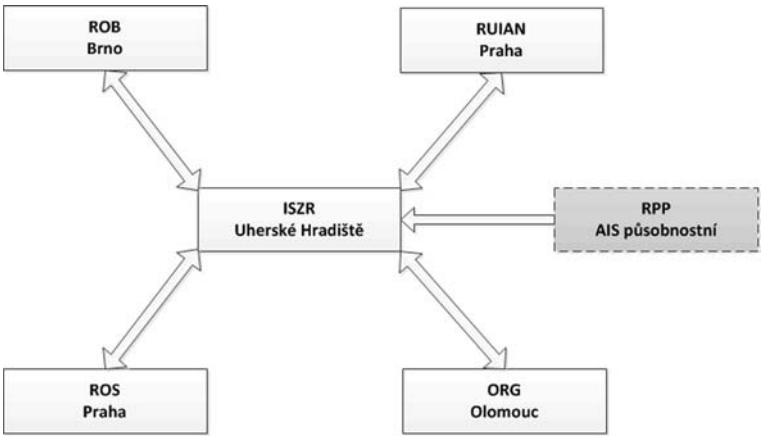
Když si vyneseme do časové osy s přesností na měsíce vyneseme hlavní milníky, dostaneme tento zajímavý obrázek 1.

V tabulce není nakresleno mnoho dalších milníků – jejich zanesením by zcela ztratila na přehlednosti.

Jeden ze zajímavých milníků by byl datum vytvoření sálu pro umístění základních registrů. Všichni realizátoři měli zadáno (kromě RUIAN), že systémy budou umístěny v jedné lokalitě, kterou poskytne CMS (Centrální Místo Služeb). Původní představa byla taková, že HW bude dodán pímo do CMS v lednu 2010. CMS mělo později být hotovo v březnu 2010, dubnu 2011, potom v říjnu 2011, ... Realita je zatím taková, že na začátku dubna 2012 stále nebylo řádně připraveno. Jeho neexistence donutila jednotlivé zadavatele umístit jednotlivé části systému doslova kde to šlo. Start testovacího prostředí proto vypadal takto (registr RPP byl přítomen pouze ve formě dat pro matici oprávnění) – obr. 2.



Obr. 1 Časový průběh realizace projektů základních registrů



Obr. 2 Základní registry a jejich dočasné rozmístění

V týdnu od 10. 4. 2012 bylo zahájena první vlna stěhování částí systému do cílových lokalit. Optimistické varianty odhadují, že zprovoznění systémů v cílových lokalitách bude dokončeno v průběhu první poloviny června.

2 Základní představy o funkcích základních registrů

Základní myšlenka základních registrů je vybavit státní správu přístupem k základní sadě údajů ze spolehlivého zdroje, kterou může pracovník státní správy použít bez toho, aby bylo nutno dokladovat že údaje jsou platné. Zákon říká doslova „Referenční údaj je považován za správný, pokud není prokázán opak nebo pokud nevznikne oprávněná pochybnost o správnosti referenčního údaje".

Základní registry disponují pouze velmi omezenou množinou referenčních údajů. Tato množina je dána jednak obavou, aby se podařilo registry v reálném čase vůbec naplnit a také patrně proto, aby nedošlo k silnějšímu protitlaku inicializovanému obavou ze shromažďování dat v jednom systému. Z tohoto důvodu také patrně byl systém dopředu rozdělen na jednotlivé registry.

Základní registry obsahují pouze aktuální údaje. Znamená to, že do nich nelze zapisovat údaje, které nabudou účinnost v budoucnosti a při skončení platnosti je nutno údaj vymazat. Platí to například o místě pobytu nebo o dokladu.

2.1 ZIFO a AIFO – identifikace fyzických osob

Opravdu revoluční myšlena je zavedení identifikátoru osoby, který bude povinně v každém informačním systému jiný. Ačkoli zákon 111/2009 Sb. hovoří výhradně o identifikátoru AIFO, mnohem důležitějším identifikátorem je ZIFO – Základní Identifikátor Fyzické osoby. Zákon bohužel pojem ZIFO nedefinuje a nepoužívá a tím vzniká trochu zmatek.

Definujme si pro další dva pojmy: fyzickou a elektronickou identitu. Fyzickou identitou a představuji si ji jako člověka jednoznačně určeného (například analýzou DNA a otisky prstů). Elektronickou identitou v systému ZR je pak jedinečný identifikátor, který se jmenuje ZIFO a generuje jej podle interních pravidel ORG.

Základní myšlenka je taková, že primární editor ROB přidělí každé fyzické identitě jednu elektronickou identitu a toto přidělení si zapíše do své agendy. Následně pak do ROB vloží záznam osoby a ostatní agendy na základě porovnání osobních údajů získají odpovídající AIFO i pro své agendy.

Zákon počítá s eventualitou, že dojde k chybnému „napárování" těchto identit – jedna fyzická identita bude mít přidělena v ORG dvě elektronické identity, nebo opačný případ, kdy dvě fyzické identity budou mít přiděleno pouze jednu elektronickou identitu. V obou případech zákon stanoví že se původní elektronické identity zneplatní a přidělí se nové. ORG poskytuje jak funkce pro provedení této operace, tak funkce pro zjištění co se se zneplatněnou elektronickou identitou stalo.

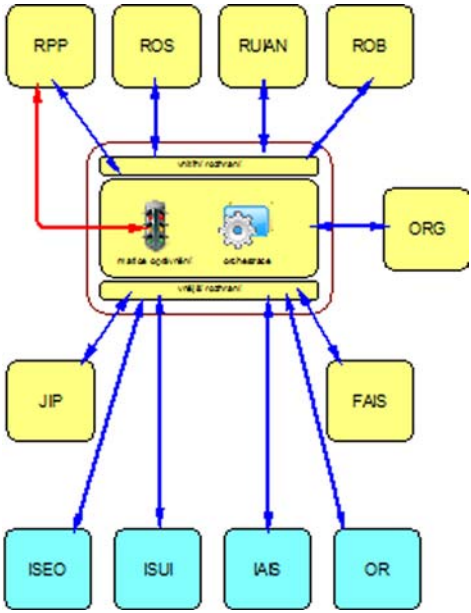
3 Co kde dělá, co uchovává

Podle zákona základní registry obsahují několik různých druhů údajů:

1. Referenční údaje (jméno, příjmení, název, ...). Podle zákona jsou to ty údaje v registru, které jsou vyjmenovány jako referenční. Správnost referenčního údaje nemusí nikdo dokazovat, považuje se za správný, pokud není označen jako nesprávný.
2. Referenční vazby. Jsou to „kódy nebo identifikátory, kterými je odkazováno na referenční údaje v základních registrech“, tj. odkazy mezi základními registry (IČO, IČP, ...).
3. Identifikátory fyzických osob – AIFO.
4. Autentizační údaje, tj. údaje umožňující provést ověření identity fyzické osoby (BOK).
5. Provozní údaje (čas změny údaje v registru, logy).

3.1 Rozdělení úloh základních registrů

Základní uspořádání systému základních registrů je na obrázku 3. Systém se skládá ze šesti částí, každá má jasně stanovenou úlohu v rámci systému:



Obr. 3 Základní registry versus agendové systémy

1. ISZR (Integrovaný Systém Základních Registrů) – centrální část, která obsluhuje vnější rozhraní na kterém jsou napojeny tzv. AIS (agendové Informační Systémy). Pomocí vnitřního rozhraní pak komunikuje se čtyřmi ZR (Základními Registry) a s ORG (převodník agendových identifikátorů fyzických osob). Veškeré přístupy ověřuje v matici oprávnění, kterou získává z registru RPP. Provádí orchestraci služeb. Neobsahuje žádné referenční údaje. Loguje veškerou komunikaci pro případné právní spory a logy udržuje po dobu 1 roku. Agendové systémy editorů jsou zdrojem dat pro registry a zákon stanoví, že základní registr musí být možné v případě havárie z agentových systémů znovu naplnit.

2. RPP (Registr Práv a Povinností). Obsahuje MO (Matici Oprávnění), ve které jsou zapsána oprávnění jednotlivých agend a rolí jejich uživatelů. Pro MO eviduje OVM (Orgány Veřejné Moci) a jejich práva vykonávat agendy. Registr dále obsahuje údaje o rozhodnutích OVM a důvodech změn referenčních údajů v základních registrech. Aby nevystupoval v roli „velkého bratra“, nepoužívá se v RPP $\mathrm{AIFO}_{\mathrm{RPP}}$, ale $\mathrm{AIFO}_{\mathrm{AIS}}$, který do RPP rozhodnutí zapisuje. Proto při čtení rozhodnutí o jedné osobě z RPP musí použít ISZR speciální postupy. Výdej dat z RPP se loguje a uchovává po dobu 1 roku.

3. ROS (Registr Osob) obsahuje základní údaje o všech ekonomicky činných subjektech a o OVM. Základním identifikátorem subjektu je IČO. Eviduje provozovny podle živnostenského zákona a přiděluje jim IČP (identifikační číslo provozovny). Výdej dat z ROS se loguje a uchovává po dobu 1 roku.

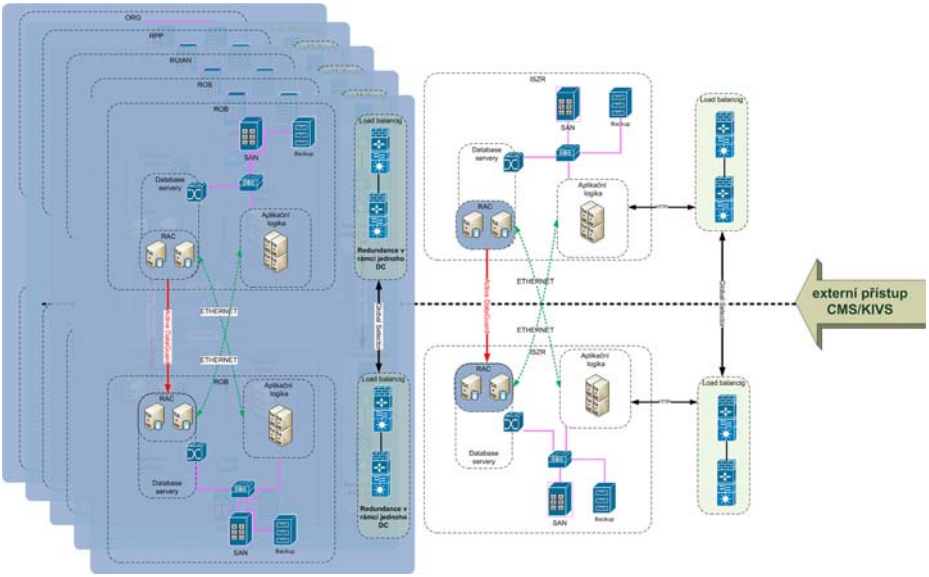
4. RUIAN (Registr Územní identifikace a Nemovitostí) obsahuje údaje o adresním systému – náhrada UIR-ADR a vybrané údaje z katastrálního systému. Vzhledem k tomu, že obsahuje veřejné údaje, loguje jen změnové požadavky.

5. ROB (Registr Obyvatel) obsahuje nejzákladnější sadu údajů o fyzických osobách pobývajících na území republiky. Poskytuje autentizační službu založenou na čísle občanského průkazu a BOK (Bezpečnostní Osobní Kód). Všechny přístupy do Rob se logují a uchovávají po celou dobu, kdy je fyzická osoba vedena v ROB a ještě 10 let po likvidaci jejích údajů v ROB.

6. ORG (převodník agendových identifikátorů fyzických osob) přiděluje pro jednotlivé informační systémy AIFO a provádí jeho převod. Služby pro převod AIFO volá při zpracování služby ISZR a tyto služby nejsou na vnějším rozhraní dostupné. Obsahuje pouze identifikátory fyzických osob a informace nezbytné pro převod AIFO, neosahuje žádné referenční údaje.

3.2 Technické řešení základních registrů

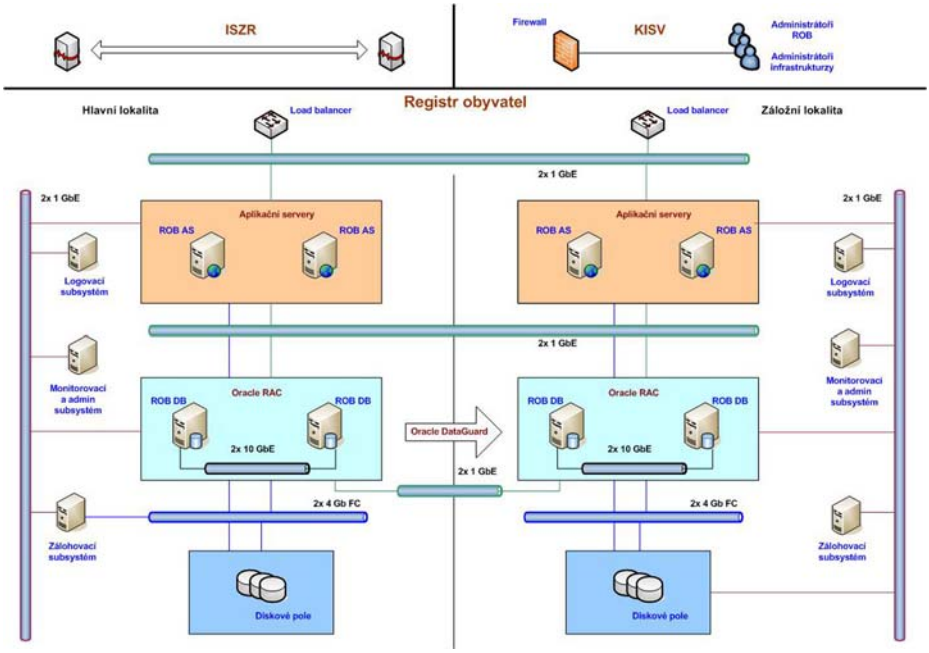
Vzhledem k požadavkům na velkou dostupnost byla od všech systémů požadováno vytvoření geoclusteru, přičemž podle zadání mají být obě části geoclusteru rovnocenné. Lokalita pak obsahuje lokální cluster (shodně jsou použity technologie s databází ORACLE) a přenos dat z primární lokality na sekundární lokalitu e realizován pomocí technologie Oracle DataGuard.



Obr. 4 Propojení sytému základních registrů v CMS

Řešení umožňuje využít primární lokalitu pro editace a „rychlé“ synchronní dotazy, sekundární lokalitu pro zpracování pomalejších (protože náročnějších) a případně asynchronních dotazů typu výdej provozních údajů. Řešení použité na ROB a ROS umožňuje, aby do zpracování služeb byly zapojeny aplikační servery na obou lokalitách s tím, že podle typu služby dochází na aplikačním serveru ke směrování dotazu do správné lokality.

Geocluster a ORACLE jsou ale jediné styčné body v technologii, jinak každá část systému má jiného výrobce HW (Orace, HP, IBM, ...) a jsou použity i různé SW platformy – například ISZR je psáno v C#, ROB a ROS v Javě. Každý systém má svoje vlastní diskové pole a zálohovací robot.



Obr. 5 Hrubá topologie geoclusteru ROB

3.3 Referenční údaje v ZR

3.3.1 RUIAN

Vede dva základní okruhy referenčních údajů – údaje katastru nemovitostí a údaje systému územní identifikace (adresní sytém).

Mezi údaje katastru nemovitostí patří: katastr, parcela, nemovitost, stavební objekt, pozemek. Neobsahuje údaje o vlastníku.

Údaje systému územní identifikace jsou: adresní místo, stavební objekt, ulice, číslo popisné, číslo orientační, obec nebo vojenský újezd, správní obvod obce s rozšířenou působností, obce s pověřeným obecním úřadem, městské obvody, městské části, okresy, kraje a vyšší správní celky.

RUIAN neobsahuje údaje o vlastnících parcel a stavebních objektů. Tyto údaje bude ale možné číst z agend primárních editorů RUIAN (ovšem nikoli jako referenční).

3.3.2 ROB

Obsahuje jen minimální množinu referenčních údajů: jméno, příjmení, datum a místo narození, adresu pobytu, doručovací adresu a identifikátor datové schrán-

ky, občanství, elektronicky čitelné doklady (pro OP také BOK) a datum a místo úmrtí.

Agendy v ROBu postrádají zejména rodné číslo, rodné příjmení, způsobilost k právním úkonům a některé další údaje.

3.3.3 ROS

Rovněž ROS obsahuje velmi minimalistickou množinu údajů

1. Pro fyzické osoby: IČO, název (= jméno a příjmení fyzické osoby), jméno a příjmení a adresu pobytu nebo AIFO, datum vzniku/zápisu, datum zániku, právní formu dle číselníku ČSÚ, identifikátor datové schránky.

2. Pro právnické osoby: IČO, název, datum vzniku/zápisu, datum zániku, právní formu dle číselníku ČSÚ, identifikátory datových schránek, statutární orgány (AIFO, nebo jméno, příjmení a adresa pobytu).

Pokud má osoba provozovny podle živnostenského zákona, vedou se tyto provozovny včetně jejich identifikátorů IČP. Editorem těchto provozoven je pro všechny osoby RŽP.

Dále se vede právní stav dle číselníku, editorem tohoto údaje je pro všechny osoby insolvenční rejstřík nebo jeho předchůdce evidence úpadců.

Identifikátory IČO a IČP přiděluje ROS na základě elektronické žádosti agendy editora.

Zákon 111/2009 Sb. Stanoví, že jedna fyzická osoba smí mít pouze jedno IČO. Dále stanoví, že IČO pro právnické osoby se vydává na základě názvu – to je revoluční, protože nebude možné získat IČO pro název, který již byl použit.

Agendy v ROS postrádají zejména vedení jiných provozoven než provozoven podle živnostenského zákona a samozřejmě také jednotlivé činnosti, které smí osoba vykonávat.

3.3.4 RPP

Obsahuje dva druhy údajů: referenční údaje o agendě orgánu veřejné moci a referenční údaje o právech a povinnostech osob. Při zápisu každého rozhodnutí musí zapisující agenda určit, které agendy mají právo rozhodnutí číst.

3.3.5 ORG

ORG nevede žádné osobní údaje a nevede ani referenční údaje – není to základní registr.

ORG si můžeme představit jako velikou tabulku, kde řádky jsou jednotlivé identity a sloupce jednotlivé výpočetní systémy. AIFO jsou pak hodnoty v buňkách. Pro převod AIFO je vždy potřeba zadat AIFO, sloupec ze kterého pochází a sloupec ze kterého se má vzít výsledná hodnota.

ORG musí zaručit, že ve sloupcích nedojde k vygenerování duplicitního čísla. Mezi sloupci jsou duplicity povoleny, protože pro převod AIFO je nutné uvést ve kterém sloupci hledat.

Tab. 1 Princip ORG

ZIFO	SK1	SK2	SK3	SK4
256	789	989	141	780
478	569	946	157	983
591	478	572	497	651
294	267	349	572	349
255	801	189	199	247

Například, převod AIFO = 572, SK3 na SK1 je 267.

Podstatné je, že o přidělení ZIFO identitě rozhoduje tzv. primární editor ROB – to znamená správce agendového systému ISEO nebo CIS. Jedině tyto agendy mají právo od ORG vyžádat vytvoření nového řádku v pomyslné matici – požádat o přidělení ZIFO. ORG přidělí interně nové ZIFO a agendě současně odvodí odpovídající AIFO. Agenda si pak AIFO zapíše do své evidence – tím je fyzické osobě jednoznačně přidělena identita.

3.3.6 ... a ještě ISZR

ISZR neobsahuje žádné referenční údaje, ale má několik důležitých a nezastupitelných úloh:

1. Na základě matice oprávnění ověřuje, zda služba smí být volána
2. Zabezpečuje orchestraci eGON služby, tj. zejména vykonává pro každou službu volání různých interních služeb

Ověření práva volat službu

Ověření se děje kontrolou záhlaví služby vůči matici oprávnění MO. MO je trojrozměrná matice, jejími rozměry jsou služba, role („cinnost!“), agenda. Každý bod matice pak obsahuje seznam údajů, které smí být ve volání služby použity. Ke každé činnosti navíc existuje seznam OVM, které ji smějí vykonávat.

Přitom platí tato pravidla:

1. Agendový systém komunikuje s ISZR na HTTPS bázi, přičemž certifikát pro tuto komunikaci vydává Správa základních registrů (používá se neve-

řejná certifikační autorita ISZR). K certifikátu se eviduje, za jaké agendy smí příslušný AIS vystupovat.

2. Komunikace se vždy navazuje z aktivity agendového systému (výjimku mohou tvořit asynchronní odpovědi).

3. Za správnost informací v hlavičce volání služby odpovídá správce systému, který dotaz posílá. ISZR tyto informace používá pro autorizaci požadavku v MO.

Tab. 2 Příklad matice oprávnění

AGENDA	ČINNOST	POPIS ČINNOSTI	robVlozObyvatele	robZmenObyvatele	robCtiAIFO	robAutentizace	robCtiPodleUdaju	robVymazObyvatele	robCtiZmeny	robCtiHromadneAIFO
A115	CR793	Správa agendy	+	+	+	+	+	+	+	+
A115	CR794	Zápis údajů MV		+	+	+	+			
A115	CR795	Zápis údajů krajským úřadem	+	+	+	+	+			
A115	CR796	Zápis údajů obecním úřadem obce s rozšířenou působnosti		+	+	+	+			
A115	CR797	Zápis údajů matričním úřadem	+	+	+	+	+			
A115	CR798	Zápis údajů ohlašovnou		+	+	+	+			
A115	CR799	Zápis údajů soudem prvního stupně		+	+	+	+			
A115	CR800	Změny nebo zrušení údajů MV		+	+	+	+			
A115	CR801	Změny nebo zrušení údajů krajským úřadem	+	+	+	+	+			
A115	CR802	Změny nebo zrušení údajů obecním úřadem obce s rozšířenou působnosti		+	+	+	+			
A115	CR803	Změny nebo zrušení údajů matričním úřadem		+	+	+	+			
A115	CR804	Změny nebo zrušení údajů ohlašovnou		+	+	+	+			
A115	CR805	Změny nebo zrušení údajů soudem prvního stupně		+	+	+	+			
A115	CR806	Poskytování údajů			x	+	+			

Pokud ISZR v matici oprávnění ověří, ze existuje povolení službu volat, ověří ještě oprávnění použít jednotlivé údaje.

Zpracování eGON služby

Při kontrole oprávnění agendy využije ISZR údaje *KodSlužby* a položky struktury *ZadostInfo*. Jak bylo popsáno, z HTTPS komunikace ví s jakým systémem komunikuje a za jaké agendy může AIS vystupovat. Příklad hodnot v žádosti:

```
<urn:KodSluzby>RobCtiAifo</urn:KodSluzby>
<urn:ZadostInfo>
  <reg:CasZadosti>2011-12-12T15:18:05.967</reg:CasZadosti>
  <reg:Agenda>A117</reg:Agenda>
  <reg:AgendovaRole>CR128</reg:AgendovaRole>
  <reg:Ovm>00006874</reg:Ovm>
  <reg:Ais>33</reg:Ais>
  <reg:Subjekt>Subjekt</reg:Subjekt>
  <reg:Uzivatel>Uživatel</reg:Uzivatel>
  <reg:DuvodUcel>Důvod a˜úče</reg:DuvodUcel>
  <reg:AgendaZadostId>d2de21bb-3230-4a8e-bb02-51080ce216c8</reg:AgendaZadostId>
</urn:ZadostInfo>
```

Nejprve se zkontroluje, že AIS = 33 sedí na certifikát a že OVM = 00006874 může pro komunikaci tento AIS využívat. V matici oprávnění ověří, že sužbu RobCtiAifo smí agenda A117 pro dané OVM a roli CR128 volat.

Dále se zkontroluje, že CasZadosti je vyhovuje stanovenému časovému oknu a že AgendaZadostId není duplicitní (duplicitní požadavek je odmítnut).

Z matice vyzvedne ISZR seznam údajů, které je možno ve službě použít.

Hodnoty Subjekt, Uzivatel, DuvodUcel ISZR neověřuje; je na agendovém systému, aby zabezpečil že tyto údaje jsou vzhledem k uživateli který službu inicioval správné. ISZR qa ROB tyto údaje logují a agenda je musí logovat rovněž. V případě kontroly musí AIS doložit která konkrétní osoba je za daný požadavek odpovědná a v rámci agendy musí být možno ověřit důvod proč byla služba volána.

Dále dojde k ověření údajů, které agenda z registu požaduje. Tyto údaje jsou ve striktuře SeznamUdaju, pro ROB například v RobSeznamUdaju:

```
<reg:SeznamUdaju>

  <reg:RobSeznamUdaju>Aifo Prijmeni Jmeno AdresaPobytu DorucovaciAdresa
  DatumNarozeni MistoNarozeni DatumUmrti DatumPravniMociUmrti MistoUmrti
  DatovaSchranka Doklad Obcanstvi </reg:RobSeznamUdaju>

</reg:SeznamUdaju>
```

ISZR porovná tento seznam se seznamem získaným z matice oprávnění. Pokud je v požadavku údaj, na který není oprávnění, je zpracování služby ukončeno z důvodu nedostatku oprávnění.

