

KOMERČNÍ CLOUD, ALTERNATIVA NEBO BUDOUCNOST?

Jiří Navrátil, Pavel Pečiva

Anotace

Ve zdravotnictví, stejně jako v jiných oborech, se výpočetní technika a internet staly jejich integrální součástí. Počet aplikací, které používají VT, dramaticky narůstá. IS v nemocnicích jsou dnes velice komplexní systémy, které mají své koncové body na každém pracovišti. Umožňují dokonalou evidenci událostí, výměnu a sdílení dat i jejich archivaci pro budoucí potřeby. V nemocnicích výrazně roste i počet instalovaných diagnostických přístrojů, které poskytují informace v obrazové formě. Data, která představují jeden snímek, jsou dnes několikanásobně větší než v minulosti. Roste i počet vyšetření. Co se dnes jeví jako akutní problém, je nárůst objemu a uchovávání dat. Bude výpočetní technika instalovaná v nemocnicích postačovat na pokrytí stále narůstajících potřeb? Jednou z aktuálních otázek budoucnosti jistě bude, jak zajistit udržitelnost a rozvoj těchto systémů. Nebude jedním z řešení použití externích služeb, např. komerčních cloudů, které nabízejí nejen dostatečné kapacity pro zpracování, ale i uložení dat?

Klíčová slova

CESNET, GEANT, Internet, cloud, IaaS, PaaS, SaaS

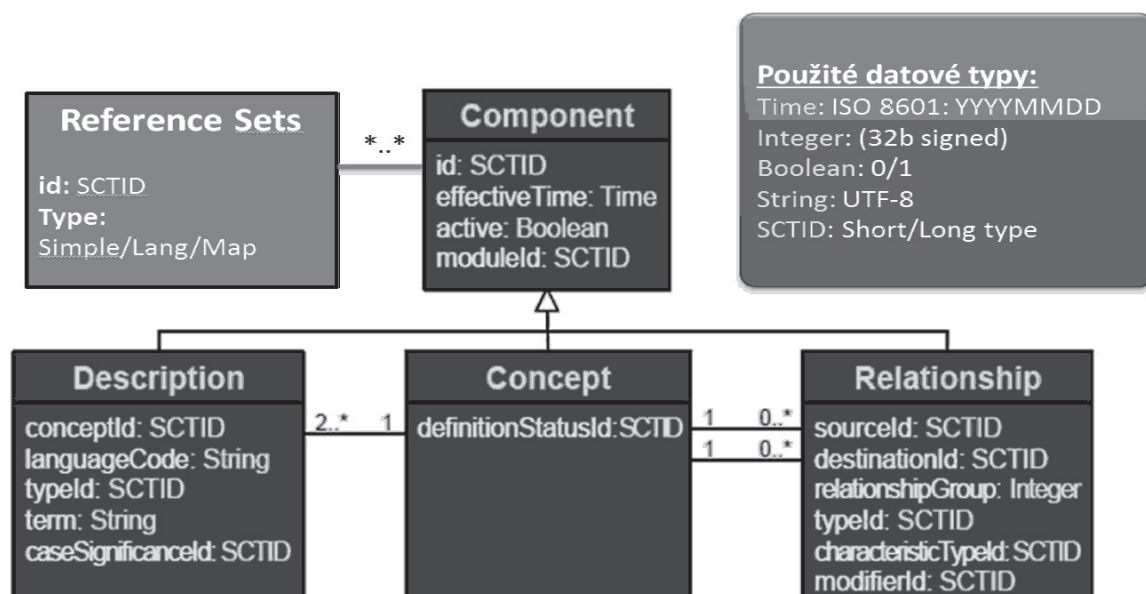
1 Úvod

Ve zdravotnictví, stejně jako v jiných oborech, se výpočetní technika a internet staly jejich integrální součástí. Samotné nemocnice jsou velice komplexní instituce, kde se prolíná mnoho činností, denně jimi projdou stovky nebo tisíce pacientů, kteří absolvují nesčetná vyšetření, podrobují se různým klinickým zákrokům nebo jsou přijímáni k několikadenní léčbě. V nemocnicích jsou provozovány komplexní informační systémy, které mají své koncové body na každém pracovišti, umožňující výměny dat o vyšetřovaných pacientů včetně přenosu obrázků z moderních přístrojů, videokonferenční spojení pro konzultace atd. Počet IT aplikací používaných v nemocnicích rychle roste. Ještě před několika lety se mluvilo o dvou. Jedním z nich byl NIS (Nemocniční Informační Systém) a druhým PACS (Picture Archiving and Communication System), který se zabývá