Kromě kontroly oprávnění musí ISZR zajistit zpracování různých informací v různých registrech. Ukážeme si to na příkladu zpracování služeb ROB, který

nemá žádnou službu kterou by bylo možno zpracovat bez volání dalších částí systému.

Vzhledem k identifikaci osob pomocí AIFO jde především o využívání volání služeb ORG pro převod AIFO. Další částí SZR která se při zpracování eGON služeb ROB musí použít je RUIAN, ve kterém se kontroluje existence referenčních odkazů a případně se doplňují referenční údaje z referenčních vazeb.

Způsob zpracování eGON služeb ROB je v tabulce 3.

Tab. 3 Princip ORG

eGON	**int. sl.**	**název služby**	**pořadí workflow**
E01	O01	robVlozObyvatele	A28 G02 O01 G27
E06	O06	robVymazObyvatele	G03 O06 G03
E102	O17	robPoskytnutiJineOsobe	G27 O17
E02	O02	robZmenObyvatele	A28 G27 O02 G27 I07
E11	O11	robVytvorBlokaci	G27 O11 G27
E12	O12	robVypisBlokace	G27 O12
E13	O13	robZrusBlokaci	G27 O13
E103	O21	robCtiZmenyZaloz	O21 G27
E03	O03	robCtiAIFO	G27 O03 G27 A28
E05	O05	robCtiPodleUdaju	A28 O05 G02 A28
E07	O07	robCtiZmeny	O07 G17
E08	O08	robCtiHromadneAIFO	G27 O08 G27 A28
E15	O16	robCtiEditora	G27 O16
E04	O04	robAutentizace	O04 G02

Tab. 4 Služby použité v tabulce 3

A28	ruianCtiProROB
G02	orgZalozAIFO
G03	orgCtiZruseneAIFO
G17	orgCtiNotifikaceAIFO
G27	orgCtiAIFO

Příklad výsledku pro službu *robCtiHromadneAifo* po ověření hodnot v RUIAN a překladu AIFO v ORG:

```
<urn:RobSyncDotazResponse xmlns:urn="urn:cz:isvs:rob:schemas:RobUnivDotazy:v1">
  <urn:KodSluzby>RobCtiHromadneAifo</urn:KodSluzby>
    <urn:OdpovedInfo>
      <reg:CasOdpovedi>2012-01-09T14:10:17.2801761+01:00</reg:CasOdpovedi>
       <reg:Status>
```

```
      <reg:VysledekKod>OK</reg:VysledekKod>
   </reg:Status>
   <reg:AgendaZadostId>2bc586df-0194-4cc9-9b2c-05b73b9ef681
        </reg:AgendaZadostId>
   <reg:IszrZadostId>15ee6f10-966e-11b2-9516-0901d7e3f144</reg:IszrZadostId>
</urn:OdpovedInfo>
<urn:MapaAifo lokalniAifoOd="2">
   <reg:PrevodAifo>
      <reg:LokalniAifo stavOvereniAifo="true">1</reg:LokalniAifo>
      <reg:GlobalniAifo>goze3rHWHpu63qBkKNtruzk=</reg:GlobalniAifo>
   </reg:PrevodAifo>
</urn:MapaAifo>
<urn:SeznamIdAdres>
  <reg:AdresniMisto stavOvereniPrvku="existuje">22986847</reg:AdresniMisto>
  <reg:AdresniMisto stavOvereniPrvku="existuje">11145161</reg:AdresniMisto>
  <reg:AdresniLokalita stavOvereniPrvku="existuje"
                                  typPrvku="OB">580031</reg:AdresniLokalita>
  <reg:AdresniLokalita stavOvereniPrvku="existuje"
                                  typPrvku="OB">500011</reg:AdresniLokalita>
</urn:SeznamIdAdres>
<urn:RobOdpoved>
 <urn2:RobCtiHromadneAifoDataResponse
       xmlns:urn2="urn:cz:isvs:rob:schemas:RobDotazyData:v1">
   <rod:RobAplikacniStatus>
     <rob:VysledekRobKodType>OK</rob:VysledekRobKodType>
   </rod:RobAplikacniStatus>
   <rod:Osoba>
      <rod:AdresaPobytu stav="spravny">11145161</rod:AdresaPobytu>
      <rod:Aifo stav="spravny">1</rod:Aifo>
      <rod:DatovaSchranka stav="spravny">Ds00001</rod:DatovaSchranka>
      <rod:DatumNarozeni stav="spravny">1991-08-23</rod:DatumNarozeni>
      <rod:DatumPravniMociUmrti stav="spravny">2011-08-23
           </rod:DatumPravniMociUmrti>
      <rod:DatumUmrti stav="spravny">2011-07-23</rod:DatumUmrti>
      <rod:DorucovaciAdresa stav="spravny" typAdresy="adresaCrOdkaz">
        <rob:AdresaCr>22986847</rob:AdresaCr>
      </rod:DorucovaciAdresa>
      <rod:Jmeno stav="spravny">JOSEF</rod:Jmeno>
      <rod:MistoNarozeni stav="spravny">
         <rob:NarozeniCr obec="true">580031</rob:NarozeniCr>
      </rod:MistoNarozeni>
      <rod:MistoUmrti stav="spravny">
         <rob:UmrtiCr obec="true">500011</rob:UmrtiCr>
      </rod:MistoUmrti>
      <rod:Prijmeni stav="spravny" zmenaCas="2011-08-20T00:00:00">
           KUPKA</rod:Prijmeni>
      <rod:Doklady stav="spravny">
         <rob:Cislo>699999501</rob:Cislo>
         <rob:Druh>P</rob:Druh>
      </rod:Doklady>
      <rod:Doklady stav="spravny">
         <rob:Cislo>699999502</rob:Cislo>
```

```
            <rob:Druh>ID</rob:Druh>
          </rod:Doklady>
          <rod:Obcanstvi stav="spravny">203</rod:Obcanstvi>
          <rod:Obcanstvi stav="spravny">36</rod:Obcanstvi>
        </rod:Osoba>
      </urn2:RobCtiHromadneAifoDataResponse>
    </urn:RobOdpoved>
  </urn:RobSyncDotazResponse>
```

3.4 Primární a sekundární editoři

Primárním editorem základního registru je agenda, která smí v tomto registru zakládat nové záznamy, případně je i rušit. Pokud odhlédneme od některých specifik RPP, platí pravidlo že primárním editorem je agenda nejvýše v jednom registru.

Sekundární editor edituje stanovené údaje o subjektu, ale nemá právo založit nebo rušit záznam v registru. Typickým příkladem je szsteém datových schránek, který do ROB a ROS zapisuje identifikátory schránek.

Tab. 5 Registr a jeho editoři

registr	Primární editoři	Sekundární editoři
RUIAN	ISKN, ISUI	–
ROB	ISEO, CIS (a „UFO“)	EOP, ECD, ISDS
ROS	OR, RŽP a řada dalších agend	ISDS, ISIR, RŽP
RPP	AISP, agendy editorů	–

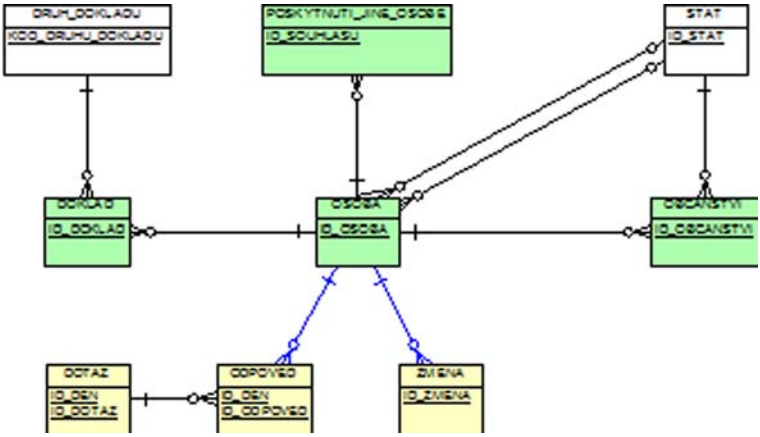
3.4.1 Základní struktura ROB

Na obrázku 6 který mapuje základní entity registru obyvatel a jejich vztahy si můžeme ukázat, jaký je význam rozdělení „pravomocí“ jednotlivých editorů.

Primární editor (ISEO nebo CIS) zakládá a ručí záznamy v tabulce OSOBA. Jednoznačným identifikátorem osoby je přitom AIFO, které přiděluje právě primární editor. Současně tento editor zakládá záznamy o občanství v tabulce OBCANSTVI. Přitom se kontroluje, že ISEO zapisuje osoby s českým občanstvím a CIS osoby bez českého občanství. Primární editor může tyto záznamy rovněž upravovat a mazat.

Záznamy o dokladech jsou složitější – pro české občany edituje občanské průkazy IS EOP, cestovní doklady IS ECD – ty ale mohou založit doklad pouze pro existující osobu. Pro cizince je editorem dokladů CIS.

Záznam o zpřístupněné datové schránce zapisuje pro osoby bez rozdílu občanství IS DS.



Obr. 6 Hlavní entity ROB

ZMĚNA se využívá pro notifikační systém – ukládají se zde všechny provedené změny (AIFO, typ měněného údaje a čas, nikoli hodnota) a tyto údaje je na dotaz možno vydat.

Všechny dotazy a odpovědi na ně se ukládají do DOTAZ a ODPOVED. Z těchto entit se vytvářejí výpisy o využití a poskytnutí údajů.

Otvorené riešenia pre cloud

Michal Fojtík

E-mail: mfojtik@redhat.com

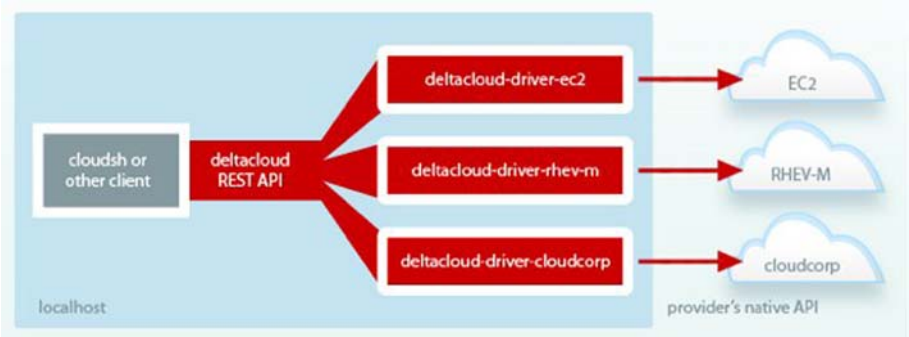
Deltacloud je API vyvíjané spoločnosťou Red Hat a konzorciom Apache Software Foundation, ktorého cieľom je abstrahovať rozdiely medzi rôznymi poskytovateľmi „cloudových“ služieb. Deltacloud bol uvedený firmou Red Hat po prvýkrát 3. Septembra 2009. V tom čase na projekte pracovali výhradne vývojári tejto firmy. V máji 2017 sa Red Hat rozhodol celý projekt otvoriť a poskytnúť komunite a previedol jeho vývoj do takz. „Apache Software Foundation Incubator“. Od toho momentu, sa o riadenie vývoja starala čisto komunita. V októbry 2011 sa Deltacloud stal „top-level“ projektom, priamo zastrešeným Apache Software Foundation, potom ako dokázal, že sa mu podarilo vybudovať dostatočnú komunitu.

Čo teda Apache Deltacloud je? Každý poskytovateľ „Infrastracture-as-a-service“ (IaaS) služieb v dnešnej dobe má svoje API. Pomocov tohto API jeho konzumenti, môžu dynamicky škálovať ich aplikácie ktoré bežia v rámci infraštruktúry týchto poskytovateľov. Je zrejmé, že každý z týchto poskytovateľov, či už sa jedná o verejný alebo privátny cloud, používa vlastné API. V tomto smere neexistuje žiaden štandard, ktorý by definoval ako by malo API na manažovanie „cloudu“ vyzerať (pozn. okrem CIMI, ktoré ešte nie je oficiálne prijaté).

V tomto vidí otvorená komunita ľudí, ktorý s cloudom pracujú obrovskú nevýhodu, ktorá otvára priestor na uzavretie zákazníka ku konkrétnej službe, teda. „vendor-lockin“, tak ako k tomu došlo v histórii už veľakrát.

Apache Deltacloud vnikol preto, aby umožnil ľudom slobodne sa rozhodnúť, akého poskytovateľa si chcú zvoliť a taktiež aby im dal možnosť kedykoľvek, bez väčších nákladov prejsť od jedného poskytovateľa k inému.

Apache Deltacloud je API založené na overenom protokole HTTP (REST, a teda veľmi jednoducho dostupné na využívanie v akomkoľvek programovacom jazyku. Komunikácia s API poskytovateľa je pre klienta úplne transparentná, klient s ním komunikuje pomocou API, ktoré poskytuje Deltacloud. Deltacloud komunikuje s API poskytovateľa prostredníctvom takz. „driverov“, pričom tie definujú, akým spôsobom, bude komunikácia prevedená.



Obr. 1: Deltacloud API – SOA diagram

Momentálne Deltacloud API podporuje všetkých hlavných poskytovateľov IaaS služieb, či už verejných, ako Amazon alebo Rackspace alebo privátnych ako RHEV-M alebo VMWare Vsphere. Počet týchto poskytovateľov sa neustále rozrastá, a to hlavne zásluhou komunity, ktorú väčšinou tvoria programátori práve týchto poskytovateľov.

Jak jsme převáděli desktopovou aplikaci FlexiBee do cloudu

Petr Ferschmann

E-mail: pferschmann@flexibee.eu

Abstrakt

Ekonomický systém FlexiBee je ve své poslední verzi nabízen i jako cloudové řešení. Povíme si o tom, proč službu poskytujeme v cloudu, jaké technické a organizační problémy jsme měli při převodu klasické aplikace do cloudu, jaké architektonické úpravy jsme provedli, co nám to přineslo a jak to vnímají zákazníci (i s ohledem na bezpečnost). Pokusíme se také vysvětlit rozdíly mezi hostingem a cloudem.

Autor příspěvek nedodal.

Kontejnerová virtualizace na Linuxu

Pavel Šimerda

E-mail: pavlix@pavlix.net

Kontejnery jsou jednou z forem izolace procesů běžících fyzicky na jednom hardware. Nejedná se o virtualizaci samotného hardware, ale pouze prostředků, které aplikace využívají. Prostředky se přerozdělují ve formě procesorového času, stránek RAM i swapu, souborových systémů, blokových zařízení, přidělených IP adres i virtuálních síťových karet. O rozdělování prostředků se stará jediné jádro operačního systému společné pro všechny kontejnery.

Kontejnerová virtualiace, nebo chcete-li separace procesů, nabízí bezkonkurenčně nízkou režii. Lze ji používat na prakticky jakémkoli podporovaném hardware, není problém si pustit desítky testovacích kontejnerů třeba na nevýkonném netbooku. Další výhodou je velmi jednoduchá správa a možnost pouštět shell či jednotlivé příkazy přímo, bez virtuálního IO. Za to je potřeba zaplatit omezením, že userspace veškerých kontejnerů sdílí jeden kernel. Ztrácíte tedy flexibilitu a některé vrstvy zabezpečení, které se používají při jiných metodách virtualizace.

Jedním z opensource projektů, které umožňují spouštění kontejnerů je OpenVZ, které se skládá z upraveného linuxového jádra a userspace nástrojů. OpenVZ s sebou nese mnoho významných úprav jádra, které nebyly jako celek nikdy začleněny do oficiálního vanilla kernelu. Naštěstí se během let daří jednotlivé změny začleňovat nebo nahrazovat funkcionalitou, která se do jádra dostala nezávisle na OpenVZ. Tím se postupně eliminují nedostatky, kterých má OpenVZ stále ještě víc než dost.

Potenciálním konkurentem je zatím nepříliš funkční sada nástrojů LXC, které vznikly právě s příchodem implementacemi izolace různých prostředků operačního systému. Ale podle všeho nástroje OpenVZ stále více používají rozhraní vanilla jádra jako LXC. Oba nástroje tedy zatím konvergují k situaci, kdy budou fungovat jako pouhé frontendy k budoucí standardní funkcionalitě jádra.

Cloud computing: právní aspekty

Jan Kolouch

E-mail: jan.kolouch@atlas.cz, jan.kolouch@cesnet.cz

Úvod

Současný svět informačních a komunikačních technologií je ohrožován řadou hrozeb. Masivní rozvoj ICT a všechny benefity s ním spojené s sebou neodmyslitelně přináší i negativní aspekty, nejčastěji v podobě kyberkriminality, či zneužívání ICT. Asi největší „hrozbou“ současnosti jsou však uživatelé samotní, protože byť mají právní subjektivitu[1], tak mají jen minimální znalosti o svých právech a povinnostech.

Tento článek má objasnit některé, zejména právní aspekty spojené s Cloud computingem[2]. Faktem je, že výše uvedené negativní jevy, jako je kyberkriminalita, zneužívání Cloud computingu, či porušování povinností zakotvených ve smlouvě, ze strany uživatelů jsou spojeny s právní odpovědností za takové jednání.

Jednou z příčin rozmachu uvedených negativních jevů je mnohdy nejsané, neurčité, značně vágní vymezení práv a povinností uživatelů, stejně jako nedostatečné preventivní a represivní reakce ze strany poskytovatelů služeb[3] či států samotných. Otázky, které jsou obsaženy v abstraktu a hledání odpovědí na ně, bylo jedním z důvodů pro zpracování tohoto článku.

Definice Cloud computingu

Současná společnost je plně závislá na informačních sítích, zejména pak na internetu. Rychlost a zejména dostupnost přenášených dat se stává klíčovým elementem dnešní doby. Uživatel zpravidla nechce a ani nemá snahu zjišťovat, kudy a jakým způsobem dochází k přenosu dat, jím do informačních sítí vložených. Nezajímá ho ani, kde se nachází adresát přenášených dat, či kde jsou data uchovávána, tím dochází k **odhmotnění obsahu od fyzické struktury informačních sítí**.

[1] Mají práva a povinnosti. Uživatelé zakládají, mění a případně ruší právní vztahy.

[2] Dále také i **CComp**

[3] V ČR upravuje práva a povinnosti poskytovatelů služeb především zákon č. 480/2004 Sb., o některých službách informační společnosti, v platném znění (dále jen ZoSIS). Problematika práv a povinností poskytovatelů připojení je v ČR řešena především prostřednictvím zákona č. 127/2005 Sb., o elektronických komunikacích, v platném znění (dále jen ZoEK).

Na jednu stranu je možné sledovat situaci, kdy jsou **společenské vztahy na internetu jsou delokalizovány**[4], což s sebou přináší problémy z hlediska aplikace práva, avšak na stranu druhou tato delokalizace umožňuje uživatelům volně („svobodně“ a bez omezení v podobě hranic) zasílat, uchovávat, měnit data.

Cloud computing je jedním z fascinujících příkladů, na kterém je možné demonstrovat, jak nezájem o technické aspekty celého procesu přenášení a uchovávání dat, tak komplikace spojené s případným legálním získáním, uchováváním, či smazáním těchto dat[5].

Velké množství společností začalo v poslední době masivně využívat Cloud computingu[6], zejména z důvodu možnosti univerzální dostupnosti dat a služeb, jakož i z důvodu snížení nákladů nezbytných na pořízení a údržbu informačních technologií. Na tomto místě je vhodné připomenout, že Cloud computing není žádnou novou službou[7], jen došlo k jejímu masovějšímu využití, které je spojeno s rozmachem ICT.

Předtím než začnou být řešeny otázky spojené s právními aspekty Cloud computingu, je třeba vymezit Cloud computing jako takový. **Cloud computing** je termín užívaný pro systém umožňující užívání (sdílené) počítačových technologií (jak hardware, tak i software) více uživateli (prostřednictvím sítě) formou poskytované služby.[8] Smyslem Cloud computingu je efektivnější utilizace výpočetního výkonu a aplikací. Další možnou definicí Cloud computingu je, že jde o *„poskytování výpočetních služeb uživatelům, skrze síťovou architekturu,*

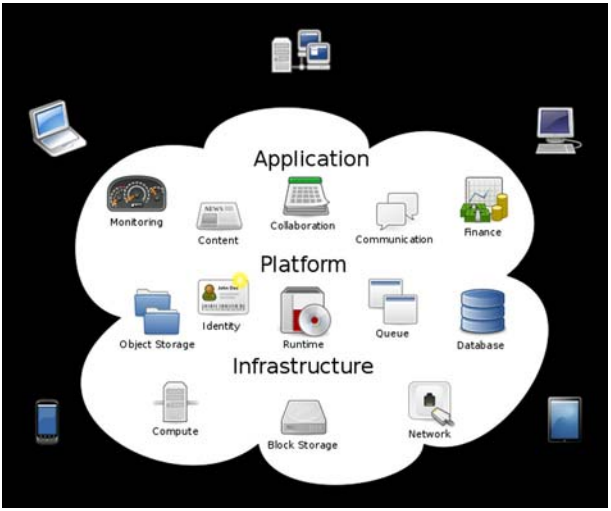
[4] *Delokalizace právních vztahů na internetu* [online]. [cit. 15. 4. 2012]. Dostupné z: http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/index.html

[5] Viz např. První dodatek k Ústavě Spojených Států Amerických: *„**Kongres** nesmí vydávat zákony zavádějící nějaké náboženství nebo zákony, které by zakazovaly svobodné vyznávání nějakého náboženství; právě tak **nesmí vydávat zákony omezující svobodu slova nebo tisku**, právo lidu pokojně se shromažďovat a právo podávat státním orgánům žádosti o nápravu křivd.“* (dostupné např. na: http://www.law.cornell.edu/constitution/first_amendment). Tento dodatek zaručuje právo na svobodu projevu v USA. Určitá jednání, zejména projevy názorů v podobě blogů a diskusí, která jsou na půdě USA pod ochranou tohoto dodatku, však mohou zakládat právní (zejména trestně právní) odpovědnost v jiných zemích světa. Běžně se pak stává, že dotčené subjekty (především **Law Enforcement Agencies** – dále jen **LEA**) požadují výmaz dat ze serverů umístěných v USA s tím, že obsah těchto dat, je v rozporu s právem jejich země. Odpovědí na takovéto žádosti zpravidla je, že umístěná data jsou v souladu s Prvním dodatkem Ústavy USA a proto vymazána nebudou.

[6] Respektive služby poskytovatele služeb informační společnosti, spočívající v ukládání informací poskytnutých uživatelem (tzv. storage nebo hosting). Tyto služby jsou regulovány Evropskou i národní úpravou – viz Článek 14, směrnice 2000/31/ES, či § 5 ZoSIS.

[7] Mezi CComp je možné zařadit i např.: **Web-based email systems** (např. Hotmail, či Yahoo!, které začaly poskytovat tyto služba na konci devadesátých let minulého století).

[8] *Cloud Computing Begins to Gain Traction on Wall Street* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.wallstreetandtech.com/it-infrastructure/212700913
Cloud computingem se rozumí poskytování služeb, programů (aplikací), prostoru pro ukládání (resp. meziukládání) dat, aj.



Obr. 1 Zobrazení Cloud computingu[10]

která umožňují vzdálený přístup k těmto službám. Tyto služby jsou zpravidla poskytovány třetí stranou.“[9]

V současnosti existuje velká řada modelů CComp, včetně různých způsobů poskytování služeb s CComp spojených. Co je však pro všechny typy CComp společné je schopnost poskytovat prostředky na vyžádání, pružně, samoobslužně a prostřednictvím přístupu ze sítě (nejčastěji Internetu). V rámci CComp je také možnost měřit spotřebované služby v rámci sdíleného fondu prostředků.

Cloud computing lze dělit z několika hledisek, přičemž nejběžněji je dělen podle služby kterou poskytuje a podle způsobu, jakým je poskytován. Uvedené dělení je nezbytné, alespoň rámcově vymezit, neboť toto vymezení je důležité z hlediska aplikovatelnosti práva. **Podle služby jakou Cloud computing poskytuje** je možné definovat tři hlavní typy služeb (distribuční modely)[11].

[9] *Security authorization. An Approach for Community Cloud Computing Environments* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.federalnewsradio.com/pdfs/SecurityAuthorizationandAssessmentSECURITYNov2009.pdf

[10] Zobrazení CComp. [online]. [cit. 15. 4. 2012]. Dostupné z: http://cs.wikipedia.org/wiki/Soubor:Cloud_computing.svg

[11] Mimo uvedené dělení je v CComp možné rozeznávat například služby:

- *Infrastrukturní*, jejichž účelem je zajistit splnění požadavků, které jsou zakotveny v dohodě, která stanovuje úroveň poskytovaných služeb [např. velikost úložného prostoru (kapacita), doba uchovávání dat, dostupnost služby, úroveň zabezpečení, aj.].
- Služby, které umožňují *funkčnost prostředí pro Cloud computing* (např. speciální účtovací software, který zajišťuje, aby v cloudových výpočetních prostředích různé velikosti a s různou úrovní poskytovaných služeb bylo možné vyúčtovat poskytnuté služby)

Jedná se o:

- **Infrastructure-as-a-Service (IaaS). Infrastruktura jako služba**[12] zavazuje poskytovatele poskytnout infrastrukturu (hardware) jiným uživatelům (typickým příkladem IaaS je vizualizace). V případech IaaS uživatel běžně platí za to, co využívá. Tento systém je také nazýván „utility computing“[13]. Typickými příklady IaaS jsou Amazon WS, Rackspace, Microsoft Azure, aj.[14]
- **Platform-as-a-Service (PaaS).** Platforma jako služba je také nazývána „**cloudware**“[15] a poskytuje uživateli „computing platform“ (v podobě jak hardwarové architektury, tak softwaru – v rámci této služby je možné kombinovat, modifikovat a vyvýjet software, respektive aplikace) a „solution stack“[16]. Jako příklady PaaS je možné uvést Google App Engine nebo Force.com.[17]
- **Software-as-a-Service (SaaS).** Software jako služba je vlastně způsobem poskytování aplikace uživateli. Aplikace je zpravidla licencována[18]

- *Konzultační*, které jsou nejčastěji poskytovány v souvislosti s přechodem na CComp, případně při odstraňování potíží s CComp.

[12] Z hlediska práva je otázkou, o jakou službu se v tomto případě jedná. V úvahu přichází několik možností:

1. Poskytování „připojení“ – v případě distribuce IP adres a poskytování připojení (pak by v ČR připadala v úvahu právní odpovědnost dle ZoEK).
2. Poskytování služeb spočívající v přenosu informací poskytnutých uživatelem (angl. Mere Conduit nebo Access Provider). De facto se jedná o:
   Operátory elektronických komunikací,
   ostatní operátory fyzických linek a
   – *operátory logických linek.*
3. Poskytování služeb spočívajících v automatickém meziukládání informací poskytnutých uživatelem (tzv. caching).
4. Poskytování „prostoru“ – storage, hosting (pak by v ČR připadala v úvahu právní odpovědnost dle ZoSIS).

Právní odpovědnost jednotlivých poskytovatelů služeb dle ZoSIS bude vymezena dále.

[13] Definice pojmu viz např.
http://searchdatacenter.techtarget.com/definition/utility-computing.

[14] http://aws.amazon.com/ (v případě využívání této služby jsou například uživatelům poskytovány unikátní IP adresy a datový prostor – on demand); http://www.rackspace.com/; http://www.microsoft.com/cze/azure/

[15] http://www.cloudwareinc.com/

[16] Součásti software, nebo komponenty, nezbytné pro chod zcela funkčních řešení (průduktů, nebo služeb). http://thecloudguytim.wordpress.com/2010/09/08/paas-solution-stacks-wins-lamp/

[17] https://developers.google.com/appengine/?hl=cs;
http://www.salesforce-crm.cz/?utm_source=adwords&utm_medium=cpc&_kk=salesforce&_kt=d73b6ddc-aa63-45b1-9133-371a0a6cc3b9

[18] V tomto případě se na ni budou vztahovat zákon č. 121/2000 Sb., zákon o právu autorském a právech souvisejících a právem autorským, v platném znění. Dále jen ZAP.

a uživatelé si tak „kupují“ přístup k aplikaci, nikoli aplikaci jako dílo. Příkladem jsou např. Google Apps.[19] Nejčastějšími příklady SaaS aplikací jsou: desktop as a service, business proces as a service, communication as a service, aj.

Podle způsobu, jakým je Cloud computing poskytován je možné rozeznat následující cloudy:

- **Veřejný cloud.** Tento typ cloudu je mnohdy označován jako klasický, model CComp. Jedná se o veřejně a volně přístupné služby[20], které jsou poskytovány neomezenému okruhu uživatelů. Tyto služby bývají volně dostupné z Internetu a typickými příklady jsou služby Free Mail, messenger, Office nebo Storage.

- **Privátní (soukromý) cloud** je typem cloudu, který je zpravidla vytvořen a provozován v rámci jedné firmy, či společnosti. Jde zpravidla o jednoúčelový, privátní cloud s externím poskytovatelem služeb. Takovýto cloud je zaměřen na plnění specifických požadavků firmy a poskytuje ICT služby dynamicky dle potřeb.

- **Hybridní cloud** je příkladem cloudu, kdy je infrastruktura cloudu sdílena několika firmami, společnostmi, skupinami jedinců, aj. V současnosti se jedná o nejběžnější formou cloud computingu.

Bezpečnost a hrozby Cloud computingu

Cloud computing v sobě přináší nesporné výhody, které se projevůjí zejména v oblasti finančích nákladů, které je nezbytně nutné vynaložit na efektivní fungování ICT. Na druhou stranu je však třeba zmínit i rizika a hrozby, které vyplývají ze samotné podstaty poskytování uvedené služby a které jsou mnohdy zcela bezostyšně přehlíženy.

Bez fyzické bezpečnosti není a nemůže být ani bezpečnost virtuální. *„Bez ohledu na to, jak virtuální a kyber a 2.0 je vaše infrastruktura, vždy má hluboké kořeny v reálném, fyzickém světě. Ovládnete-li fyzickou podstatu, ovládáte vše. Někdo teď možná namítne, že kryptografie mění pravidla hry, a na to budu muset kontrovat, že pravidla zůstávají beze změny, jen čáry na hřišti se posouvají. Šifrované informace jsou chráněny nanejvýš tak dobře, jak dobře jsou chráněny šifrovací klíče. Ty můžeme zašifrovat taky, a znovu a znovu, ale nakonec vždy skončíme s klíčem v otevřené podobě. A jelikož zatím neexistuje prakticky použitelná metoda, jak provádět užitečné operace na zašifrovaných datech, tak se*

[19] http://www.google.com/apps/intl/cs/business/index.html#utm_campaign = cs&utm_source = cs-ha-emea-cs-bk&utm_medium = ha&utm_term = %2Bgoogle%20%2Bapps

[20] Byť jsou ve většině případů upraveny a podmíněny souhlasem s licenčním ujednáním.

data zpracovávají vždy v otevřené podobě – oblak neoblak. Vzpomeňte si na to, až vám zase někdo bude nabízet, že vaše data v oblacích zabezpečí pomocí šifrování. Abych nebyl nespravedlivý, šifrování může zvýšit bezpečnost dat v oblaku. Otázkou je, o kolik?“[21]

V případě využívání CComp je třeba řešit otázky spojené zejména s **důvěrností**[22], **intergitou**[23] **a dostupností**[24] **dat uložených v Cloudu**.

Z hledika bezpečnosti je dále třeba řešit i otázku, k čemu má být cloud využit a jaká data by v něm měla být uložena. Zejména kritická a velmi citlivá data by měla zůstávat uložena mimo cloud nebo v privátním cloudu.

Mezi největší hrozby v rámci Cloud comutingu v současnosti patří[25]:

1. Zneužití, či „podlé“ využití CComp.
2. Nezabezpečené rozhraní a APIs.
3. Osoba „škodící“ nebo zneužívající služeb CComp.
4. Ztráta/únik dat.
5. Narušování přenosu dat či účtu.
6. Neznámý nebezpečný profil.
7. Větší zranitelnost sdílené technologie.

Právní úprava Cloud computingu

Internet, který de facto tvoří kyberprostor, je otevřený a snadno přístupný všem, ***„. . . neplatí zde žádné zvláštní zákony a je třeba se řídit obecně závaznými normami.“***[26]

[21] *Cloud computing: Bezpečnost v oblacích? Snad příště.* [online]. [cit. 15. 4. 2012]. Dostupné z: http://stipek.wordpress.com/2010/03/16/bezpecnost-v-oblaku-snad-priste/

[22] V momentě umístění dat do cloudu k nim samozřejmě získá přístup i cloud provider. Z hlediska statistik však bývají největší hrozbou osoby, které mají k datům přístup zenitř organizace.
Významnou otázkou však je co se stane s daty, pokud se rozhodnete cloud opustit (ukončíte smlouvu). Kdo zaručí, že budou Vaše data smazána?

[23] Data v cloudu mohou být smazána, či pozměněna neoprávněnou osobou, nebo v důsledku selhání HW či SW.

[24] Z hlediska dostupnosti je důležité, kde se nachází cloud provider, respektive, kde se nachází daný hardware. V případě zemětřesení spojeného s vlnou tsunami v Japonsku, či Thajsku, je pravděpodobné, že zařízení dislokovaná v těchto destinacích, jakož i cloudy na nich běžící nebudou dostupné po určitou dobu. Jako další příklady je možné zmínit DDoS útoky vedené proti Estonsku a Gruzii nebo DDoS útok na cloud botnetem Bredolab, který zahltil více než 700 000 uživatelů Facebooku, aj.

[25] *Top threats to Cloud Computing V1.0* [online]. [cit. 15. 4. 2012]. Dostupné z: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[26] SMEJKAL, V. *Internet a §§§*. 2. aktualiz. a rozš. vyd. Praha : Grada, 2001. s. 32.

Díky delokalizaci subjektů práva v různých zemích na celém světě je otázkou, jaký právní systém (jestli vůbec nějaký) se bude vztahovat na případné úkony (či protiprávní jednání) učiněné v Internetu.

Obecně je možné konstatovat, že **na kyberprostor a veškeré aplikace, jakož i další služby, je možné aplikovat standardní kriteria**[27], **která jsou uplatňována v návaznosti na skutečnou fyzickou lokalizaci dat či informací. Druhou možností je** vytvoření nových kriterií, pro aplikaci principu místní působnosti (jedná o **virtuální lokalizaci právních vztahů**).[28]

Na Cloud computing, respektive na jednotlivé elementy CComp je třeba aplikovat stávající právní úpravu.[29] Je otázkou, o jakou právní úpravu se v jednotlivých případech bude jednat, neboť CComp a služby s ním spojené jsou v drtivé většině případů poskytovány ze zahraničí a tudíž podléhají právu té které země.[30]

V poslední době je možné pozorovat výraznou snahu zejména EU, v oblasti CComp, jejímž cílem je rekodifikace zákonů sloužících k ochraně a ukládání dat. Současné zákony jsou v moderním pojetí ICT zastaralé a nemohou sloužit jako účinný nástroj na eliminaci problémů spojených s CComp.

Na problematiku CComp je zaměřen i akční plán Komise Digitální agenda pro Evropu.[31] Evropa by podle komisařky Neelie Kroes měla ke Cloud computingu přistupovat aktivněji. Zároveň tato komisařka vyzvala poskytovatele Cloud computingových služeb, aby dostatečně řešili ochranu údajů. V současnosti je připravována evropská strategie pro Cloud computing (Komise ji předloží v roce 2012) a je pracováno i na směrnici sloužící k ochraně údajů v CComp.

Problematice CComp se věnuje i **ENISA** (European Network and Information Security Agency), zejména ve zprávách: Cloud Computing Risk Assessment[32]; Security and Resilience in Governmental Clouds.[33]

---

[27] Z hlediska trestního práva je třeba například vyřešit otázku: *„Kde byl trestný čin spáchán?“* je třeba využít institutů uvedených v trestním zákoníku (zákon č. 40/2009 Sb., trestní zákoník, v platném znění – dale jen **trestní zákoník, nebo TZK**), neboť Česká republika se zavazuje stíhat trestné činy i tehdy, pokud se pachatel nacházel mimo území ČR. Ve vztahu ke kyberkriminalitě dojde především k využití **zásad teritoriality** (§ 4 odst. 1 TZK), **personality** (§ 6 TZK), **ochrany** (§ 7 odst. 1 TZK) **a univerzality** (§ 7 odst. 2 TZK).
U internetové trestné činnosti pak bude pro posouzení otázky, zda stíhat či nestíhat trestný čin, zpravidla rozhodujícím místem **místo, kde nastal účinek trestného činu**, neboť velmi často se jednání pachatele odehraje na území jiného státu, než na kterém nastal právě účinek.

[28] Blíže viz Reed, C. Internet Law. Cambridge : Cambridge University Press, 2004, str. 218.

[29] V tomto případě je možné využít i analogie ITC outsourcingu, neboť ten v sobě zahrnuje podobné aspekty jako CComp.

[30] Např. právo: Irské (Microsoft), USA – CA (Google), USA – WA (Amazon), aj.

[31] http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/199&format=HTML&aged=0&language=EN&guiLanguage=en

[32] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[33] http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/

Na právní úpravy Cloud computingu je třeba nahlížet ze dvou rovin a to z **roviny soukromoprávní a roviny veřejnoprávní**[34]. Z pohledu soukromoprávního se bude pozornost primárně zaměřena na vymezení smlouvy, respektive licence k využívání služeb cloud computingu. Z pohledu veřejnoprávního pak půjde zejména o ochranu osobních údajů[35], odpovědnost poskytovatelů služeb informační společnosti (dle ZoSIS), aplikovatelnost institutů trestního a správního práva, aj.

Soukromoprávní aspekty Cloud Computingu

V rovině soukromoprávní je třeba největší pozornost věnovat vymezení smlouvy (licence) k využívání služeb (aplikací) Cloud computingu. Licenční smlouva je alfou i omegou práv a povinností jak uživatele, tak poskytovatele CComp.

Jak již bylo uvedeno výše, CComp není novou službou, jen v současné době prochází masivním boomem. Velmi málo lidí si uvědomuje, že za několik posledních let bylo de facto „podepsáno“ několik desítek, či stovek milionů Cloud computingových smluv. Tyto smlouvy mají podobu licenčního ujednání, které uživatelé odsouhlasili (uzavřeli) s provozovateli např. freemailových schránek, game portálů, komunikačních aplikací, aj.[36]

Pokud se jedná o freemaily není nutné požadovat písemnou kopii licenčního ujednání[37], či řešit neshody s provozovatelem služby prostřednictvím žaloby u soudu (snad vyjma případů např. zásadního porušení licenčního ujednání, či porušení podmínek ochrany osobních údajů, stanovených ZOOU).

Pokud se ale jedná například o společnost, která v prostředí cloudu provozuje aplikaci důležitou pro její chod, je více než na místě, upravit smluvní podmínky mezi uživatelem a poskytovatelem služby písemně a pokud možno mít právo se podílet na tvorbě či modifikaci takovéto smlouvy. V případě CComp je důraz kladen na popis plnění, které uživatel očekává, rychlost a dosažitelnost takového plnění, než na fyzickou podstatu (hmatatelnou substanci). Uživatel si prostřednictvím smlouvy o službě v CComp nekupuje fyzickou věc (zboží), ale pouze službu. Pokud by se jednalo o koupi fyzické věci, bylo by možné využít institutů obsažených v obchodním zákoníku. V případě CComp tohoto institutu využít nelze a je proto třeba přesně a jasně vymezit práva a povinnosti jednotlivých stran (poskytovatel a uživatel) ve smlouvě.[38]

deliverables/security-and-resilience-in-governmental-clouds

[34] Některé veřejnoprávní aspekty budou řešeny v dalších částech tohoto článku.

[35] Zákon č. 101/2000 Sb., o ochraně osobních údajů, v platném znění. Dále jen ZOOU.

[36] V uvedených případech se jedná o službu SaaS.

[37] V souvislosti s freemailem je třeba věnovat pozornost i klauzuli umožňující jednostrannou modifikaci licence (zpravidla provedenou pouze poskytovatelem služby).

[38] Je nezbytné dbát na správné a jasné formulování smluvních práv a závazků, protože je značný rozdíl mezi povinností a snahou. Např. formulace: *„poskytovatel je povinen zajistit, že aplikace bude zákazníkovi dostupná 95 procent provozní doby poskytování služby“* a její

Dalším významným aspektem CComp spojeným s licenční smlouvou je možnost změny rozsahu poskytovaných služeb. Tato flexibilita je pro uživatele na jednu stranu výhodou, ale zároveň se může stát i jeho zhoubou.[39] Z hlediska bezpečnosti je v tomto případě naprosto nezbytné stanovit jasné a předem vymezené procesy a pravidla, které definují jak poskytování služeb (jejich změnu – change management či demand management), tak proces přidělování uživatelských práv (včetně přístupu k informacím).

Kritickým bezpečnostním prvkem v případě využívání CComp je minimální, či nulová schopnost uživatele kontrolovat fyzické umístění dat.[40] Pokud je to možné, je vhodné do smlouvy včlenit některé z následujících ustanovení:

- Právo být neprodleně informován o výpadcích služby.
- Právo mít přístup k systémovým informacím a logům, ze kterých je možné zjistit aktuální lokaci vlastních dat a přístupů k nim.
- Právo provést (provádět) penetrační test – za účelem ověření zabezpečení ICT poskytovatele.
- Právo žádat provedení bezpečnostního auditu ICT poskytovatele CComp.
- Právo obdržet kopi bezpečnostního auditu.
- Vyžadovat certifikaci ISO (např. 27001 či 22307).[41]

(zdánlivě vhodnější) *alternativu „poskytovatel vyvine maximální úsilí k tomu, aby zákazník mohl aplikaci užívat 99,95 procenta provozní doby poskytování služby“*. V druhém případě sice poskytovatel deklaruje vyšší dostupnost, ale zákazník se svého práva na takovou dostupnost nemusí vždy domoci, protože poskytovatel sice vyvinul maximální úsilí, ale ono to zkrátka nestačilo. Obdobný příklad se týká samotného parametru *„dostupnost služby“*, kdy může být lákavé mít smluvní závazek dostupnosti 99,95 procenta, ale pokud je dostupnost služby měřena za období jednoho roku, může být výpadek znatelně delší než v případě, kdy je dostupnost měřena na obvyklejší měsíční bázi.
Blíže viz *Právní aspekty cloud computing* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.systemonline.cz/clanky/pravni-aspekty-cloud-computingu.htm

[39] V praxi může nastat případ, kdy jsou služby CComp poskytovány společnosti (firmě), včetně možnosti jejich změn, bez pevných pravidel pro realizaci změn. Zaměstnanec firmy nastaví („odkliká“) v administrátorském rozhraní výrazně vyšší počet služeb než firma ve skutečnosti potřebuje. Tyto služby jsou okamžitě poskytnuty uživateli a je vyžadováno finanční plnění za jejich poskytnutí. Reklamace čerpání takové služby je více než obtížná.
Právní odpovědnost „aktivního, hloupého, či ve zlém úmyslu jednajícího zamestnance“ je značně různorodá. Může jít o potrestání v rámci pracovního práva, občansko právní spor, či může dojít k zahájení trestního řízení vůči této osobě.

[40] Což v sobě nese i aspekt určité omezenosti ochrany těchto dat před neoprávněným přístupem ze strany uživatele.

[41] Blíže viz *Právní aspekty cloud computing* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.systemonline.cz/clanky/pravni-aspekty-cloud-computingu.htm.

Veřejnoprávní aspekty Cloud computingu

Odpovědnost poskytovatelů služeb informační společnosti

Při řešení případné odpovědnosti poskytovatele CComp je třeba primárně vycházet z vymezení druhu poskytované služby (IaaS, PaaS, SaaS) a tyto pak subsumovat pod ustanovení zákona o některých službách informační společnosti.

V případě odpovědnosti poskytovatelů služeb informační společnosti nebube pozornost věnována již charakterizovaným licencím[42], ale případné odpovědnosti za ukládaná a přenášená data.

„Obecně platí zásada, že je-li informace protiprávní a ISP neměl ani povědomosti o jejím vytvoření či komunikaci, je ISP zbaven odpovědnosti ze zákona.“ [43]

1. **Poskytovatelé služeb spočívajících v přenosu informací poskytnutých uživatelem.**

   Tyto poskytovatele nelze činit odpovědné za kvalitu informace (kterou mu nelze přičíst), a to i v případě, že si je vědom protiprávnosti přenášené informace.[44] Zvláštní požadavky a podmínky jsou však stanoveny vůči operátorům služeb elektronických komunikací. Tyto podmínky stanoví ZoEK. Ustanovení čl. 12 směrnice č. 2000/31/ES umožňuje členským státům nařídit Poskytovateli, aby přerušil poskytování služeb, skrze něž dochází k přenosu informací, jež neoprávněně zasahují do práv jiného. Tato možnost je jedním z prostředků, jak zabránit protiprávnímu jednání. Příkaz k přerušení poskytování služeb zpravidla vydává soud.

2. **Poskytovatelé služeb spočívajících v automatickém meziukládání informací poskytnutých uživatelem (tzv. caching).**

   Tito Poskytovatelé **nejsou** zbaveni odpovědnosti za kvalitu informací, pokud dojde z jejich strany k porušení standardních či smluvených technických podmínek cachingu.[45]

3. **Poskytovatele služeb spočívajících v ukládání informací poskytnutých uživatelem (tzv. storage nebo hosting).**

[42] **Ve všech dále popsaných případech se předpokládá, že bude uzavřena SLA (Service Level Agreement), či EULA (End User Licence Agreement) mezi poskytovatelem služby a uživatelem.**

[43] POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* 1. vyd. Brno : Computer Press, 2007. s. 55.

[44] Srov. čl. 12 směrnice č. 2000/31/ES a ust. § 3 odst. 1, 2 ZoSIS

[45] Srov. čl. 13 směrnice č. 2000/31/ES a ust. § 4 ZoSIS
Srov. POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* 1. vyd. Brno : Computer Press, 2007. s. 58.

Zde je situace s odpovědností nejsložitější.[46] Opět se vychází z ustanovení směrnice č. 2000/31/ES, jejíž doporučení přejal český zákonodárce do § 5 ZoSIS. V tomto ustanovení je dána podmínka alespoň nevědomé nedbalosti[47] poskytovatele ve vztahu k protiprávnímu obsahu informace u něj uložené. **Zákonodárce** však **neukládá Poskytovatelům povinnost aktivně vyhledávat protiprávní informace uživatelů**[48] (neboť by v mnohých případech šlo de facto o zásah do základních práv a svobod zaručených LZPS – např. čl. 13[49]).

V případě nemožnosti uplatnění norem veřejného práva, lze vůči poskytovatelům připojení či služeb uplatnit normy soukromoprávní.[50] Půjde zejména o § **415 ObčZ**[51], který stanoví, že **každý by se měl chovat tak, aby nedocházelo k porušování práv jiných** (každý je povinen počínat si tak, aby nedocházelo ke škodám na zdraví, na majetku, na přírodě a životním prostředí.) **a k případným újmám na jejich právech**. Dále je možné užít i § **420 ObčZ**, který stanoví, že *„každý odpovídá za škodu, kterou způsobil porušením právní povinnosti.“*[52] Pokud je tedy kterýkoli z poskytovatelů upozorněn na protiprávní jednání v rámci služby, kterou poskytuje, měl by učinit vše, aby zabránil dalšímu protiprávnímu jednání.

[46] Srov. čl. 14 směrnice č. 2000/31/ES a ust. § 5 ZoSIS
Poskytovatelé storage služeb dávají svým uživatelům prostor k uložení dat. Tento prostor je poskytován **na základě smlouvy o uložení informací či dat**. Je otázkou, zda je rozumné a proveditelné požadovat od těchto poskytovatelů, aby u všech uložených informací zjišťovali a posuzovali jejich obsah a jejich legálnost či nelegálnost.
Poskytovatel storage služby, odpovídá za obsah informací uložených na žádost uživatele jen tehdy, pokud mohl vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, anebo dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.
Poskytovatel storage služeb je dále plně odpovědný za obsah uložených informací, pokud vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele.

[47] Srov. ust. § 16 odst. 1 písm. b) TZK. Podle práva ČR je poskytovatel storage služeb odpovědný v i případě, kdy o protiprávním charakteru informace nevěděl, ač vzhledem k okolnostem a k svým osobním poměrům vědět měl a mohl. Podle českého práva stačí prokazatelná možnost, dozvědět se o protiprávním charakteru informace.

[48] Srov. čl. 15 směrnice č. 2000/31/ES a ust. § 6 zák. č. 480/2004 Sb.

[49] ***Nikdo nesmí porušit*** *listovní* ***tajemství*** *ani tajemství jiných písemností a* ***záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem****, s výjimkou případů a způsobem, které stanoví zákon.* ***Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.***

[50] V soukromoprávní oblasti srov. např. nařízení Evropského parlamentu a rady **(ES) č. 593/2008 – Řím I**.

[51] Zákon č. 40/1964 Sb., občanský zákoník, v platném znění. Dále jen **ObčZ**.

[52] § **420 odst. 3 ObčZ** stanoví, že **odpovědnosti se zprostí ten, kdo prokáže, že škodu nezavinil**.

Lokace dat v Cloudu a práva k nim

Z právního hlediska je významné zjištění místa ukládání a zpracování dat v CComp. Bohužel v praxi je velmi problematické zjistit, jaké aplikace a jaká data se v daný okamžik nachází na tom kterém serveru. Z hlediska nepřetržité funkčnosti CComp jsou data duplikována a dislokována na několika serverech, v různých destinacích, najednou. Benefitem tohoto přístupu bezesporu je větší záruka zachování dat při výpadku, poškození nebo zničení jednoho z center.

Z tohoto pohledu nemá uživatel možnost kontrolovat fyzické umístění dat.[53] Odlišná situace nastává zpravidla v soukromých cloudech, kde má uživatel (zpravidla na základě smlouvy) možnost kontrolovat a monitorovat operace s daty.

Samostatnou pozornost pak vzbuzuje otázka smazání dat, pokud se uživatel rozhodne, že přestane využívat služby CComp. Uživatel je oprávněn se dovolávat licenční smlouvy, ve které je zpravidla zakotvena i klauzule o ukončení poskytování služby výpovědí, Je však otázkou, zda dojde po takovémto ukončení smlouvy skutečně k fyzickému zničení (ať přesouvaných, nebo mazaných) dat. V případě veřejného Cloudu, se tak nelze než spolehnout na „poctivost“ poskytovatele služby.[54]

Pokud jde o aplikovatelnost práva, bude zpravidla využit princip teritoriality, který je uplatňován v návaznosti na skutečnou fyzickou lokalizaci dat či informací.

Povaha ukládaných dat, aneb Cloud a krávy

Jedním z významných problémů spojených s CComp je i povaha ukládaných a spravovaných dat[55]. Evropská unie stanovila přísná omezení pro informace, která smějí být o jejích občanech ukládána a to včetně stanovení doby ukládání. Obdobná situace pak vyvstává i v případě finančního sektoru[56], zdravotní péče[57], aj.

[53] Toto tvrzení není doktrínou, neboť např. Společnost Google například dovoluje zákazníkům určit, kde jsou uložena data aplikací Google Apps, díky Postini:
http://www.google.com/postini/

[54] Většina poskytovatelů CComp nemá v současnosti vytvořeny postupy a metodiky pro takové operace, zejména pokud se jedná o „malého“ uživatele.

[55] Právní regulace a ochrana osobních údajů je značně odlišná i v jednotlivých zemích EU, natož v celosvětovém měřítku.

[56] Vlaná většina bankovních institucí (byť se jedná o nadnárodní korporace) vyžaduje, aby data klientů byla dislokována v zemi původu, či pobytu klienta.

[57] Např. Belgická společnost zabývající se asistovaným způsobem života a E-healt, není oprávněna uchovávat ve svých cloudech data o pacientech či zdravotních úkonech (i když nejsou spojeny s konkrétní osobou) z jiných zemí, byť je tato aplikace využívána jako součást mezinárodního projektu EU.

Na tomto místě bych rád uvedl jeden absurdní příklad, který demonstruje obstrukce, které mohou nastat, pokud mají ukládaná data „citlivou povahu“ a pokud jsou ukládána na cloud umístěný v zahraničí.

Cloud a krávy je případ, kdy ochrana osobních dat nesmyslně zasáhla do efektivního využívání CComp. Lucemburské právo vloni vytvořilo překážku, pro kterou nemohl Holandský podnikatel Remi Caron využít aplikaci, která měla pravidelně odesílat „zdravotní data“ o jím chovaných kravách (v Holandsku) do cloudu (v Lucembursku). Jakkoli prospěšná, efektivní a přínosná daná aplikace byla[58], porušovala Data Protection Directive, neboť odesílala „osobní údaje“ do cloudu, který byl umístěn v jiné zemi, než ve které se nacházely „subjekty“ jichž se dané informace týkaly.[59]

Za jakých podmínek je možné k datům získat přístup

Garance nezasahováni do dat neoprávněnými osobami

Využívání cloudových služeb s sebou přináší značnou redukci významného bezpečnostního prvku v podobě ochrany dat ze strany uživatele samotného. Uživatel má minimální možností, jak zabránit jiným subjektům, ve fyzickém přístupu ke svým datům. V CComp je odpovědnost za ochranu vložených dat přenesena na poskytovatele CComp služeb a v případě porušení jejich povinností při správě vložených dat je možné aplikovat jak instituty soukromého, tak veřejného práva.

Je třeba mít na paměti možnost, že i přes všechny prvky ochrany dat v cloudu, které budou zabraňovat nelegálnímu přístupu k datům prostřednictvím Internetu, může v extrémním případě dojít k odcizení dat ve světě reálném (v podobě krádeže, či poškození fyzické infrastruktury cloudu).

Možnost získaní dat pro oprávněné subjekty (LEA)

Významným právním předpisem, který se snaží sjednotit právní úpravu v kyberprostoru z hlediska LEA, je Convention on Cybercrime[60]. Tato úmluva v sobě

[58] Docházelo k monitoringu základních životních funkcí krav, včetně určení pozice, prostřednictvím senzorů umístěných v obojku.

[59] Blíže viz *Cloud computing hampered by cow data protection.* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.euractiv.com/specialreport-cloud-computing/cloud-adoption-hampered-cow-data-protection-news-509135

[60] Úmluva Rady Evropy o kyberkriminalitě č. 185 (Convention on Cybercrime) Dále jen Úmluva nebo CCC. Tato úmluva byla otevřena k podpisu 23. 11. 2001 v Budapešti. The Convention is intended to be the „first international treaty on crimes committed via the Internet and other computer networks.“
Its provisions particularly deal with infringements of copyrights, computer-related fraud, child pornography, and **violations of network security**.

mimo jiné zahrnuje i možnosti získání informací z CComp. Úplná implementace Úmluvy o kyberkriminalitě, je v případě zisku dat z cloudů, důležitější než cokoli jiného. LEA jsou oprávněni získat data z cloudů pouze v mezích zmocnění právních norem té které země.

Celou oblast přístupu k datům z pohledu LEA je možné rozdělit do tří podsekcí:

1. **Přístup k datům v rámci jursdikce LEA** (LEA má právo vyhledat, shromáždit a zajistit důkazy v elektronické podobě – **čl. 14 Úmluvy**).

2. **Data v cloudu jsou umístěna v zahraničí** (LEA – má možnost požádat o pomoc LEA v zemi ve které se nacházejí servery cloudu – **čl. 31 Úmluvy**).

3. **Přímý přístup k informacím uloženým v zahraničí** [přeshraniční přístup k datům uloženým v zahraničí bez kontaktování příslušných zahraničních autorit (LEA), nebo ISP. Typicky se jedná o veřejně přístupná data. V tomto případě může LEA využít **čl. 32b), nebo čl. 19 odst. 2 Úmluvy**].

4. **Přístup k datům na základě spolupráce s ISP nebo poskytovateli služeb CComp.**

V ČR mohou orgány činné v trestním řízení využít k zajištění informací z cloudu zejména ustanovení § 8 odst. 1, § 78, 79, 88 a 88a trestního řádu.[61]

Závěr

Cloud computing je jev, který je v současnosti na vrcholu „hype cycle“ křivky[62]. V budoucnosti má tedy Cloud computing čekat strmý pád a následně vstup do fáze produktivního užívání.[63]

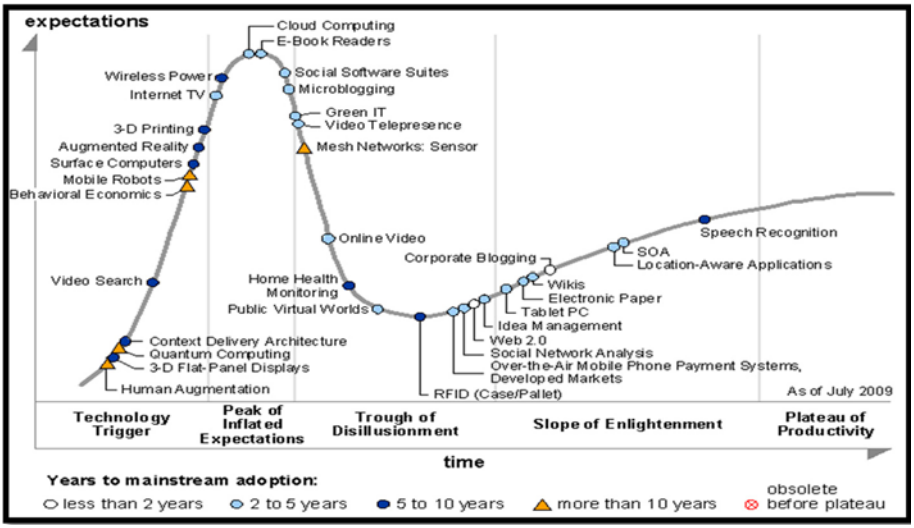
Je otázkou, do jaké míry je možné s tímto tvrzením souhlasit. Jak již bylo uvedeno, Cloud computing není novou službou, jedná se o službu, ketá prochází evolucí. Neboť např. *„pronájem strojového času je znám od vzniku počítačů, systémy klient – server jsou také dlouho známy, virtualizace byly možné již za dob mainframů, atd.“* [64] Cloud jako takový je možné vnímat jako jakousi supersložbu

[61] Zákon č. 141/1961 Sb., trestní řád, v platném znění. Dále jen trestní řád.

[62] Viz obrázek 2.

[63] Blíže viz *Cloud computing: Bezpečnost v cloudu a rizika* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.cleverandsmart.cz/cloud-computing-bezpecnost-v-cloudu-a-rizika/

[64] http://informaticke-praxe.tul.cz/?ident = 49&action. . .presenter = Action



Obr. 2 Cloud Computing HypeCycle

(čili stav, kdy je „vše“ poskytováno jako služba)[65]. **V tomto kontextu je pak možné téměř celý Internet označit jako Cloud.**

Pokud akceptujeme tuto úvahu, pak je více než zarážející, že oblasti legislativy a vynutitelnosti práva je věnována žalostně malá pozornost. Do budoucna je dle mého názoru potřeba plně implementovat Úmluvu o kyberkriminalitě nejen do českého právního řádu, ale do právních řádů vyspělých zemí.

Významnou podmínkou při sjednocování práva jednotlivých zemí je i jasné a deklarování toho, jaké právo bude za předem daných okolností využito. Tímto krokem dojde i k posílení právní jistoty uživatele.

Dalším nezbytným krokem je pak preventivní a výuková činnost, která by zvýšila právní podvědomí společnosti o právní odpovědnosti za jednání uskutečněné v kyberprostoru. Uživatel by si měl být vědom toho, že odsouhlasením licenčního ujednání došlo k vytvoření právního vztahu mezi ním a poskytovatelem služby. Proto by se měl maximálně zasadit o to, aby uvedená licence co nejvíce vyhovovala jeho požadavkům. Licence sama o sobě není schopna zabránit narušení, či zcizení dat, ale je schopna vytvořit kvalitní základ pro využívání služeb CComp bez výraznějších komplikací.

[65] Rimal at all (2011) Rimal B., P., Jukan, A., Kastros, D. and Goeleven, Y., Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. *Journal of Grid Computing* Volume 9, No. 1/2011, pp. 3–26. ISSN 1570-7873 (Print), 1572-9184 (Online)

Pokud jde o bezpečnostní aspekty Cloud computingu, pak je na místě zmínit dvě přísloví, která z mého pohledu naprosto přesně defnují Cloud computing a sním spojené služby.

„Důvěřuj, ale prověřuj.“
a
„Přežije jen paranoik.“[66]

Literatura

[1] Zákon č. 40/1964 Sb., občanský zákoník, v platném znění.

[2] Zákon č. 480/2004 Sb., o některých službách informační společnosti, v platném znění.

[3] Zákon č. 127/2005 Sb., o elektronických komunikacích, v platném znění.

[4] Zákon č. 121/2000 Sb., zákon o právu autorském a právech souvisejících a právem autorským, v platném znění.

[5] Zákon č. 101/2000 Sb., o ochraně osobních údajů, v platném znění.

[6] Zákon č. 141/1961 Sb., trestní řád, v platném znění.

[7] Směrnice 2000/31/ES.

[8] Úmluva Rady Evropy o kyberkriminalitě č. 185 (Convention on Cybercrime).

[9] *Cloud a bezpečnost* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.zive.cz/clanky/cloud-a-bezpecnost/sc-3-a-159557/default.aspx

[10] *Cloud Computing Begins to Gain Traction on Wall Street* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.wallstreetandtech.com/it-infrastructure/212700913

[11] *Cloud computing hampered by cow data protection* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.euractiv.com/specialreport-cloud-computing/cloud-adoption-hampered-cow-data-protection-news-509135

[12] *Cloud computing: Bezpečnost v oblacích? Snad příště.* [online]. [cit. 15. 4. 2012]. Dostupné z: http://stipek.wordpress.com/2010/03/16/bezpecnost-v-oblaku-snad-priste/

[66] Andrew S. Growe

[13] *Cloud computing: Bezpečnost v cloudu a rizika* [online]. [cit. 15. 4. 2012]. Dostupné z:
http://www.cleverandsmart.cz/cloud-computing-bezpecnost-v-cloudu-a-rizika/

[14] *Cloud computing: Proč se ho nemusíte obávat?* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.cicar.cz/article/show-article/
cloud-computing-proc-se-ho-nemusite-obavat

[15] Delokalizace právních vztahů na internetu [online]. [cit. 15. 4. 2012]. Dostupné z:
http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/index.html

[16] http://aws.amazon.com/

[17] http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/
199&format=HTML&aged=0&language=EN&guiLanguage=en

[18] http://searchdatacenter.techtarget.com/definition/utility-computing

[19] http://thecloudguytim.wordpress.com/2010/09/08/
paas-solution-stacks-wins-lamp/

[20] http://www.cloudwareinc.com/

[21] http://www.enisa.europa.eu/activities/risk-management/
emerging-and-future-risk/deliverables/
security-and-resilience-in-governmental-clouds

[22] http://www.enisa.europa.eu/activities/risk-management/files/
deliverables/cloud-computing-risk-assessment

[23] http://www.google.com/apps/intl/cs/business/index.html#utm_campaign=
cs&utm_source=cs-ha-emea-cs-bk&utm_medium=
ha&utm_term=%2Bgoogle%20%2Bapps

[24] http://www.google.com/postini/

[25] http://www.law.cornell.edu/constitution/first_amendment

[26] http://www.microsoft.com/cze/azure/

[27] http://www.rackspace.com/

[28] http://www.salesforce-crm.cz/?utm_source=adwords&utm_medium=
cpc&_kk=salesforce&_kt=d73b6ddc-aa63-45b1-9133-371a0a6cc3b9

[29] https://developers.google.com/appengine/?hl=cs

[30] http://informaticke-praxe.tul.cz/?ident=49&action...presenter=Action

[31] *Právní aspekty cloud computing* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.systemonline.cz/clanky/pravni-aspekty-cloud-computingu.htm

[32] *Security authorization. An Approach for Community Cloud Computing Environments* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.federalnewsradio.com/pdfs/SecurityAuthorizationandAssessmentSECURITYNov2009.pdf

[33] *Top threats to Cloud Computing V1.0* [online]. [cit. 15. 4. 2012]. Dostupné z: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[34] *Zobrazení Cloud computingu* [online]. [cit. 15. 4. 2012]. Dostupné z: http://cs.wikipedia.org/wiki/Soubor:Cloud_computing.svg

[35] SMEJKAL, V.: *Internet a §§§*. 2. aktualizované a rozšířené vydání. Praha : Grada Publishing, 2001. 283 s. ISBN 80-247-0058-1.

[36] POLČÁK, R.: *Právo na internetu. Spam a odpovědnost ISP.* 1. vyd. Brno : Computer Press, 2007. 150 s. ISBN 978-80-251-1777-4.

[37] Rimal, at all (2011) Rimal, B. P.,Jukan, A., Kastros, D., Goeleven, Y.: Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. *Journal of Grid Computing*, Volume 9, No. 1/2011, pp. 3–26. ISSN 1570-7873 (Print), 1572-9184 (Online).

Robotické operace

Jan Schraml

E-mail: jan.schraml@mnul.cz

Abstrakt

Díky rozvoji moderních technologií, které byly zavedeny do miniinvazivního operování, jsme my operatéři mohli odložit „bílou slepeckou hůl“. Nyní navíc díky možnostem i přenosu tohoto obrazu v 3D HD kvalitě se v reálném čase můžeme podílet na edukaci napříč světovými kontinenty. Takto je možné výrazně posunout hranice nejen edukačních možností.

Autor příspěvek nedodal.

Monitorovací systém Icinga/Nagios

Miloš Wimmer

E-mail: wimmer@cesnet.cz

Nagios je svobodný softwarový produkt určený pro automatizované sledování téměř jakýchkoliv veličin a stavů služeb a zařízení, která jsou nějakým způsobem dostupná přes počítačovou síť. Při zjištění nedostupnosti sledovaného stroje nebo služby anebo při překročení limitu měřené hodnoty dokáže systém informovat odpovědnou osobu e-mailem nebo SMS, případně může vyvolat i jinou akci.

Historii zjištěných stavů a naměřených hodnot poskytuje ve formě logů a grafů. Nagios je primárně vyvíjen pro Linux a je vydáván pod GPL licencí. Je součástí všech hlavních linuxových distribucí.

Netsaint, Nagios, Icinga, ...

Systém Nagios je nástupcem původního systému Netsaint. NAGIOS je akronym slovního spojení *„Nagios Ain't Gonna Insist On Sainthood“* – *„Nagios není připravený stát se svatým“*. Nagios si získal oblibu u řady techniků zabývajících se monitorováním síťové infrastruktury a síťových služeb. Ačkoli se na jeho vývoji a na vývoji pluginů, bez kterých by své popularity nedosáhl, podílí široká komunita, jeho jádro zůstává pevně v rukách hlavního vývojáře. Ten se postupem času rozhodl vydávat i placenou komerční verzi Nagios XI a přestal mít zájem o aplikování úprav rozšiřujících vlastnosti svobodné verze, přestože je do ní v podobě patchů zasílali vývojáři z komunity. Nespokojenost komunity s uzavřením vývoje vyústila v roce 2009 k rozhodnutí vytvořit odnož (fork) Nagiosu. Pro nový projekt bylo vybráno jméno Icinga, které v jazyce Zulu znamená *„podívat se kolem“* nebo *„hledat“*.

Icinga je řízena jako otevřený projekt, má několik hlavních vývojářů, přijímá úpravy z komunity a zveřejňuje časový i obsahový plán vydávání nových verzí. Do Icingy byla implementována řada funkcí, které byly do té doby dostupné jen v Nagios XI a navíc řada zcela nových vlastností. Vylepšení doznala i implementace jádra celého systému. Její vývoj je rychlejší, než u Nagiosu.

Icinga nezměnila filozofii fungování systému. V jejím prostředí lze proto využívat všechny pluginy, které byly v minulosti vytvořeny pro Nagios. Nezměnil se

ani způsob konfigurace, takže uživatelé Nagiosu mají umožněn bezproblémový přechod.

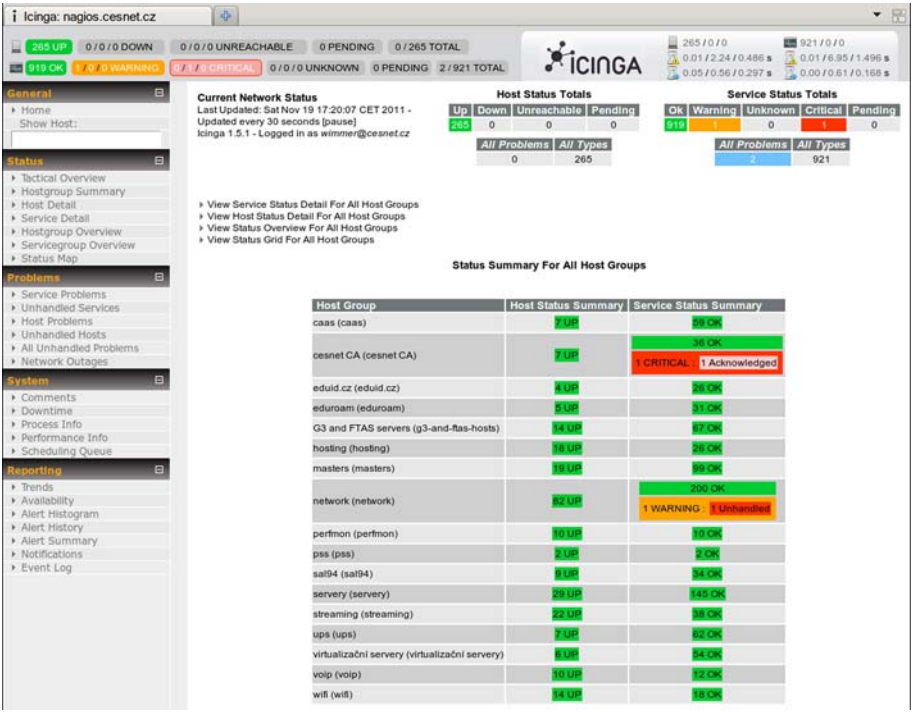
Já osobně preferuji systém Icinga před Nagiosem. V následujícím textu budu popisovat funkci a prostředí Icingy, většinou platí totéž i pro systém Nagios. Jméno Nagios se vžilo i jako obecné označení pro tento typ monitorovací služby.

Základní funkce a principy

Základní funkcí monitorovacího systému Icinga je sledování určených zařízení/hostů a služeb a posílání upozornění kontaktním osobám, dojde-li ke změně jejich stavu anebo ke změně sledované hodnoty mimo stanovené meze.

Icinga může provádět:

- sledování síťové dostupnosti hostů
- sledování síťových služeb (HTTP, SMTP, IMAP, POP3, FTP, NNTP, ...)
- sledování stavu zařízení (servery, stanice, aktivní prvky, tiskárny, UPS, ...)
- sledování stavu operačních systémů (Linux, Windows, ...)
- sledování aplikací (Apache, Exhange, JBOSS, SAP, ...)
- vytváření souhrnného pohledu v prostředí webu na stav všech sledovaných objektů
- zpřístupnění pohledu do historie sledovaných objektů (logy, grafy)
- vytváření trendů a reportů o dostupnosti (SLA)
- generování upozornění o změně stavu sledovaného objektu pro jeho správce a dohledovou službu (e-mail, SMS, RSS, Jabber), případně jejich eskalace
- zápis komentářů k jednotlivým hostům a službám v prostředí webu
- provázání s dokumentačními weby (informace o umístění na sále, odkazy na správce, odkazy na návody s postupy pro operátory, ...)
- vytváření agregovaných stavů dílčích služeb – tzv. Business Process View
- integraci s RT systémem
- apod.



Obr. 1: Rozhraní „Icinga classic web interface“

Monitorovací systém Icinga může přímo sledovat řádově tisíce hostů a služeb, při využití distribuovaného monitorování může jít až o stovky tisíc objektů. Lze jej využít pro odhalení různých anomálií v chování infrastruktury i k efektivnímu plánování jejího dalšího rozvoje.

Icinga se skládá ze třech základních komponent – jádra, API a webového rozhraní.

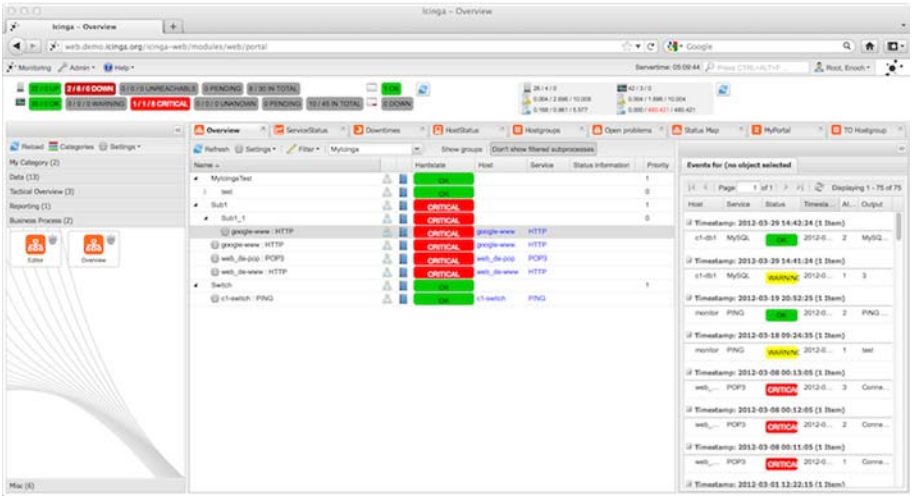
Jádro systému řídí plánování provádění jednotlivých kontrol sledovaných objektů, přijímá a zpracovává výsledky kontrol a v závislosti na zjištěných hodnotách spouští akce pro upozornění odpovědných osob. Vlastní kontroly sledovaných objektů jádro neprovádí – k tomu volá pluginy. To mohou být malé kousky kódu, které se pokouší kontaktovat přes počítačovou síť sledovaný objekt a zjišťují jeho stav. Výsledky svého měření pak poskytují jádru Icingy. V otevřenosti a v jednoduchosti rozhraní mezi jádrem a pluginem spočívá jeden z důvodů značného rozšíření služby Nagios. Administrátor této služby může využívat ohromného množství již vytvořených pluginů, které jsou volně dostupné v repozitářích Nagiosu a Icingy. K dispozici jsou pluginy pro všechny běžně používané síťové

služby i pro zjišťování stavu interních zdrojů serverů a aktivních prvků. Navíc v případě potřeby si může administrátor poměrně jednoduchým způsobem vytvořit svůj vlastní plugin.

Jádro Icingy napsané v jazyku C běží v operačním systému jako démon. Hodnoty získané od volaných pluginů ukládá do lokálních struktur v paměti a na disku, případně do relačních databází.

Komponenta API se používá jako vrstva umožňující webovému rozhraní a dalším rozšířením (např. subsystémům grafů) komunikaci s jádrem.

Icinga poskytuje dvě webová rozhraní. Původní web označovaný jako „Icinga classic web interface“ je součástí jádra. Je založen na technologii CGI. Nový „Icinga Web“ je založen na moderních dynamických technologiích a uživatelům dává možnost značné konfigurovatelnosti prostředí (dashboard). Mezi uživateli Icingy existují dva poměrně početné tábory, které preferují jeden druh webového rozhraní a odmítají druhý. Proto Icinga obsahuje obě rozhraní a volbu použitého nechává na vůli administrátora.



Obr. 2: Dynamické rozhraní „Icinga Web“

Plugin

Plugin je program nebo skript, který je volaný jádrem Icingy a který vykonává vlastní kontrolu jednotlivého hosta nebo služby. Plugin může v sobě volat jiný program obecného použití (např. ping, wget). Podstatné je, aby podle výsledku provedeného testu poskytoval návratový kód v hodnotách 0, 1, 2 nebo 3, které odpovídají následujícím stavům:

0 = OK Test provedený pluginem byl úspěšně proveden a zjištěná hodnota se pohybuje v mezích určených pro stav OK.

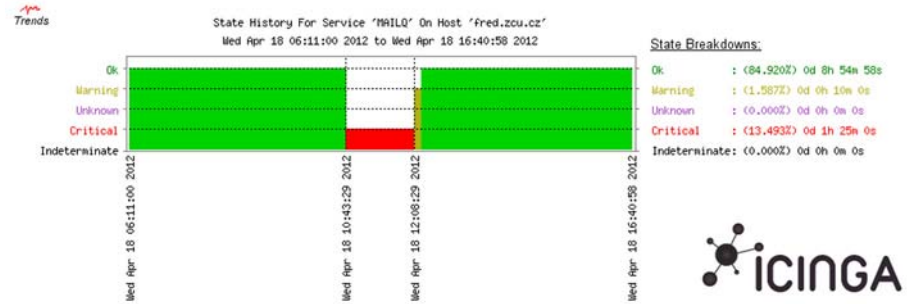
1 = Warning Test provedený pluginem byl úspěšně proveden, ale zjištěná hodnota se dostala do mezí určených pro stav Warning.

2 = Critical Test provedený pluginem nebyl proveden úspěšně anebo se zjištěná hodnota dostala do mezí určených pro stav Critical.

3 = Unknown Test nemohl být proveden anebo došlo k neznámé chybě.

Kromě návratového kódu může plugin na svůj výstup vypisovat textovou informaci včetně získaných hodnot. Tato informace je pak u dané služby dostupná v prostředí Icingy, může se přenášet do upozornění zasílaných příslušným osobám a může sloužit ke generování grafů.

Icinga obsahuje interní nástroj pro vytváření trendů sledované služby nebo hosta. Tím se rozumí generování grafu stavů, v nichž se určený objekt v zadaném časovém intervalu nacházel.



Obr. 3: Graf trendu služby

Kromě grafů trendů dovoluje Icinga vytvářet i grafy naměřených hodnot, k tomu ale používá externí rozšíření, jako např. Nagiosgraph nebo PNP4Nagios.

Obr. 4: Graf měřené veličiny

Pluginy pro sledování běžných služeb jsou součástí linuxových distribucí. Tisíce dalších pluginů lze získat z oficiálních repozitářů exchange.nagios.org a monitoringexchange.org.

Konfigurace

Konfigurace systému Icinga se zapisuje do textových konfiguračních souborů. Existují i nadstavby, které dovolují vytvořit konfiguraci klikáním na webových formulářích, ale nejčastěji se používá přímý zápis administrátora do konfiguračních souborů.

Definici sledované služby musí předcházet definice hosta, na kterém kontrola probíhá. Definice hosta může vypadat např. takto:

```
# ‘rs.cesnet.cz‘ host definition
define host{
    use                 generic-host          ; jméno použité šablony
    host_name           rs.cesnet.cz          ; jméno hosta
    alias               Mail Server           ; popis hosta
    address             rs.cesnet.cz          ; IPv4 adresa hosta
    address6            rs.cesnet.cz          ; IPv6 adresa hosta
    parents             ic-cat6509-gw.zcu.cz  ; nadřazený síťový host
    check_command       check_multi!check_multi_host_dualstack.cmd -r 1+2+4+8
                                      ; příkaz pro kontrolu dostupnosti hosta
    max_check_attempts    3     ; počet opakování kontrol při její neúspěšnosti
    notification_interval 120   ; interval opakování posílání upozornění
    notification_period   24x7  ; časová perioda pro posílání upozornění
    notification_options  d,u,r ; při jakém stavu hosta se upozornění posílá
    contact_groups        admins      ; kontakty, na které se upozornění posílá
}
```

Poté může být definována vlastní služba, např. tímto způsobem:

```
# Service definition
define service{
   use               generic-service  ; jméno použité šablony
   host_name          rs.cesnet.cz    ; jméno hosta
   service_description      MAILQ    ; jméno sledované služby
   check_period             24x7  ; časová perioda pro provádění kontroly služby
   max_check_attempts       3     ; počet opakování kontrol při její neúspěšnosti
   check_interval           5     ; interval provádění kontroly
   retry_interval           1
   notification_interval    120
   notification_period      24x7
   notification_options     w,u,c,r
   contacts                 jdoe
   contact_groups           admins
   check_command            check_nrpe!check_mailq!500 1000 ; příkaz pro kontrolu
   action_url /nagiosgraph/cgi-bin/show.cgi?host=$HOSTNAME$&service=$SERVICEDESC$
                             ; automatické generování grafu
}
```

Parametr notification_options určuje, při jakém stavu kontrolované služby má Icinga poslat upozornění kontaktním osobám svázaným s danou službou. Parametr může nabývat následujících hodnot:

w = Warning Služba je ve stavu varování.

u = Unknown Nebylo možné získat informaci o stavu služby.

c = Critical Služba je v kritickém stavu.

r = Recovery Služba se vrací do stavu OK.

f = Flapping Služba často mění stavy OK a chybový.

s = Scheduled downtime Upozornění bude posláno při zahájení a ukončení plánované odstávky.

n = None Nebude posíláno žádné upozornění.

Parametrem check_interval definujeme dobu, za jakou budou opakovaně plánovány dané kontroly. Nejčastěji se používá interval 5 minut.

Parametry contact a contact_groups zavádíme do prostředí Icingy záznamy uživatelů a jejich skupin, kterým má být posíláno upozornění. Určujeme komu, jakým způsobem, při jakém stavu kontrolované služby a v jakých časových periodách má být upozornění posíláno:

```
define contact{
    contact_name                    jdoe
    alias                           John Doe
    service_notification_period     24x7
    host_notification_period        24x7
    service_notification_options    w,u,c,r
    host_notification_options       d,r
    service_notification_commands notify-service-by-email,notify-service-b y-sms
    host_notification_commands      notify-host-by-email,notify-host-by-sms
    email                           jdoe@cesnet.cz
    pager                           420123456789
}
```

Časovou periodu definujeme např. takto:

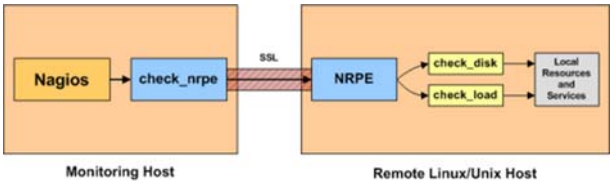
```
define timeperiod{
    timeperiod_name  24x7
    alias            24 Hours A~Day, 7 Days A~Week
    sunday           00:00-24:00
    monday           00:00-24:00
    tuesday          00:00-24:00
    wednesday        00:00-24:00
    thursday         00:00-24:00
    friday           00:00-24:00
    saturday         00:00-24:00
}
```

Obr. 5: Zobrazení všech sledovaných služeb daného serveru, včetně připsaného komentáře

Pro zvýšení přehlednosti zobrazování sledovaných hostů a služeb v prostředí webu můžeme použít jejich sdružování do skupin hostů (hostgroups) nebo skupin služeb (servicegroups).

Většinu kontrol provádíme přímým způsobem – tzn. že plánovač Icingy určí čas provedení konkrétní kontroly a jádro Icingy v daný čas spustí příkaz spojený s kontrolou dané služby. Tím se např. spustí plugin, který provede spojení na testovaný server a pokusí se ověřit stav sledované služby.

V některých případech však nejsou kontrolované služby nebo veličiny dostupné po síti přímo. Pak můžeme využít službu NRPE. Ta se skládá z démona běžícího na vzdáleném serveru, kde poslouchá a vykonává příkazy přicházející z Icinga serveru a dále z pluginu check_nrpe, který je spouštěn lokálně na Icinga serveru, odkud příkazy na NRPE server posílá, získává od něj odpovědi a ty předává do Icingy. Službu NRPE si lze představit jako proxy server.



Obr. 6: schéma NRPE služby

Celou situaci dobře osvětlí konkrétní příklad. Řekněme, že na vzdáleném serveru stream.cesnet.cz streamujeme vysílání televize, které přijímáme na připojené DVB-T kartě. V prostředí Icinga serveru bychom chtěli sledovat stav přijímaného signálu a jeho úroveň. K tomu můžeme na streamovacím serveru použít program femon, který poskytuje výstup:

```
stream.cesnet.cz:~# femon -H -c 1
FE: DiBcom 7000PC (DVBT)
status SCVYL | signal  53% | snr   0% | ber 0 | unc 0 | FE\_HAS\_LOCK
```

Prvním krokem je napsání pluginu check_dvbt, který bude spouštěný lokálně na streamovacím serveru, z výstupu programu femon bude kontrolovat,

zda druhé slovo je „SCVYL“ a na svůj standardní výstup bude vypisovat jeho hodnotu. Navíc přidá i hodnotu pátého slova odpovídající úrovni signálu.

```
#!/bin/sh

STATE_OK=0
STATE_WARNING=1
STATE_CRITICAL=2
STATE_UNKNOWN=3

line=‘femon -H -c 1 | grep "^status"‘
status=‘echo $line | awk ‘{print $2}‘ ‘
level=‘echo $line | awk ‘{print $5}‘ | cut -d"%" -f1‘

case $status in
        SCVYL)  code=$STATE_OK;;
        SCV)    code=$STATE_WARNING;;
        *)      code=$STATE_CRITICAL;;
esac

echo "DVB-T stutus=$status, signal=$signal | signal=$signal"
return $code
```

Stav kontrolované služby je určen hodnotou návratového kódu pluginu. Výrazy za znakem „|“ ve výstupu plugin jsou nazývány „performance data“. Používají se pro přenos dalších hodnot do vnitřního prostředí Icingy – v našem případě textového vyjádření stavu signálu a číselné hodnoty jeho úrovně, kterou si pak necháme graficky znázorňovat.

Druhým krokem je definice služby v konfiguraci Icingy:

```
# Service definition
define service{
   use                             generic-service
   host_name                       stream.cesnet.cz
   service_description             DVB-T
   check_period                    24x7
   check_interval                  5
   contact_groups                  admins
   notification_period             24x7
   check_command                   check_nrpe_1arg!check_dvbt
   action_url /nagiosgraph/cgi-bin/show.cgi?host=$HOSTNAME$&service=$SERVICEDESC$
}
```

Tím si Icinga zavolá v okamžiku spuštění kontroly služby DVB-T svůj lokální plugin check_nrpe, který se připojí na port NRPE démona cílového hosta stream.cesnet.cz a předá mu požadavek na vykonání příkazu check_dvbt. NRPE démon spustí lokální plugin check_dvbt. Jeho návratový kód i textový výstup pak check_nrpe plugin předá Icinga serveru.

Komunikace mezi check_nrpe pluginem a NRPE démonem je zabezpečená pomocí SSL. NRPE démon spouští jen příkazy definované v jeho konfiguraci.

Distribuované monitorování

Plánovač Icingy se snaží rozkládat vykonávání testů jednotlivých služeb rovnoměrně v čase. Tím významně snižuje požadavky na systémové zdroje serveru. Přesto u velkých instalací, kde se sledují desítky tisíc služeb, může být lepší rozložit sledování mezi několik Icinga serverů. Rozdělení sledování je účelné i v případech, kdy z důvodů bezpečnosti nechceme umožnit „hlavnímu“ Icinga serveru přímý přístup ke všem hostům a službám.

Sledování služeb rozložené mezi několik Icinga serverů označujeme za distribuované monitorování. Při něm se využívá možnosti získávat hodnoty sledovaných stavů a veličin z interních lokálních struktur Icingy.

Tato technika bude více srozumitelná na příkladu. Řekněme, že máme jádro páteřní infrastruktury, které není dostupné pro okolní svět. Chceme monitorovat jeho stavy, ale povolení přístupů z Icinga serveru připojeného do veřejné sítě považujeme za nebezpečné. V takovém případě můžeme do páteřní infrastruktury zapojit dedikovaný Icinga server, který bude kontroly provádět. Do jeho konfigurace navíc přidáme modul MK Livestatus, který poskytuje rozhraní pro přístup k interní struktuře naměřených hodnot.

K tomu, abychom měli hodnoty provedených kontrol k dispozici i na hlavním Icinga serveru, můžeme použít službu NRPE, přes níž spouštíme na dedikovaném Icinga serveru plugin check_multi, který vrací naměřená data (nebo jejich agregovanou podobu) z interních struktur. Hlavní Icinga server definuje tyto služby obvyklým způsobem, ale při jejich kontrole se provádí jen přenesení stavu kontroly, kterou provedl dedikovaný Icinga server. V případě, kdy by v době provádění kontroly nebyl dedikovaný server dostupný, přiřadí hlavní Icinga server dané službě stav Unknown.

Závěr

Monitorovací systém Icinga je univerzální dohledový nástroj, který díky své otevřenosti a srozumitelnému rozhraní pro pluginy najde uplatnění pro sledování téměř jakýchkoliv služeb a systémů. Jeho výhodou je i velké množství dostupných pluginů. K dispozici jsou také klienti pro přímý přístup z desktopů a z mobilních zařízení. Icingu lze dobře integrovat do existující infrastruktury.

Odkazy

[1] http://www.icinga.org

[2] http://www.nagios.org

[3] http://exchange.nagios.org

[4] http://monitoringexchange.org

Monitorovaci system Zabbix

Lukáš Malý

E-mail: Iam@LukasMaly.NET

1 Úvod

S pojmem monitorovací systém se setkal každý, kdo provozoval větší množství serverů či rozsáhlejší síť. Kde funkčnost neověříme jen díky používání těchto systému. Od toho nám slouží nástroje a mechanismy systematicky kontrolující funkčnost a dostupnost serverů a služeb.

Pojmy se kterými se běžně v Zabbixu setkáme:

Host – síťové zařízení, které chceme monitorovat za pomocí IP/DNS.

Host group – logická skupina hostů, existuje i speciální skupina Template, která obsahuje jen definice. Skupiny se používají pro lepší orientaci a hlavně se na ně aplikují práva uživatelů.

Item – položka definující samotná data.

Trigger – definuje hraniční hodnoty, pomocí kterých se vytváří notifikační akce.

Event – událost, která nastane v momentě, kdy je splněna podmínka Triggeru.

Action – definice, která říká kdo má být upozorněn na nějakou změnu skrze Trigger. Je možno nechat spustit např. nějaký script.

Escalation – definice scénáře následných akcí, které mají nastat v průběhu času od výskytu vzniklé události.

Media – definuje doručovací kanál Email, Jabber, RemoreScript.

Notification – zpráva o události zaslaná skrze definované Medium.

Remote command – pojmenovaný script, který lze použít při Akci nebo Notifikaci.

Template – definice hodnot (items, triggers, graphs, screens, applications).

Application – speciální typ skupiny Itemů, jen organizační pojmenování pro lepší přehlednost.

Web scenario – jeden nebo více definovaných HTTP požadavků, simulující klikání na obsah webu s ověřením, zda na stránce existuje požadovaný text, nebo zda požadavek vrací správný HTTP kód např. 200.

Frontend – webové rozhraní Zabbixu.

Zabbix API – Zabbix API povoluje užití JSON RPC protokolu vytvoření, aktualizace nebo získání Zabbix objektu (hosts, items, graphs a ostatní).

Zabbix-Server – hlavní část systému, která má uloženou konfiguraci a řídí, kdy a jak se co bude sledovat, odesílá notifikační zprávy zodpovědným osobám za sledované zařízení.

Zabbix-Agent – SW běžící na sledovaném serveru (UNIX nebo Windows). Agent poskytuje informace o stavu serveru, běhu definovaných procesů, paměti, procesoru a např. síťové karty atd.

Zabbix-Proxy – obdoba serverů určená pro běh ve vzdálených destinacích. Neukládá data, jen je pořizuje a předává Zabbix serveru.

Node – Zabbix server konfigurován jako součást distribuovaného monitorování. Může být použit pro monitorování specifické lokality.

2 Monitorovací systémy

Seznam existujících monitorovacích systému je vskutku velmi rozsáhlý. Existují drahá komerční řešení, ale též otevřené nekomerční. Před volbou použití monitorovacího systému je vždy nutno zvážit veškeré faktory. Cena je dnes velmi důležitá, protože mnoho otevřených systémů poskytuje velmi širokou funkcionalitu, kterou získáme zadarmo. Nutno dodat, každý monitorovací systém vyžaduje patřičně proškoleného admina. A to platí jak u komerčních ta i u nekomerčních systémů.

Pěkná a přehledná tabulka porovnání monitorovacích systému je na wikipedi. http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems

Monitorovací systémy jsou nástroje pro oddělení, které mívají často název NOC – Network Operation Center, nebo též **Operations Support Systems** (zkráceně OSS) se do češtiny překládají jako **systémy pro podporu provozu**.

Známé typy sledování

- Pasivní monitoring (sledování událostí, logů, ...)
- Aktivní monitoring (měření výkonnostních ukazatelů, cyklické testy)
- Správa (konfigurace zařízení, aplikací)
- Reporting (historická i aktuální data)

2.1 Otevřené

Zástupců otevřených systémů, je vskutku celá řada, uvedu jen pár známých aplikací. Cacti, Incinga, MRTG, Nagios, OpenNMS, Zabbix, Zenoss. Přesné porovnávání těchto systémů je hodné někoho kdo dané systémy podrobně zná

a ovládá veškeré jejich funkcionality již někde implementoval. Osobně jsem většinu z těchto systému minimálně testoval.

2.2 Komerční

Placených systémů je též celá řada, IBM Tivoli, HP OpenView , Microsoft System Center, WhatsUpGold.

Problém ohledně srovnání komerčních aplikací a otevřených spočívá spravidla v tom, že neexistují nějaké testovací verze, kde vyzkoušíme patřičnou funkcionalitu. Např. obdobná funkcionalita jako je Zabbix Proxy je nedostupná pro demo či jiné verze.

Zabbix jako produkt je plně otevřený bez nějakých Profesional nebo Enterprise verzí. Je to pravý Open Source, za kterým stojí firma zajišťující placenou podporu. Není to jen komunitní systém, ikdyž i takové systémy jsou patřičně konkurence schopné.

2.3 Vlastnosti Zabbixu

Distribuovaný monitoring a výkon

- centralizovaná správa monitoringu systémů – sběr dat do jednoho místa
- vzdálená správa prostřednictvím webového rozhraní
- testováno až se 100 000 monitorovanými zařízeními

Monitoring v reálném čase

- monitoring výkonu zařízení
- monitoring dostupnosti zařízení
- monitoring integrity
- definovatelné podmínky pro notifikace o problémech systémů
- notifikace uživatelů o problémech (Email, SMS, Jabber)
- podrobné logování problémů a jejich výstup na dashboard

Vizualizace informací

- uživatelsky definovatelné pohledy na data
- zobrazování informací pomocí grafů
- zobrazování informací ve zvolených časových intervalech např. za hodinu, půlden, celý den apod.

Reportování

- reportovací funkce umožňující přehledný soupis o běhu systému za dané období

WEB monitoring

- monitorování webových stránek a rychlosti odezvy
- podpora pro POST a GET metody

Flexibilita

- podpora pro IPv4 a IPv6
- běží na většině platforem
- klientská část (agenti) dostupná téměř pro všechny významné OS

Agregovaný monitoring

- monitorování skupiny zařízení jako jednoho systému

Monitoring zařízení bez nutnosti instalace sběrného agenta(pasivní monitoring)

- monitoring vzdálených služeb jako FTP, SSH, http apod.
- podpora pro SNMP v1,2,3
- podpora pro IPMI

Agenti pro sběr informací o systémech dostupné pro všechny běžné platformy (UNIX, Windows apod.)

- monitoring využití paměti
- monitoring síťových operací
- monitoring diskových operací a zatížení disků
- kontrola místa na disku
- kontrola checksumu souborů
- monitoring změny systémových souborů

Zabezpečení pružné nastavení přístupů per uživatel s možností definování přístupu na monitorovaná zařízení

- autentizace na základě IP adresy
- ochrana proti síťovým útokům ‚brute force‘

Eskalace problémů a notifikace

- opakované notifikace
- neomezená eskalace
- notifikace o vyřešení problému

Dashboard

- upravitelný dashboard zobrazující vybrané informace
- agregované pohledy
- zobrazování eskalovaných problémů

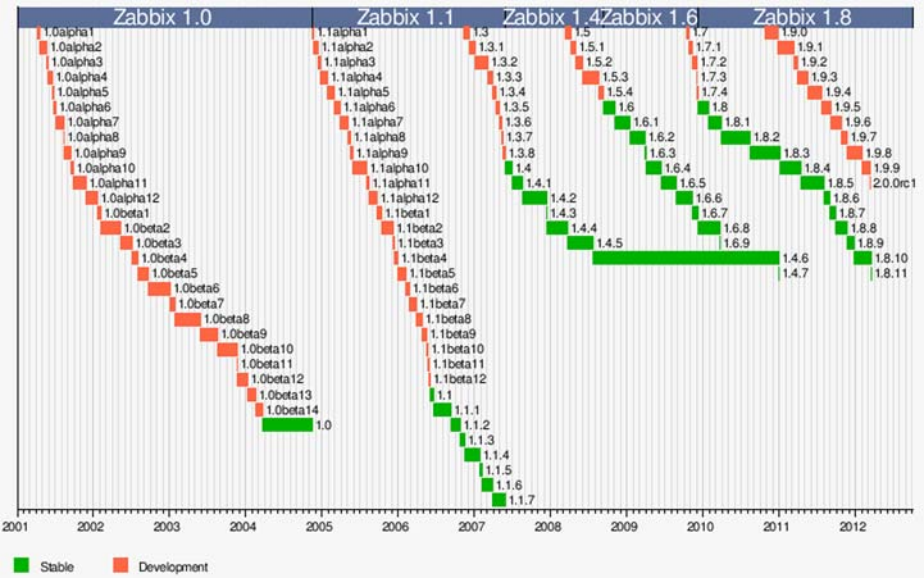
3 Historie

Zabbix byl vyvíjen jako interní projekt jedné Litevské banky. Autorem je Alexei Vladishev, který Zabbix ve verzi 1.0alpha1 7. 4. 2001 uvolnil pod licencí GPL. O tři roky později vyšla první stabilní verze Zabbix 1.0. Alexei založil společnost Zabbix SIA, která je dnes tvůrcem a propagátorem tohoto systému. Společnost uzavírá partnerské smlouvy, poskytuje placenou pětistupňovou podporu, zajišťuje konzultační a instalační služby. Jako produkt je plně otevřený bez nějakých Profesional nebo Enterprise verzí.

Aktuální verzí je Zabbix 1.8.11 a ve vývoji je verze Zabbix 2.0.0rc2, která má přinést nové funkcionality. Nejzajímavější novou vlastností je podpora Javy, která lze do serveru i agenta zkompilovat. Zabbix JMX monitoring umožňuje nativní bezpečné monitorování Java applikací a populárních aplikačních serverů JBoss, WebSphere a WebLogic.

4 Verze systému

Po dobu co se Zabbix aktivně vyvíjí což je již 11 let urazil velký kus cesty.



Obr. 1 Vývoj Zabbix – tabulka

5 Instalace systému

5.1 Appliance

Pro rychlé vyzkoušení Zabbixu tvůrci pravidelně vydávají Zabbix Appliance. Je založena na distribuci OpenSuSE Linux s podporou MySQL jako back-end. Zabbix software je předinstalován a nakonfigurován pro okamžité použití. Pravidelně připravované jsou tyto formáty.

- VMware/VirtualBox (.vmdk)
- Open virtualization format (.ovf)
- Live CD/DVD (.iso)
- Preload ISO
- USB stick/hard disk image
- Xen guest

5.2 Balíčky distribucí

Většina Linuxových distribucí má pro Zabbix připravené patřičné baličky. Např. instalace balíčků Debian/Ubuntu zajistí instalaci závislostí, jako je MySQL, Apache a PHP. Instalace je rychlá a provede se i založení patřičné databáze a uživatele spolu s importem SQL struktury dat.

NeLinuxový OS FreeBSD má též patřičný port, který zajistí instalaci binárek spolu se závislými programy, ale založení databáze a import SQL struktury dat musíme udělat ručně.

Nespornou výhodou FreeBSD oproti Debian/Ubuntu je fakt, že porty jsou nezávislé na verzi OS. Např. když máme systém FreeBSD 8.2, tak si na daném systému zprovozníme aktuální verzi portu zabbix-server-1.8.10, tutéž verzi můžeme mít zprovozněnou i na FreeBSD 9.0.

U distribucí Debian/Ubuntu je verze Zabbixu závislá na daném release distribuce. V průběhu života např. distribuce Ubuntu 10.04.4 LTS se verze Zabbix serveru nebo Zabbix Agenta nepovyšuje, jen se vydávají případné opravy balíčku. Což k poměrně aktivnímu vývoji Zabbixu je dosti omezující. Osobně jsem ve verzi 1.8.x zaznamenal časté úpravy Zabbix frontendu, které přinášely známe opravy chyb a nové ovládací funkce.

5.3 Source Code

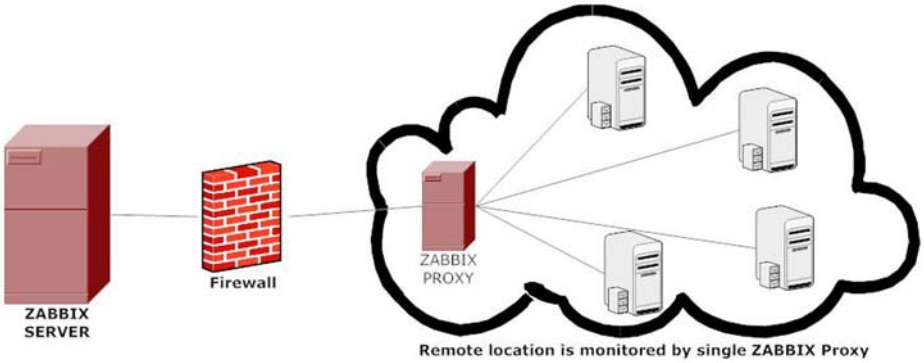
Osvědčenou instalací je manuální kompilace a instalace systému ze zdrojových kódů. Je to pracnější postup, vyžadující instalaci devel balíčků, které jsou nutné pro kompilaci. Nevýhodou je že operační systém o daném software nic neví. Veškeré opravy SW a aktualizace musíme realizovat ručně.

5.4 Vlastní repository

Pro velké společnosti, využívající jednotné Linuxové prostředí se vyplatí vytvářet a udržovat si vlastní verze balíčků jak RPM tak např. deb.

6 Zabbix Server, Proxy, Node

Jak již bylo zmíněno v úvodu, Zabbix má několik režimů používání. Samotný Server ke svému běhu vyžaduje relační databázi, na výběr jich je hned několik. Asi nejpoužívanější je MySQL, dále PostgreSQL, SQLite, Oracle nebo IBM DB2. Volbu vhodné databáze je vždy nutné posoudit, před instalací. Musíme předem vědět, jak velké množství zařízení budeme monitorovat. Mnoho databází dnes podporuje partitioning. Pro tunning výkonu zabbixu se často objemné tabulky přenastavují do tohoto režimu. Výrazně se tím zvýší výkon celého monitorovacího systému.



Obr. 2 Zabbix Proxy – schema

Pro monitorování vzdáleních destinací např. pobočka nebo nějaká síť, která není v rozsahu internetu, má zabbix k dispozici Zabbix Proxy, což je vzdálený server, který sbírá data a předává je Zabbix serveru. Proxy serverů můžeme mít libovolné množství, jen jej musíme mí patřičně nakonfigurován. V momentě, kdy sledovanému hostu přiřadíme danou proxy v patřičných časových intervalech server zasílá konfiguraci monitorování do proxy serveru.

Běžně používáme Zabbix Server v režimu standalone. Existuje možnost provozovat více nodů serverů. Toto řešení je vhodné použít pro monitorování např. v nějaké velké korporátní organizaci, kdy je třeba oddělit sledování velkého množství serverů a sítí. Nutno dodat, že pokud překlopíme standalone server na node01 musí se patřičně překonvertovat data v databázi, protože jednotlivé nody spolu komunikují a data se nesmí pomíchat.

Zabbix server má několik interních procesů

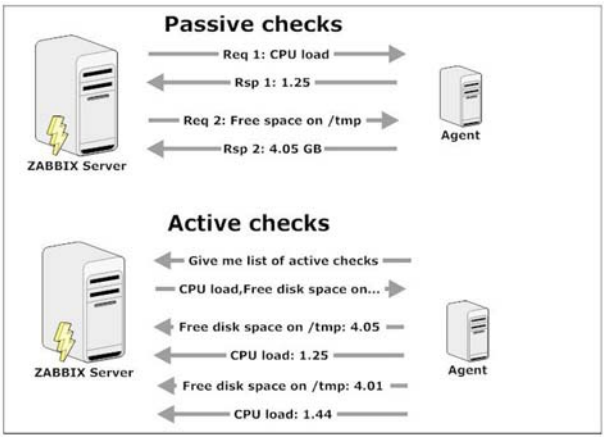
- poller
- trapper
- impi poller
- discoverer
- icmp pinger
- http poller
- proxy poller
- unreachable poller

Jednotlivé interní procesy se konfigurují v nastavení serveru, kolik jich má být startováno atd. Zabbix umí poměrně efektně monitorovat sám sebe.

6.1 Zabbix Agent

Pro monitorování serverů můžeme využít Agenta, což je SW běžící na daném serveru. Konfigurace server a Agent je preferována. I když některé hodnoty se dají získat jak z Agenta tak pomocí protokolu SNMP, je Agent upřednostňován, kvůli vyšší spolehlivosti. Navíc Agent podporuje Aktivní i Pasivní režim. Dále nám agent umožňuje definování vlastních proměnných, jejich hodnoty jsou sbírány vlastními scripty, které mohou být psány v libovolném jazyce atd.

Komunikace mezi Server <> Agent probíhá pomocí protokolu ZBX, který je postaven na JSON. Stejný protokol je používán pro komunikaci Server <> Proxy či Server Node01 <> Server Node02.



Obr. 3 Typy komunikace Agenta

Jednoduchým testem fungování agenta je např. připojení pomocí telnetu na patřičný port.

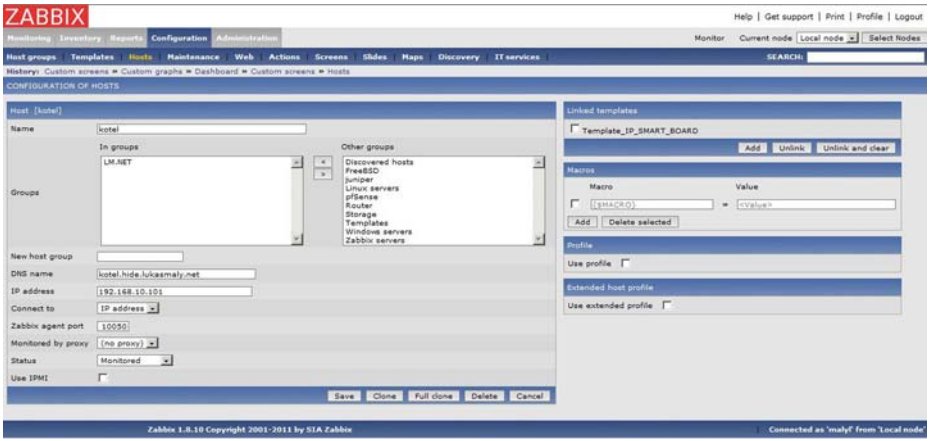
```
[malyl@monitor ~]$ telnet mimas 10050
Trying 192.168.42.10...
Connected to mimas.hide.lukasmaly.net.
Escape character is '^]'.

ZBXDZBX_NOTSUPPORTEDConnection closed by foreign host.
```

Pokud na serverech používáme lokální firewall, je třeba povolit patřičnou komunikaci ve správných směrech. Pomocí telnetu prověříme, zda nám agent odpovídá. Obdobně tomu je u komunikace mezi Server <> Proxy atd.

7 Jak monitorujeme

Jako ukázku jsem zvolil sledování malého zařízení IP SMART BOARD, které používám jako termostat. Jsou k němu připojeny dvě teplotní čidla. Zařízení má implementováno SNMP a již v minulosti jsem si pro dané zařízení vytvořil template se sledovanými hodnotami. Template je ve formě XML ke stažení na URL http://ftp.smejdil.cz/Zabbix/Template_IP_SMART_BOARD.xml



Obr. 4 Konfigurace hosta

Ve webovém admin rozhraní přidáme hosta a nastavíme potřebné údaje, jako je skupina, IP, Template, případně Proxy atd.

Obrázek 5 ukazuje definici jedné hodnoty z Template_IP_SMART_BOARD

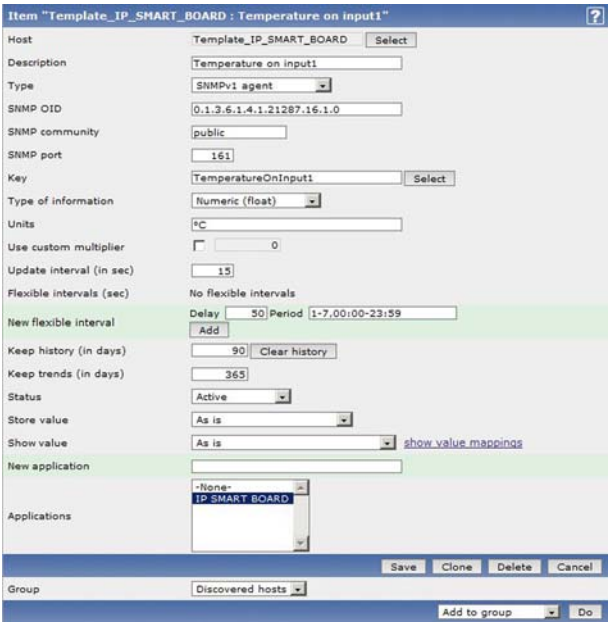
Nejdůležitějším prvkem je **Item type**, kterým říkáme jak budeme danou hodnotu získávat. Typů je celá řada a je vhodné si pročíst důkladně dokumentaci, pro jejich používání. Volbou Item type se často výrazně změní celý zadávací formulář s ohledem na typ získání hodnoty.

V dokumentaci najdeme přehlednou tabulku všech podporovaných hodnot.
http://www.zabbix.com/documentation/1.8/manual/config/items
http://www.zabbix.com/documentation/2.0/manual/config/items/itemtypes

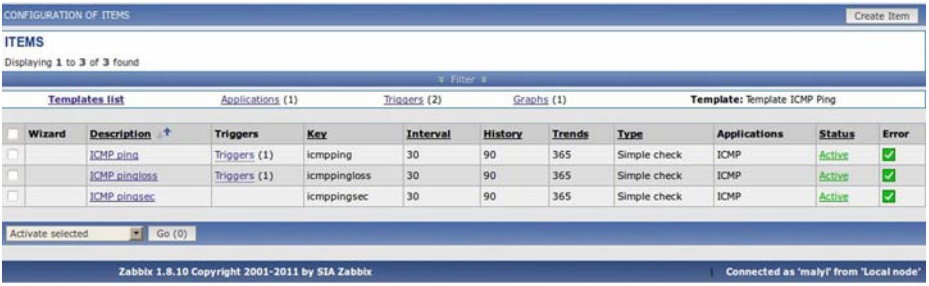
Podrobněji je to rozepsáno v dokumentaci k verzi 2.0.

8 Jednoduchá kontrola pomocí Ping

Zabbix má jeden z mnoha Item Type – **Simple Check**. Pomocí něj můžeme vytvořit Template_ICMP pro kontrolu jakéhokoliv zařízení. Zde je obrazová ukázka jak vypadá Items, Trigger, Graph výsledný graf naměřených hodnot.



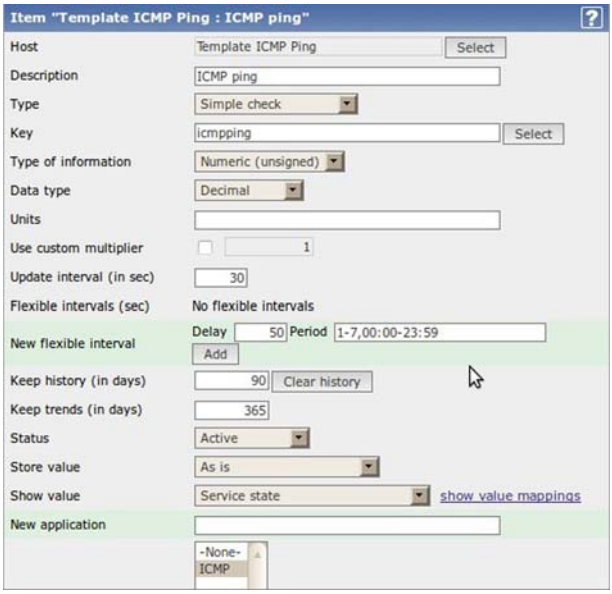
Obr. 5 Definice Items SNMP



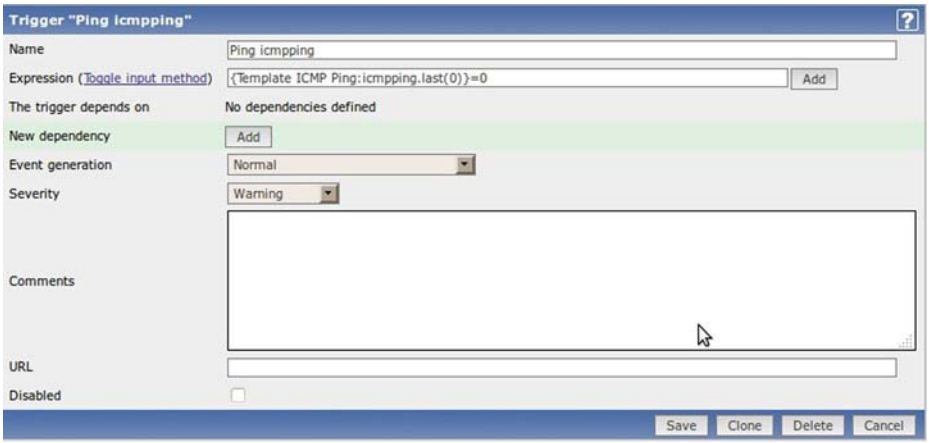
Obr. 6 Konfigurace Items

Nově vytvořený template obsahuje tři hodnoty a dvě z nich mají definován trigger. Přehledná tabulka nám prozradí informace o položkách. Ne vše je zde vidět. Pro podrobnější nastavení musíme položku případně editovat.

Ve formuláři je nejdůležitější Item Type a Key. Dále můžeme nastavit i Units, které se zobrazují v grafu.

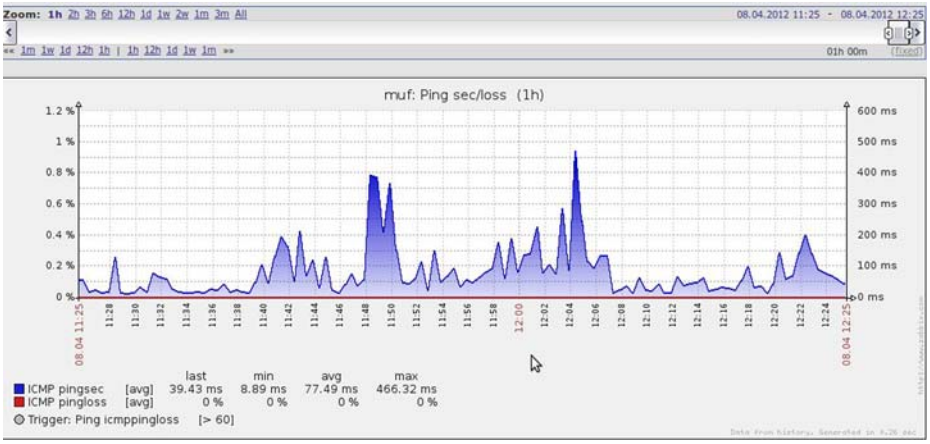


Obr. 7 Formulář pro nastaveni Items



Obr. 8 Nastavení Triggru

Graf je dynamický a je možno si jeho zobrazení přiblížit nebo oddálit. Pomocí horní lišty a předdefinovaných hodnot. Dále je na ní i scrollbar, který je též modifikovatelný do prava a do leva, čímž se definuje časový interval zobrazený na grafu. Dále při kliku na graf se nám označí a vybere požadovaný časový úsek a ten se nám přiblíží – graf se překreslí.



Obr. 9 Graf hodnot pingu

9 Rozšíření použití Zabbix Agenta

Implementovány jsou v Agentu jen některé klíče či hodnoty. Pokud nám to nestačí, můžeme si nadefinovat vlastní hodnoty ke sledování. V konfiguraci Zabbix Agenta existuje direktiva

```
UserParameter=key,command
```

klíč v UserParameter musímě nějak pojmenovat a za „,“ máme příkaz, který se má vykonat. Jeho návratovou hodnotou může být, integer, float i text. V patřičném template pak musíme mít nadefinován Item s odpovídajícím klíčem. Konfigurace se provádí v souboru **zabbix_agentd.conf.**

Na těchto URL jsou ukázky použití vlastních uživatelských parametrů.
http://www.zabbix.com/documentation/1.8/manual/config/user_parameters
http://www.zabbix.com/documentation/2.0/manual/config/items/userparameters
http://www.zabbix.com/documentation/2.0/manual/config/items/userparameters/extending_agent

10 SNMP – Simple Netwwork Management Protocol

Jedním z hojně používaných protokolů používající pro monitoring je SNMP. Dá se říci, že tento protokol je starý a složitý. Tento protokol je již mnoho let implementován do celé řady síťových zařízení, od switchů počínaje až po

printservery nebo tiskárny. Často se objevuje i u specifických embeded zařízení pro řízení výroby atd.

Pokud výrobce protokol SNMP implementuje, je velmi důležité, aby správně použil i definování MIB[1]. Bohužel ne každý výrobce dodává podrobnou dokumentaci.

10.1 Mikrotik

Měl jsem tu možnost mít přístup k velkému množství různých verzí routrového OS Mirotik. Měl jsem snahu sestavit Template pro Zabbix, ale narážel jsem na, podle mého soudu špatnou implementaci SNMP. Více popisuji na svém blogu.

Příspěvek na Blogu

http://blog.smejdil.cz/2012/03/zabbix-snmp-vs-mikrotik.html

Zabbix podporuje SNMP ve verzích 1, 2, 3. Nutno dodat, že po instalaci Zabbixu nemáme SNMP plně funkční. Měli bychom si doinstalovat MIB soubory od IETF, případně od jednotlivých výrobců HW. Pokud budeme tvořit vlastní template můžeme použít OID v číselné podobě, ale pokud máme MIBy můžeme použít i jmenné názvy OID.

Např. pro vypsání všech typů interface na routeru můžeme použít patřičné MIB OID.

```
snmpwalk -On -c public -v 2c 10.10.1.2 IF-MIB::ifType
.1.3.6.1.2.1.2.2.1.3.1 = INTEGER: ethernetCsmacd(6)
.1.3.6.1.2.1.2.2.1.3.2 = INTEGER: ethernetCsmacd(6)
.1.3.6.1.2.1.2.2.1.3.3 = INTEGER: ethernetCsmacd(6)
.1.3.6.1.2.1.2.2.1.3.4 = INTEGER: ieee80211(71)
.1.3.6.1.2.1.2.2.1.3.5 = INTEGER: ieee80211(71)
.1.3.6.1.2.1.2.2.1.3.6 = INTEGER: ieee80211(71
```

Zabbix podporuje i dynamické indexy, které nám umožní snadnější přístup k sledovaným hodnotám.

Syntax

```
<base OID of data>["index","<base OID of index>","<string to search for>"]
```

Example

```
ifInOctets["index","ifDescr","GigabitEthernet0/1"]
```

11 IPMI – Intelligent Platform Management Interface

V Zabbixu je implementováno OpenIPMI, což je otevřená implementace Intelovského standardu – protokolu IPMI.

[1] MIB je zkratka management information bases, definuje hierarchii jmenných názvů objektů SNMP.

Standard IPMI poskytuje možnosti vzdáleného přístupu, monitorování a administrace serverů a dalšího hardware, nová verze specifikace 2.0 je nyní podporována i mnoha servery optimalizovanými do rackových skříní a blade servery. Ačkoliv standard IPMI verze 2.0 byl již přijat více než 150 výrobci serverových technologií, přesto jeho používání v podnikových sítích není příliš rozšířeno.

Servery s funkčností dle standardu IPMI umožňují administrátorovi přístup a monitoring hardware serverů, jeho diagnostiku a dokonce i obnovení funkčnosti zamrzlého serveru. Tyto schopnosti jsou umožněny speciálním procesorem zvaným baseboard management controller (BMC), umístěným na motherboardu serveru nebo v šasí blade serveru. Procesor BMC je spojen s hlavním procesorem a dalšími jednotkami základní desky jednoduchou sériovou sběrnicí. Pomocí ní monitoruje základní parametry motherboardu (např. teplotní senzory, status CPU, otáčky větráků a napájení), umožňuje vzdálené řízení napájení serveru (čili schopnost restartu serveru) a přístup ke konfiguraci BIOSu a informacím konzole operačního systému. Protože BMC je samostatný procesor, systém pracuje bez ohledu na to, běží-li hlavní procesor serveru nebo ne.

Přístup administrátora k informacím poskytovaným procesorem BMC je možný buď pomocí správní aplikace kompatibilní se standardem IPMI ze síťového desktopu nebo vzdáleně pomocí webového rozhraní z tzv. out-of-band zařízení se zabudovaným IPMI firmware.

Bohužel se mi pod ruku nedostal žádný HW, na kterém bych prakticky IPMI a Zabbix vyzkoušel.

12 WEB monitoring

Pro monitorovací scénáře sledování webových prezentací, používá zabbix cURL, přesněji knihovnu libcurl.

Scénář obsahuje několik definovaných URL, na které zabbix přistupuje. Výslednou stránku můžeme kontrolovat na daný obsahující text. Monitorováním webů zjistíme rychlost přenosu jednotlivých URL.

Pomocí proměnných POST a GET umí Zabbix simulovat i jednoduché přihlášení do webové aplikace.

Z grafů pak můžeme dohledat problémy např. s pomalým generováni webového obsahu.

13 API

Pro integraci zabbixu s jinými systémy, či pro vlastní přístup z vlastní webové presentace máme API[2]. Uživatel využívající API musí mít nastaveno patřičné

[2] API – Application Programming Interface

právo. API nám umožňuje vytvářet hosty, nahlížet na grafy atd. Více je patřičně zdokumentováno.

Hlavním mechanismem fungování API je JSON-RPC[3] známe implementace jsou v těchto jazycích Ruby, PHP, Python.

PHP Class jednou z nejpoužívanějších.
http://andrewfarley.com/php/zabbix-1-8-api-php-class-v1-0

Ukázka použití API:

```
require_once("ZabbixAPI.class.php");

// This enables debugging, this is rather verbose but can help debug problems
//ZabbixAPI::debugEnabled(TRUE);

// This logs into Zabbix, and returns false if it fails
ZabbixAPI::login(‘ http://genbook/zabbix/‘ ,‘ apiuser‘ ,‘ ap1‘ )
    or die(‘ Unable to login: ‘ .print_r(ZabbixAPI::getLastError(),true));

// This gets the version of the zabbix server
$version = ZabbixAPI::fetch_string(‘ apiinfo‘ ,‘ version‘ )
    or die(‘ Unable to get Zabbix Version:
 ‘ .print_r(ZabbixAPI::getLastError(),true));
echo "Server running Zabbix API Version: $version\n";

// Fetch the user ids on the server, fetch_column ensures we just get the first
// item if you want to understand why I do this, put fetch_array instead and see!
$users = ZabbixAPI::fetch_column(‘ user‘ ,‘ get‘ )
    or die(‘ Unable to get user ids: ‘ .print_r(ZabbixAPI::getLastError(),true));
echo "User IDs found: ".implode($users,‘ ,‘ )."\n";

// Fetch hosts, but with extend option to get more data, and limit records
        returned
$five_hosts = ZabbixAPI::fetch_array(‘ host‘ ,‘ get‘ ,array(‘ extendoutput‘ =>1,
 ‘ limit‘ =>5))
    or die(‘ Unable to get hosts: ‘ .print_r(ZabbixAPI::getLastError(),true));
echo "Retrieved maximum of five hosts: ".print_r($five_hosts, true)."\n";

// Do a simple update of userid = 1, set refresh = 1000
// NOTE: If this fails, it‘ s because your API user is not a super-admin
ZabbixAPI::query(‘ user‘ ,‘ update‘ ,array(‘ userid‘ =>1, ‘ refresh‘ =>1000))
    or die(‘ Unable to update: ‘ .print_r(ZabbixAPI::getLastError(),true));
echo "Updated userid 1 with refresh value of 1000!\n";
```

14 Knihovny a nástroje třetích stran

Zabbix zjevně díky otevřenosti s oblibou používá mnoho uživatelů a firem. Díky tomu vzniká spousta dalších nástrojů a aplikací. Osobně jsem testoval mobilní

[3] JSON-RPC – JavaScript Object Notation – remote procedure call protocol

přístup z telefonu se systémem Android. Kvalita těchto aplikací je různá, ale použitelné jsou.

- DbforBIX, Oracle, PostgreSQL, MySQL – konektory pro Zabbix do DB
- Zapcat – JMX Bridge > Tomcat, WebSpheare, WebLogic
- JSON/RPC (Ruby, PHP, Python)
- Zabcon – Ruby
- Android/iPhone – ZBX Mobile Pro, ZAX, Mobbix Lite

15 Zabbix konference, CeBIT 2012

Na podzim loňského roku se v Litvě ve městě Riga konala konference vývojářů a administrátorů. Bylo na ni presentováno mnoho přednášek na zajímavá témata.

Pěkné info, jak zoptimalizovat běh zabbix serveru http://www.zabbix.com/conf2011_agenda.php.

Dále blogu Zabbixu nedávno proběhla informace o účasti společnosti Zabbix SIA na veletrhu CeBIT 2012.

16 Závěr

Tento monitorovací systém dle mého soudu již dozrál do takových kvalit, že do značné míry může nahradit komerční systémy. Při vhodném použití může být velmi slušným konkurentem.

Literatura

[1] Domovská stránka projektu Zabbix http://www.zabbix.com/

[2] Vladishev, A.: Riga Litva. http://www.netways.de/uploads/media/Alexei_Vladishev_Open_Source_Monitoring_with_Zabbix.pdf

[3] *Zabbix User's Manual* http://www.zabbix.com/documentation/1.8/start http:///www.zabbix.com/documentation/2.0

[4] *Zabbix Wiki* http://www.zabbix.com/wiki/

[5] Macura, L.: Opava http://www.cesnet.cz/akce/2011/monitorovani-kampusovych-siti/p/macura-zabbix.pdf

[6] Ptáček, J.: http://www.svetsiti.cz/
clanek.asp?cid=IPMI-V20-zjednodusuje-spravu-serveru-28112005

[7] *Zabbix 1.8 Network Monitoring* – Packt Publishing, 2010.
ISBN 978-1-847197-68-9.

Prezentace stavu infrastruktury pro lamy

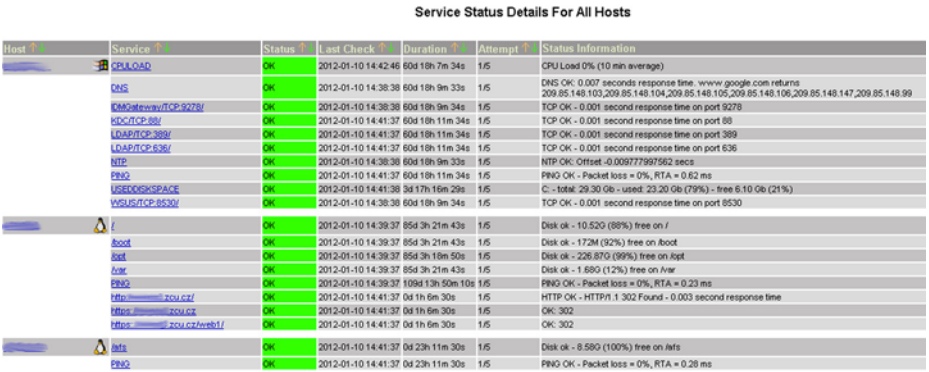
Petr Hanousek

E-mail: phanousk@civ.zcu.cz

1 Jaký byl náš cíl

Běžný uživatel (operátor HelpDesku) by měl mít šanci na první pohled porozumět významu informací při pohledu do monitorovacího systému. Rozhodli jsme se, že toho dosáhneme zjednodušením prezentovaných informací a jejich grafickým znázorněním. Cílem tedy bylo přejít od hromady informací (listu sledování) k nějakému strukturovanějšímu pohledu.

Na obrázku 1 je zobrazen pohled do Nagia (http://www.nagios.org), který běžně používají administrátoři systémů. Je to v podstatě „plochý“ seznam sledovaných služeb, přiřazených pod nějaké fyzické stroje.



Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
[redacted]	CPULOAD	OK	2012-01-10 14:42:46	60d 18h 7m 34s	1/5	CPU Load 0% (10 min average)
	DNS	OK	2012-01-10 14:38:38	60d 18h 9m 33s	1/5	DNS OK: 0.007 seconds response time. www.google.com returns 209.85.148.103,209.85.148.104,209.85.148.105,209.85.148.106,209.85.148.147,209.85.148.99
	IDMGateway/TCP:9278/	OK	2012-01-10 14:38:38	60d 18h 9m 34s	1/5	TCP OK - 0.001 second response time on port 9278
	KDC/TCP:88/	OK	2012-01-10 14:41:37	60d 18h 11m 34s	1/5	TCP OK - 0.001 second response time on port 88
	LDAP/TCP:389/	OK	2012-01-10 14:41:37	60d 18h 11m 34s	1/5	TCP OK - 0.001 second response time on port 389
	LDAP/TCP:636/	OK	2012-01-10 14:41:37	60d 18h 11m 34s	1/5	TCP OK - 0.001 second response time on port 636
	NTP	OK	2012-01-10 14:38:38	60d 18h 9m 33s	1/5	NTP OK: Offset -0.009777997562 secs
	PING	OK	2012-01-10 14:41:37	60d 18h 11m 34s	1/5	PING OK - Packet loss = 0%, RTA = 0.62 ms
	USEDDISKSPACE	OK	2012-01-10 14:41:38	3d 17h 16m 29s	1/5	C: - total: 29.30 Gb - used: 23.20 Gb (79%) - free 6.10 Gb (21%)
	WSUS/TCP:8530/	OK	2012-01-10 14:38:38	60d 18h 9m 34s	1/5	TCP OK - 0.001 second response time on port 8530
[redacted]	/	OK	2012-01-10 14:39:37	85d 3h 21m 43s	1/5	Disk ok - 10.52G (88%) free on /
	/boot	OK	2012-01-10 14:39:37	85d 3h 21m 43s	1/5	Disk ok - 172M (92%) free on /boot
	/opt	OK	2012-01-10 14:39:37	85d 3h 18m 50s	1/5	Disk ok - 226.87G (99%) free on /opt
	/var	OK	2012-01-10 14:39:37	85d 3h 21m 43s	1/5	Disk ok - 1.68G (12%) free on /var
	PING	OK	2012-01-10 14:39:37	109d 13h 50m 10s	1/5	PING OK - Packet loss = 0%, RTA = 0.23 ms
	http://[redacted].zcu.cz/	OK	2012-01-10 14:41:37	0d 1h 6m 30s	1/5	HTTP OK - HTTP/1.1 302 Found - 0.003 second response time
	https://[redacted].zcu.cz	OK	2012-01-10 14:41:37	0d 1h 6m 30s	1/5	OK: 302
	https://[redacted].zcu.cz/web1/	OK	2012-01-10 14:41:37	0d 1h 6m 30s	1/5	OK: 302
[redacted]	/afs	OK	2012-01-10 14:41:37	0d 23h 11m 30s	1/5	Disk ok - 8.58G (100%) free on /afs
	PING	OK	2012-01-10 14:41:37	0d 23h 11m 30s	1/5	PING OK - Packet loss = 0%, RTA = 0.28 ms

Obr. 1 Služby v Nagiovi – zobrazení pro správce

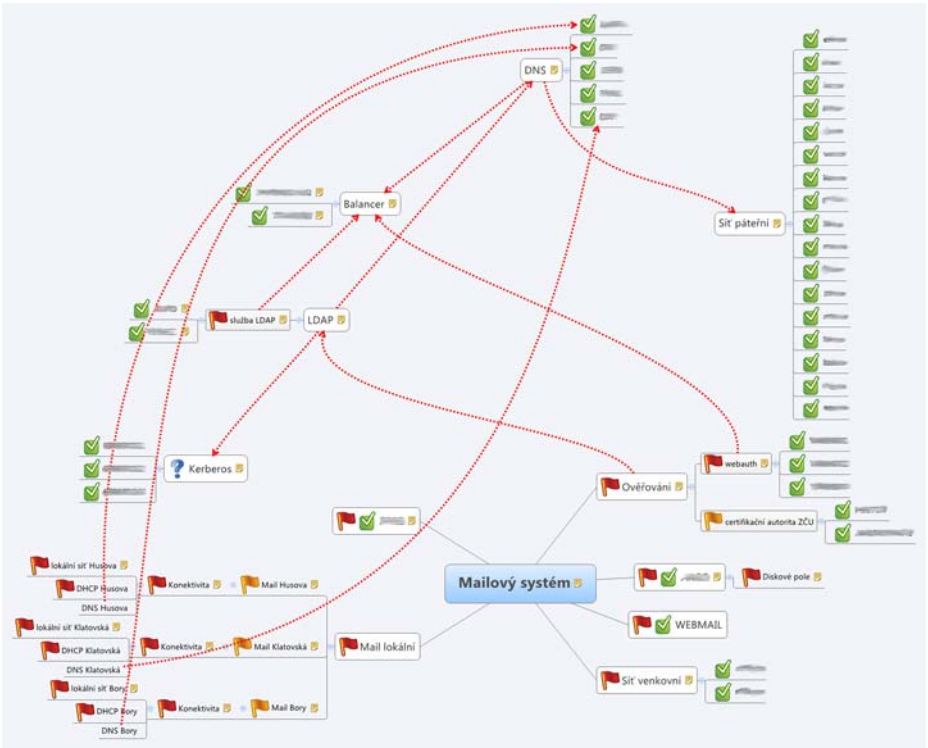
Tento pohled je ale nepřehledný a pro běžného uživatele nevhodný. Nepřehledný je proto, že nemá vhodnou strukturu, kromě příslušnosti služeb k serverům. Nevhodný proto, že služby jsou pojmenované tak, aby jim rozuměli administrátoři, kteří potřebují pojmenování služeb spíše podle běžících procesů na serverech a expertně ví, co která služba ve skutečnosti dělá, co to znamená když nefunguje, jaké další služby nebudou návazně fungovat také a podobně. Názvy

jsme tedy potřebovali zřídit takové, aby jim běžný uživatel alespoň trochu rozuměl. To není například *„dhcpd“*, ale už to může být *„DHCP“*.

Navíc jsme potřebovali nějak zapsat (zobrazit) onu zmiňovanou expertní znalost administrátorů, tedy povědomí o tom, co na co navazuje a co se stane (co všechno nebude chodit, kam se to promítne), když „spadne DNS“.

2 Postup při řešení, způsob řešení

Řešení mělo dvě části, administrativní a technickou. V administrativní části bylo nutné vytipovat viditelné služby z pohledu uživatele (elektronická pošta, informační systémy, datové úložiště, ...) a namapovat je na již zavedené sondy v Nagiovi. K tomu jsme kromě rozhovorů se správci služeb použili i nástroj Xmind (http://www.xmind.net), který umožňuje jednoduché a přehledné kreslení „krabiček“ včetně jejich závislostí. Příklad definované high-end služby je na obrázku 2.



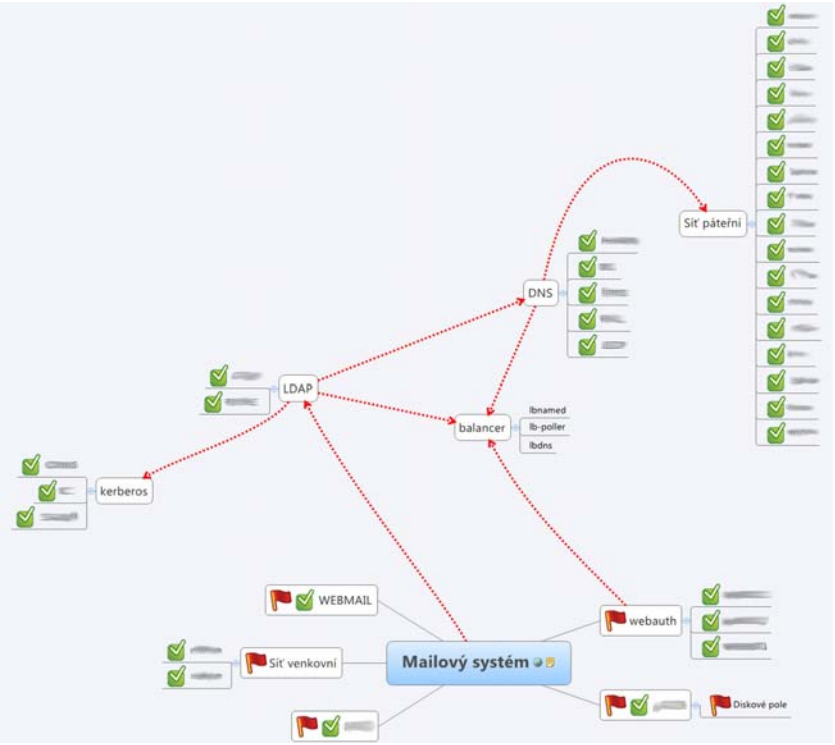
Obr. 2 Definice závislostí služeb a strojů

Vysvětlivky:

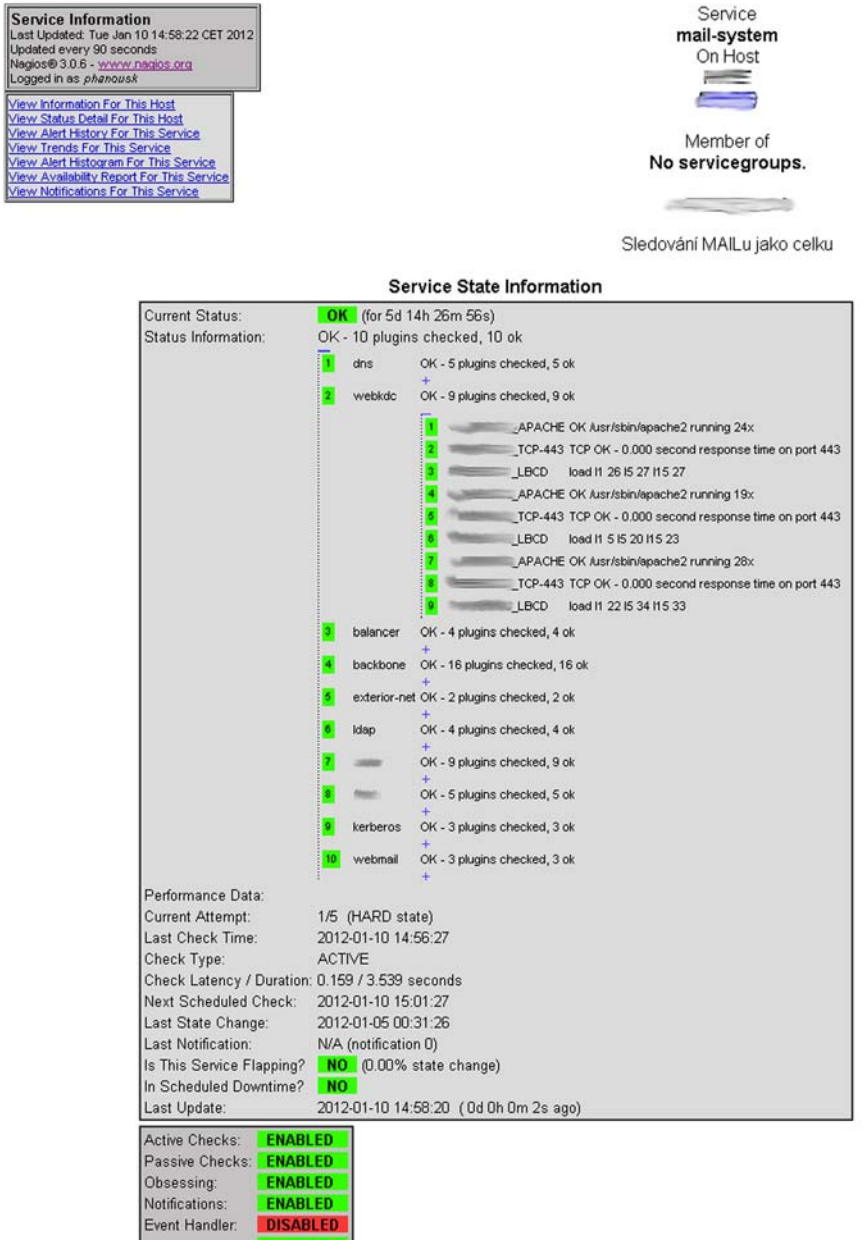
- Červené šipky a vlaječky znamenají kritickou závislost – když nepůjde odkazovaná služba, nebude fungovat ani nadřazená služba, nebo nebude fungovat korektně),
- žluté vlaječky jsou „varování“ – když nepůjde služba se žlutou vlaječkou, její rodič má problém, který uživatel pozná jenom někdy,
- zelená zaškrtávátka značí koncový server – tyto *hosty* už jsme měli v Nagiovi definované, včetně na nich provozovaných služeb, viz obrázek 2.

Jak vyplývá z obrázků, museli jsme v Nagiovi definovat nové služby, které do sebe s potřebnou logikou sdružují již v minulosti nadefinované služby.

Při definici nových souhrnných služeb v Nagiovi bylo dobré již nakreslené obrázky s vazbami zoptimalizovat. Postup proto není stejný pro každou nově sledovanou službu, ale záleží na tom, z čeho a jak je konkrétní služba postavená. V praxi jsme proto původní formální návrh značně proškrtali a provedli řez grafu tak, aby nevznikaly smyčky (viz obrázek 3).



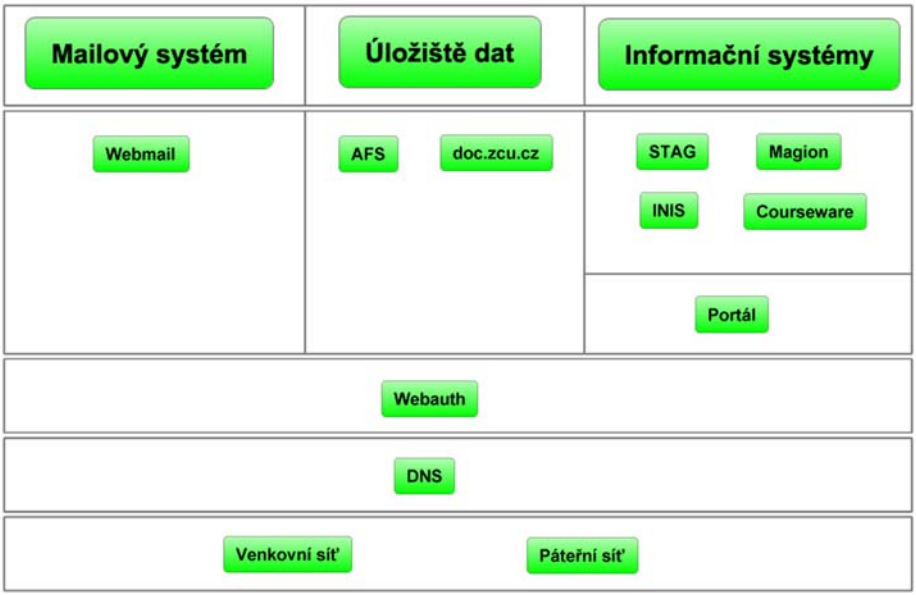
Obr. 3 Optimalizovaná verze návaznosti služeb



Obr. 4 Nově nadefinovaná souhrnná služba

Za technické řešení, vedoucí k dosažení cílů, jsme zvolili několik rozšíření do Nagiosu, konkrétně pluginy NagVis (http://www.nagvis.org) a check_multi (http://my-plugin.de/wiki/projects/check_multi/discussion). Plugin check_multi umožnil definovat logické vazby mezi již zavedenými sledováními v Nagiovi a vytvořit tak provázanou strukturu sledování služeb. Tato vlastnost koneckonců pomůže i administrátorovi, protože nemusí pořád „lovit v paměti“ detaily ke každé spravované službě. Příklad souhrnné služby nadefinované pluginem check_multi je na obrázku 4.

Plugin NagVis přehledně zobrazí stav jakýchkoliv služeb, strojů a skupin. Grafický výstup přes NagVis lze vidět na obrázku 5, online je pak k vidění na stránkách uživatelské podpory ZČU http://support.zcu.cz/index.php/Přehled_dostupnosti_poskytovaných_služeb. Zde v současné době běží výstup z NagVisu přes iframe na wiki stránce. Řešením s lepšími vlastnostmi by bylo použití wiki pluginu z http://www.mediawiki.org/wiki/Extension:NagVis, ale v době implementace nebylo toto dostupné pro aktuální verzi NagVisu.



Obr. 5 Výstup z Nagia pro běžné uživatele

Kvůli snadné konfigurovatelnosti Nagia jsme navíc zavedli do Nagia plugin nConf (http://www.nconf.org), který umožňuje jednoduše přidávat služby i uživatelům, kteří se nedostanou na souborový systém serveru s běžícím Nagiem.

3 Dosažené cíle

Kromě zavedení strukturovaného pohledu na Nagiem sledované služby jsme navíc koupili tři PC s třemi televizními obrazovkami, které jsme umístili na tři pracoviště HelpDesku CIV. Na PC běží operační systém Debian Linux, který je zkonfigurovaný tak, aby po naběhnutí automaticky spustil prohlížeč Mozilla Firefox s výše uvedenou předdefinovanou stránkou. Apache serveru, na kterém běží instance NagVis je nakonfigurovaný pro automatickou autentizaci všech požadavků na adresu se zobrazenou mapou služeb.

Operátoři HelpDesku nyní mohou jednoduše sledovat stav služeb, který jim, jakožto IT amatérům, dá lepší přehled o funkčnosti infrastruktury.

Podle připomínek uživatelů se dále pracuje na přehlednosti, jednoduchosti a přitom výmluvnosti zobrazení stavu služeb. Při každém výpadku služeb také testujeme, jestli zobrazení odpovídá realitě a v případě potřeby návaznosti služeb dále upravujeme.

Zákulisí provozu Seznam.cz

Michal Doleček

E-mail: Martin.Dolecek@firma.seznam.cz

Abstrakt

Během přednášky se podíváme pod pokličku provozování desítek služeb a tisíců serverů společnosti Seznam.cz. Blíže se zaměříme na serverovny (lokality, objem, odběr, zabezpečení atd.), používaný hardware (servery, storage, network), typy softwaru (open-source, proprietární, instalace), aplikace pro podporu provozu (monitoring, management, ...), kdo se o provoz stará a nakonec si ukážeme, co nás v blízké budoucnosti v provozu čeká.

Autor příspěvek nedodal.

Streamovací servery pro použití WEBCAST

Jan Kynčl

E-mail: kyncl@dacc.cz

Wowza Media Server

WOWZA 3 současnosti jeden z nejpoužívanějších multiplatformních streamovacích service server pro LIVE a VOD audio/video a rich internet aplikací. Výhodou tohoto streamovacího serveru

Historie

První verze byla vydána únoru 2007 pod názvem Wowza Media Server Pro 1.0. Byla založena na protokolu RTMP, podporovala streamování audio-video obsahu a poskytovala levnější alternativu k produktu Flash Media Server 2.0.

Verze 1.5, která byla vydána v květnu 2008, přidala podporu RTSP a RTP protokolů a podporu několika kodeků.

Ke konci roku 2009 spatřila světlo světa verze 2.0 a název serveru byl zkrácen na Wowza Media Server 2. Tato nová verze přinesla podporu pro technologie Silverlight, iPhone/iPod, QuickTime a mobilní zařízení na bázi Symbian, Palm webOS, Android, Blackbery a některá další zařízení, jako jsou například herní konzole.

V říjnu 2011 byla vydána zatím poslední verze Wowzy to verze 3.0 tato verze přinesla funkce Live Stream Transcoderu, Network DVR a DRM (Verimatrix a MS PlayReady).

Server je založen na Javě a je pro následujících operační systémy: Linux, Mac OS X, Solaris, Unix a Windows. Wowza Media Server může streamovat do více typů přehrávání klientů a zařízení současně, včetně Adobe Flash Player, Microsoft Silverlight přehrávačem Apple QuickTime přehrávač a IOS zařízení odst. iPad, iPhone, iPod Touch), 3GPP mobilní telefony (Android, BlackBerry OS, Symbian , atd.), IPTV set-top boxy (aminobox, Enseo a další) a herní konzole jako Nintendo Wii a PS3).

Hlavní funkce

- Live streaming videa a zvuku s využitím RTMP, RTP/RTSP MPEG-TS a kodéry
- On-demand video nebo audio streaming a simulované živé streamování pomocí funkce playlistu
- On-line rádio re-streamování ze snímačů starších SHOUTcast/Icecast a serverů
- Interaktivní komunikace: video chat a konferencí, audio/text chatu, whiteboarding (kolaborativní plocha), sdílení obrazovky a online hry

Podporované streaming protokoly:

- Real Time Messaging Protocol (RTMP – Adobe Flash Player)
- Flash HTTP Streaming (San Jose Streaming – Adobe Flash Player)
- Apple HTTP Live Streaming (Cupertino Streaming – iPhone, iPad, iPod touch)
- Smooth Streaming (Microsoft Silverlight)
- RTSP/RTP/MPEG-TS (QuickTime, VLC, mobile devices, set top boxes, encoders)

Podporované audio a video kodeky pro streaming:
(neplatí pro všechny streamovací protokoly!)

VIDEO

- H.264
- VP6 (live only)
- SorensonSpark (live only)
- Screen Shared codec (live only)

AUDIO

- AAC-AAC, AAC Low Complexity (AAC LC), High Efficiency AAC v1 and v2 (HE-AAC)
- MP3
- Speex (live only)
- NellyMoser ASAO (live only)

Podporované audio a video kodeky pro transcoding addson:

Video (decoding)

- MPEG2
- MPEG4 Part 2

Video (encoding)

- H.264
- Audio (decoding)
- MP3
- MPEG1 Part 1/2
- Speex
- G.711 (a-law and mu-law)

Audio (encoding)

- AAC

Transcoding modul je vhodný zvláště pro vstupy live ze zařízení, která nemají nativní h.264 výstup popřípadě pro online transcoding do více kvalit streamu.

Porty použité serverem:

- TCP 1935: RTMP (all variants), RTSP, Smooth and Cupertino Streaming
- UDP 6970-9999: RTP UDP Streaming
- TCP 8084-8085: JMX/JConsole Monitoring and Administration
- TCP 8086: HTTP Administration
- TCP 80: RTMPT, Smooth Streaming, Cupertino Streaming
- TCP 443: RTMPS
- TCP 554: RTSP

Konfigurace celého serveru je přes několik XML souborů.

Licencování

- Developerská licence: 10 streamů + časové omezení zadarmo
- Denní $5
- Měsíční $52
- ECM Cloud $52 jedná se o speciální edici pro Amazon Cloud
- Perpetuální $995

Základní schéma streameru

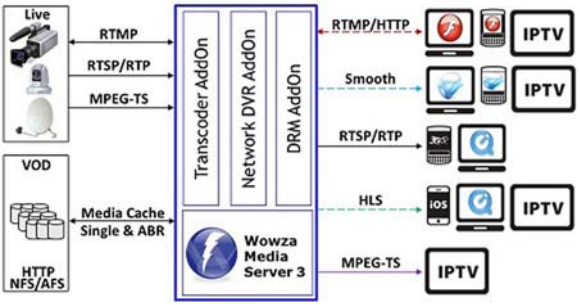


Schéma transconderu

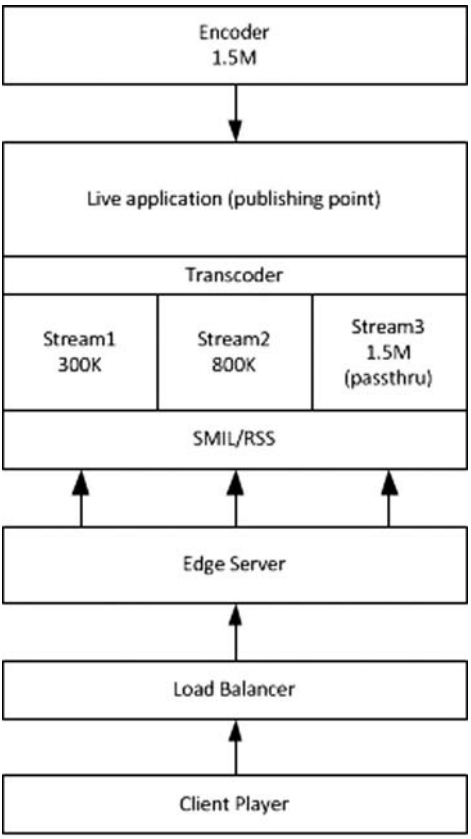


Schéma jednoduchého loadbalanceru

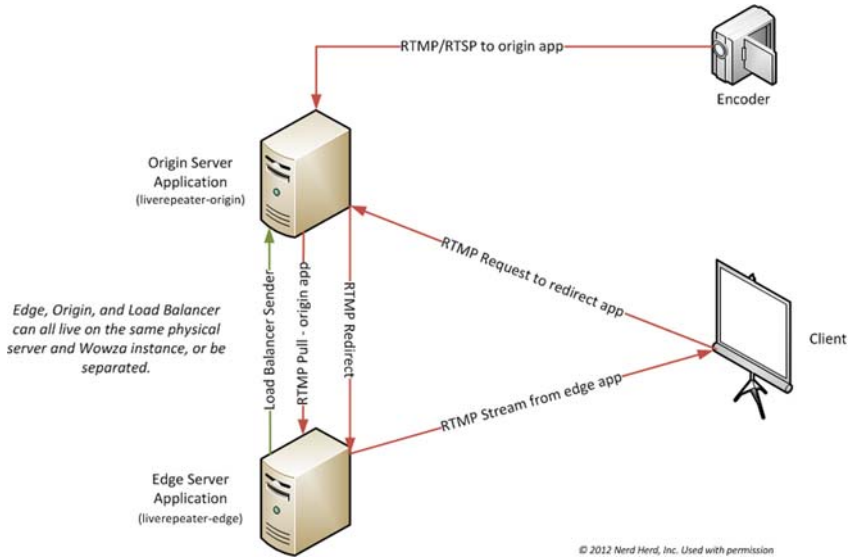
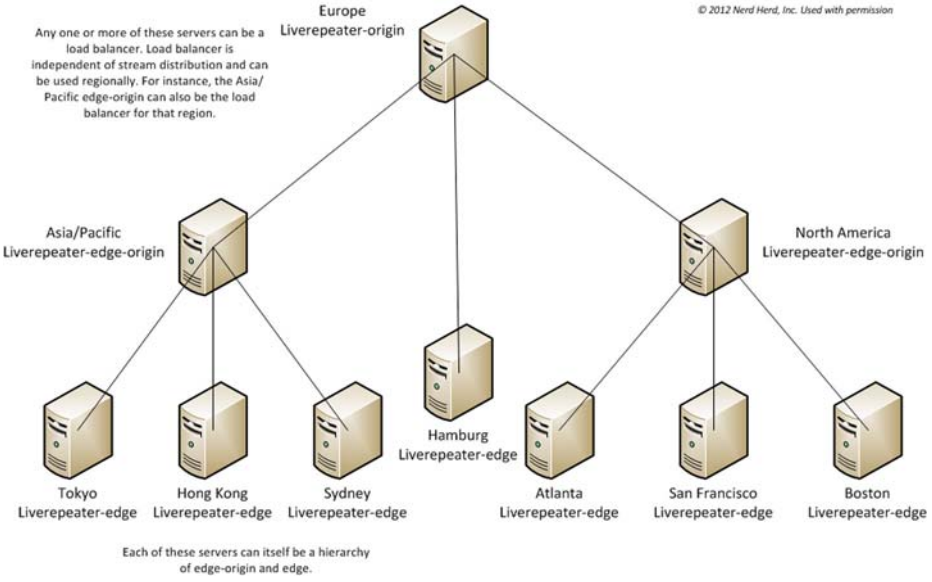


Schéma složitějšího loadbalanceru kde každý server muže být loadbalancer



Adobe Flash Media Server

Původní koncept streamovacího serveru od společnosti Adobe byl určen pro vojenské použití. Konkrétně za účelem videokonferenčního spojení vojáků s jejich rodinami. Od časů této první koncepce uběhlo již několik let a tyto roky byly uvážlivě investovány do vývoje na poli flashového streamování. Streamovací servery Adobe jsou dnes považovány za špičku na trhu. Bohužel většinu potenciálních zájemců o Adobe Flash Media Server dokáže spolehlivě odradit cena tohoto produktu.

Historie

Prvním produktem myslícím na flashové streamování byl Macromedia Flash Player 6 vypuštěný v březnu 2002, který obsahoval veškeré funkce potřebné pro spolupráci s nově připravovaným produktem společnosti Macromedia označeným jako Flash Communication Server MX. Flash Communication Server MX 1.0 byl vydán v červenci 2002 a obsahoval základní objekty pro flashové streamování: NetConection, SharedObject a NetStream. V březnu 2003 byla vydána verze serveru 1.5, ve které byla zahrnuta podpora HTTP tunelování, Linuxu a nová vývojová verze serveru, která byla poskytována zdarma. V listopadu 2005 u příležitosti vypuštění verze 2.0 byl server přejmenován na Flash Media Server z komerčních důvodů a aby jméno produktu lépe definovalo jeho funkce. Verze 2.0 upravovala především serverový ActionScript pro podporu XML, XMLSocket, SOAP a adresářových operací. Poté co byla společnost Macromedia v prosinci roku 2005 zakoupena společností Adobe, bylo rozhodnuto o pokračování vývoje serveru. To vyústilo ve vydání verze 3.0 v prosinci 2007 a poté v lednu 2009 verze 3.5.

Licencování

- Developerská licence: 10 streamů zadarmo
- Perpetuální 1 instance jen live $1 000
- Perpetuální 1 instance plná $4 500

RED5 open source Streamovací server

RED5 je streamovací server napsaný v jazyce Java, distribuovaný pod licencí open source. To je také jeho nesporně největší výhodou oproti placeným profesionálním streamovací serverům. Server Red5 je vyvíjen především komunitou

jeho uživatelů. Aktuální verze serveru je 1.0. Vzhledem k poměrně velké komunitě a stále rostoucímu množství pokusů o komerční využití Red5 serveru je jeho vývoj překvapivě pomalý. Bohužel dokumentace Red5 serveru nedosahuje kvality dokumentace k serverům Adobe a Wowza. Server také trpí množstvím nedodělků a absencí stabilních příkladových řešení. Proto je jeho používání v porovnání s placenými streamovacími servery obtížnější a problematické.

Ale tento projekt má velké ambice!

FFserver open source Streamovací server

Je http/RTSP je multimediální streamovací server pro živá broadcastová vysílání. Podporuje také posun času. Obsahuje ovšem mnoho chyb. Je součástí opensource projektu Ffmpeg.

Slovník pojmů/zkratek

encodér – vysílací stanice nutná pro odesílání (tzv. encoding) živého videa z místa akce směrem ke streamovacím serverům umístěným na páteřní síti.

Dělí se na:
Softwarové např.

- Windows Media Encoder 9 – zdarma pro Win, umí encódovat ve více kvalitách zároveň
- Adobe Flash Live Media Encoder – zdarma pro Win a Mac, umí encódovat ve více kvalitách zároveň, umí průběžně automaticky snižovat kvalitu encódovaného videa v případě poklesu rychlosti uploadu
- Microsoft Expression Encoder – od cca 3 tis. Kč pro Win, podporuje více kamer, titulky atp.
- Wirecast – od cca 8 tis Kč pro Win i Mac, streamuje ve Flashi i Windows media, podporuje více kamer zároveň, titulky atp.

Hardwarové např.

- Teradek Cube – řada kompaktních výkonných HD encodérů, s podporou SDI, HDMI a WiFi, možnost přichycení přímo na kameru, od cca 22 tis. Kč
- NewTek Tricaster – kombinované zařízení střižna + Flash i Windows Media encodér, od cca 160 tis. Kč

- minCASTER – malý HD encodér s podporou SDI, HDMI a WiFi, vlastní baterií a vlastním záznamovým médiem. Cena cca 35 tis. Kč.

Streaming (z anglického stream – proud) je technologie kontinuálního přenosu audiovizuálního materiálu mezi zdrojem a koncovým uživatelem. Streaming může probíhat v reálném čase jako tzv. Live streraming, nebo systémem Video on demand (VOD). V současné době se na internetu pro streraming nejčastěji používají protokoly rtmp, http, rtp, rtsp (přenosové protokoly).

RTMP streaming (Flash Streaming) původně proprietární protokol firmy Adobe (respektive firmy Macromedia, otevřen k licensovanív roce 2009) jedná transportní protokol na bázi TCP protokolu vyvinutý společností Adobe pro použití s flash přehrávačem (v současnosti je to asi nejrozšířenější protokol por streamování videa na Internetu,není podporován firmou Apple v zařízeních IOS:). Umožňuje přehrávat všechny druhy audio-vizuálního obsahu, který je zároveň podporován aplikací Adobe Flash Player. RTMP byl do roku 2009 uzavřenou technologií, poté byl firmou Adobe otevřen a byl tak umožněn jeho další vývoj. RTMP protokol umožňuje plynulou komunikaci a přenos signálu mezi serverem a klientem v přítomném čase. Podporuje až 64 datových proudů (streamů) na jedno připojení. Streamovaný obsah je rozložen na AMF pakety (většinou 64–128 bitů pro video a 64 bitů pro audio). Poté je streamován ke klientovi. Velikost streamovaných částí mezi klientem a serverem může být plynule měněna. Přenos může být i zastaven pokud je to vyžadováno. Komunikace v rámci RTMP protokolu je vždy inicializována klientem.

Druhy RTMP:

- **RTMP (Real-Time Messaging Protocol)** Standardní konfigurace protokolu. Přednastavený na port 1935, pokud není specifikováno jinak.
- **RTMPT (Tuneling Real-Time Messaging Protocol)** Tato konfigurace umožňuje datům, jež jsou přes RTMP odesílána pomocí http, pronikat přes firewall. Protokol je standardně přednastaven na port 80.
- **RTMPS (SSL Real-Time Messaging Protocol)** V této konfiguraci je protokol RTMP odesílán skrze SSL (Secure Socket Layer). SSL je protokol, jenž umožňuje chráněné TCP/IP připojení. Tato konfigurace je přednastavena na port 443.
- **RTMPE (Encrypted Real-Time Messaging Protocol)** Jedná se o kódovanou verzi RTMP protokolu. Je rychlejší než RTMPS, navíc nevyžaduje přednastavení portu.
- **RTMPTE (Encrypted Tuneling Real-Time Messaging Protocol)** Jde o kombinaci RTMPE a RTMPT protokolu. Využívá tunelovou vlastnost RTMPT protokolu a obohacuje ji o kódování RTMPE protokolu. Přednastavení port pro tuto konfiguraci je 80.

RTMP protokol na vnitřní úrovni má podporu RPC procedur, toto se používá při tvorbě interaktivních Rich Internet aplikací (např. audio,video chaty, collaborative black boards,videokonference atd.)

RTMFP proprietární protokol firmy Adobe jedná se o nástupce protokolu RTMP, je založen na bázi UDP protokolu, mezi jeho hlavní výhody patří velmi rychlé navazování spojení a včetně změn IP klienta v případě mobilních zařízení. Zajímavá je podpora multicastu na urovni klienta (Flash Player => 10.0) kde je možné distribuovat data skupině. Zatím je podporován je Adobe Flash Media serverem a velmi experimentálně v open sourcovém RED5 serveru.

Flash HTTP Streaming (Adobe Flash Player, San Jose streaming) – http stream protokol firmy Adobe do flash přehrávačů, tento protokol je velmi podobný http streaming protokolu Apple viz dole, nicméně podobnost neznamená kompaktibilita.

HTTP Live Streaming (HLS, Cupertino streaming) je technologie streaming pro ohraničených (VOD) či neohraničených (LIVE) multimediálních dat. Protokol byl představen společností Apple jako součást balíčku Quicktime a používá se hlavně pro streamování do zařízení s IOS (Iphone, Ipad, Ipod) a to přes video tag HTML5, dotazy v rámci protokolu probíhají nad http protokolem. Možné je také nasazení je do sítí CDN.Videa je také možné v přenosu zašifrovat a to pomocí AES-128 klíčů. Video pak působí jako náhodný shluk dat.

Smooth Streaming JE technologie firmy Microsoft je implememtovaná v IIS media services serveru (4.0.), které umožňuje adaptivní streaming médií klientům přes protokol HTTP. Společnost Microsoft poskytuje hladké streamování Client Software Development Kit pro Silverlight s Windows Phone 7, streaming Porting Kit, který lze použít pro jiné klientské operační systémy, jako je Apple iOS, Android, a Linux. V roce 2010 Microsoft ve spolupráci s výrobcem grafických karet NVIDIA testoval živé streamování 1080p stereoskopické 3D formátu video do PC vybavených NVIDIA 3D technologií.

Real Time Streaming Protocol (RTSP) streamovací protokol firny Real Networks slouží k doručování obsahu formou datového proudu jednosměrového vysílání (Unicast). Jedná se o protokol na úrovni aplikací, který byl vyvinut speciálně pro řízení doručování dat v reálném čase, např. zvukového obsahu nebo obsahu videa. Je implementován prostřednictvím transportního protokolu s opravou chyb. Podporuje ovládací funkce přehrávače (např. zastavení, pozastavení, převíjení zpět a vpřed) RTSP je protokol řízení, který společně s protokolem doručování dat RTP (Real Time Protocol) umožňuje doručování obsahu klientům.

Pokud adresa URL pro připojení používá protokol RTSP[1], vyjedná tento protokol automaticky nejlepší způsob doručování obsahu. Potom nasměruje protokol RTP na doručení obsahu datového proudu pomocí protokolu UDP nebo

[1] Např. rtsp://server/adresar_pro_publikovani/soubor

TCP v síti, která nepodporuje protokol UDP. Standardní port 554 jak pro TCP/UDP).

Protokol používají servery Wowza,FFserver,Realmedia serve, Helix a původní verze Windows media services. Je také velmi často používán IP kamerami pro streaming video (nejčastěji mpeg4, 3gpp) do mobilních zařízení.

Pseudostreaming simuluje chování skutečného streamingu, a to zejména na straně serveru. Svými možnostmi a schopnostmi se zdaleka nevyrovná skutečnému streamingu. Většinou se jedná o http server (Apache, Lighttpd, Nginx) s nainstalovaným modulem mod_flv nebo mod_h264 který umožnuje přecházet v časové ose audiovizuálního záznamu na jakoukoliv pozici bez toho, aniž by uživatel musel čekat na načtení dat celého záznamu. Není to to tak dávno co obsahové servery jako Youtube.com nebo Stream.cz používaly právě toto řešení. Pseudostreaming nelze použít pro šíření LIVE obsahu, ale jen pro VOD.

Digital Rights Management (DRM), což lze přeložit jako „Správa digitálních práv“, je zastřešujícím pojmem pro technické metody, jejichž účelem je kontrolovat či omezovat používání obsahu digitálních médií. Nejčastěji je technikami DRM chráněna hudba, eknihy, obrazové umění, počítačové hry, videohry a filmy. Cílem takové ochrany je především zajistit užívání obsahu v souladu s autorskými právy, respektive v souladu s licenčními podmínkami, vztahujícími se k obsahu (např. zakoupené hudby v podobě hudebních souborů, jež jsou za tím účelem ošetřeny DRM technologií). Nejpoužívanější systémy pro DRM jsou Microsoft PlayReady, Verimatrix a Google Widevine.Nyní se uvažuje nad přidáním této technologie i do HTML5. Adrian Bateman (Microsoft), David Dorwin (Google) a Mark Watson (Netflix) již zaslali organizaci W3C návrh zveřejněný pod názvem Encrypted Media Extensions, který předpokládá využití současného potenciálu HTML5 pro streamování multimediálního obsahu.

CDN – Content Delivery Network je sotisfikovaná služba (kombinace hardware a software) zajišťující distribuci živého či statického videa velkému množství diváků. Využití CDN je nutné pokud je potřeba zajistit vysokou dostupnost videa (servery jsou umístěny v různých lokalitách a u různých internetových poskytovatelů). CDN je vhodná pro poskytovatele videoobsahu, kteří mají více jak cca 1 tis. současných diváků a užitečná v případě, pokud hostují více jak několik stovek GB videa. Samotnou CDN je možné rozšířit o transcoding videa (viz níže). Ve výsledku CDN umožňuje pokrýt vysokou poptávku po videu a zároveň snížit náklady poskytovateli obsahu (za konektivitu a hardware).

VIDEO KODEKY

- **h264** – moderní a zřejmě nejefektivnější formát komprimace videa vhodný zejména pro distribuci videa přes internet a to i do mobilních zařízení. H264 je až o 60 % úspornější než běžný DVD formát MPEG2. V porovnání s MPEG4 nabízí při stejném datovém toku až 4× větší rozlišení.

- **WEBM** je otevřený video formát umožňující video kompresi pro použití HTML5 videem. Vývoj projektu je sponzorován Googlem. Soubor WebM se skládá z video streamu ve formátu VP8 a audio streamu ve formátu Vorbis, uložených v kontejneru založeném na formátu Matroska.

KLIENTSKÝ SOFTWARE/prostředí

- **Silverlight** je to platforma určená pro tvorbu dynamického online obsahu a interaktivní práce s ním. Kombinuje text, vektorovou i bitmapovou grafiku, animace a video.pomocí malé stažitelné komponenty (plug-in) umožní interaktivní ovládání her nebo aplikací a přehrávání multimédií ve většině současných webových prohlížečů (Internet Explorer, Firefox, Safari, Opera, Chrome) na platformách Windows a Mac OS X. Na Linuxu je dostupný pod názvem Moonlight, vyvinutý společností Novell. Tato jinak nepříliš úspěšná technologie zažívá technologický comeback jako jedna z hlavních platforem implementace DRM (Microsoft PlayReady)

- **FLASH** je grafický vektorový program, momentálně ve vlastnictví společnosti Adobe (dříve Macromedia). Používá se především pro tvorbu (převážně internetových) interaktivních animací, prezentací a her. Rozšíření Flashe na internetu pomohla malá velikost výsledných souborů, protože se uchovávají ve vektorovém formátu, a proto ve většině případů vytlačily flashové bannery ty klasické, dříve používané ve formátu GIF. Flash má také vlastní implementovaný programovací jazyk ActionScript, který slouží k rozvinutí všech možností interaktivní animace a vývoji robustních aplikací, v aktuálních verzích je ActionScript poměrně vyspělý objektově orientovaný programovací jazyk.

- **HTML5**

Odkazy a zdroje

[1] http://www.red5.org/ Domovská stránka opensource serveru.

[2] http://www.wowza.com/ Wowza media server

[3] http://www.adobe.com/products/flashmediaserver/fvss/
Adobe Flash media server

[4] http://www.unified-streaming.com/ Další z možných stream serverů

[5] http://www.rtmpd.com/ Další z možných stream serverů

[6] http://ffmpeg.org/ffserver.html
Ffserver aFFmpeg opensource nástroje pro encoding,decoding a streaming

[7] http://www.mr-webcam.com/Wowza.php
Stránka věnovaná rich internet aplikacím

[8] http://www.longtailvideo.com/ JW-player populární flash video přehrávač

[9] http://flowplayer.org/ Flow-player populární flash video přehrávač

[10] http://www.videolan.org/ Pokud neznáte nejste ajťáci

[11] http://www.learningapi.com/jw-player-plugins/
slidesyncslidescroller-example-page/
Ukázka pluginu jak synchronizovat video například s presentací VOD

[12] http://blog.ianbeyer.com/
Blog borce co pro streaming pro desítky nepotřebuje CDN:)

[13] http://cuepoint.org/ Externí titulky pro HTML5

[14] http://www.xuggle.com/ Zajímavý realtime encoder decoder

[15] http://en.wikipedia.org/wiki/Real_Time_Messaging_Protocol
RTMP Wikipedia

[16] http://wiki.gnashdev.org/RTMP
RTMP dissemblován reverzním inženýringem

[17] http://www.telestream.net/wire-cast/overview.htm
Webcast live feeder s online režií

FFserver – streamovací server

Mirek Slugeň

E-mail: thunder.m@email.cz

Abstrakt

FFserver – je streamovací server pro Unix systémy, který umožňuje realtime streamovat audio a video formáty, mezi jeho hlavní výhody patří široká podpora formátů, kompletní otevřenost, malé nároky na HW, podpora unicast i multicast streamování a v neposlední řadě také podpora streamování pro Flash Player včetně h264, přednáška se bude týkat možného využití, zkušeností se stabilitou, příklady konfiguračních skriptů a zevrubně i popisu interního fungování.

Autor příspěvek nedodal.

Jak dostat video na český Internet?

Michal Krsek

E-mail: michal@krsek.cz

Abstrakt

Pro doručování videa v IP/IPv6 sítích existuje mnoho krásných protokolů (například multicast nebo rtp/rtsp). Bohužel v Internetu můžeme na většinu těchto elegantních doručovacích mechanismů zapomenout. Jakým způsobem můžeme doručovat video desítkám tisíc diváků v Internetu? Vyplatí se budovat rozsáhlejší překryvnou infrastrukturu pro doručování videa na tak malém trhu jako je ČR? Tento příspěvek shrne poznatky při budování dvou generací české sítě doručování obsahu (CDN) NACEVI (Národní centrum videa), kterou používají Česká Televize nebo TV Nova.

Autor příspěvek nedodal.

HTML5 a video

Štěpán Bechynský

E-mail: Stepan.Bechynsky@microsoft.com

Abstrakt

Asi nejdiskutovanější částí specifikace HTML5 je element video. Specifikace W3C neobsahuje doporučení, jaký formát videa použít a tak vznikly „formátové války“. V tuto chvíli se pro element video používají tři formáty – H264, Ogg Vorbis a WebM. Z mého pohledu je podpora video formátů ze strany výrobců prohlížečů spíše vedena filozoficky a obchodně než technicky. V semináři se podíváme na jednotlivá úskalí využití elementu video pro přehrávání video obsahu na internetu.

Autor příspěvek nedodal.