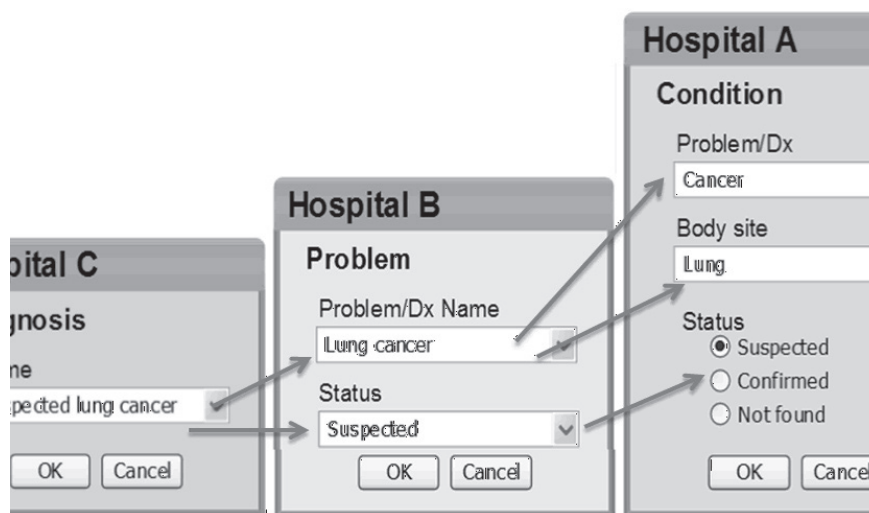
zpracováním a archivací pořizovaných digitálních rtg. snímků a dalších obrazových informací z CT, MRI nebo ultrazvuku. Dnes na otázku, jaký informační systém běží v nemocnici, dostanete odpověď, který máte na mysli? Takže když se podíváme jen na počty IT systémů, které v nemocnicích dnes běží, dostáváme se k počtům kolem několika desítek. Záleží na tom, jak jsou vzájemně propojeny a integrovány. Častým příkladem centrálním IS v nemocnicích je FONS Enterprise, který je velmi komplexní, s plnou podporou procesů, s vysokou dostupností a výtěžností všech evidovaných informací a zahrnující podporu řízení kvality léčby. Vedle něj však musí běžet další specializované systémy, jako LIMS Collector pro zpracování laboratorních dat, genetický systém, systém pro zpracování cytostatik, systém pro zpracování kardiologických dat nebo již zmíněný PACS. Mimo profesní systémy tam musí běžet i další systémy, které jsou potřebné v každé organizaci, jako je personální systém, účetní systém atd., avšak velké nemocnice se neobejdou ani bez systému pro stravování. Co je důležité říci je to, že se provozují na vlastní infrastrukturu, která je v mnohých případech virtualizovaná, a tak umožňuje provozovat každý systém na individuálním virtuálním stroji v těsné spolupráci s dodavatelem těchto systémů.

Z pohledu nároků na objem dat, jejich zpracování a archivaci jsou nejnáročnější systémy zpracovávající obrazová data. To je především PACS. V podstatě se dnes v nemocnicích používají jen tři typy PACS systémů: Maria, AMIS a JiveX. Jejich vlastnosti jsou velmi podobné. Pracují na jednom nezávislém serveru, popř. dvou vzájemně zálohovaných serverech a se samostatným datovým úložištěm v rozsahu několika TB. Data jsou přístupná jak přes specializované grafické terminály, tak prostřednictvím internetu a webového prohlížeče. To umožňuje, aby tyto systémy pracovaly jak pro specialisty, tak pro další lékaře a jejich data byla sdílena více subjekty.

V posledních několika letech se nemocnicích objevují nové a nové přístroje, které kopírují dynamický rozvoj elektroniky. Stejně jako dnešní TV mají mnohonásobně vyšší rozlišovací schopnost než předchozí generace, a to až do úrovně 4K, pracují s 3D obrazem, pořizují HD videozáznamy atd. Pokud v minulosti byly snímky DICOM z MRI používané s rozlišením (256×256 bodů) a CT pracovaly s rozlišením 512×512 nebo 1024×1024 bodů a bitové hloubce šedi mezi deseti a čtrnácti bity (10-14 MB), a byť šlo o stovky až tisíce obrázků, tak to reprezentovalo jen několik desítek GB. Dnes na jeden barevný snímek



Obrázek 1 – Diagnostické přístroje se zobrazením 4K.



Obrázek 2 – Datová centra

4K (3840x2160) a 24 bity pro barevný pixel potřebujeme cca 200 MB. Ať už jsou nebo nejsou tyto systémy integrovány do PACS, tak to samo o sobě vznáší nové požadavky na ukládání velkých dat. Dá se očekávat, že počet diagnostických přístrojů s touto rozlišovací schopností poroste. Tím bude i mnohonásobně vyšší počet vyšetření, a tedy i IS na to budou muset reagovat.

2 Infrastruktura, virtualizace, koncentrace a standardizace

Mnoho nemocnic investovalo do rozvoje infrastruktury hodně peněz (často z Evropských fondů) a v mnoha případech dosáhlo úrovně, která je srovnatelná se zahraničím. Avšak samotný provoz rozsáhlejší infrastruktury a údržba mnoha licencovaných systémů stojí stále víc a víc provozních peněz. Je pravidlem, že IT infrastruktura se musí obnovovat zhruba po 5 letech. Budou nemocnice, ale nejen ty, ale i další organizace v oblasti, které jsou financovány ze státního rozpočtu, připraveny takovou infrastrukturu obnovit a případně rozvíjet? Nebude se muset hledat nějaké jiné řešení, jak se s tím vyrovnat? Nemocnice znají, kolik je stojí dnešní provoz IT infrastruktury, a vědí i kolik budou muset investovat do obnovy. Umí si také představit, bez jakých služeb a informací by se neobešly. V tom se dost podstatně liší od jiných organizací této sféry. Tam ta situace není tak kritická. Mám však pocit, že jen málokdo ví, kolik by je mohlo stát principiálně jiné řešení. Tedy řešení, kdy by infrastrukturu nevlastnily, ale jenom si ji pronajímaly. Tím nemyslíme „řešení na klíč“ a odevzdání provozu cizím subjektům, ale svým řešením v cloudu.

S růstem složitosti a specializace stále víc platí, že odborná práce by se měla svěřit odborníkům. Toto pravidlo může být použito v mnoha rovinách. Dnes už je normální, že si nemocnice nevyrábí vlastní software jako v minulosti, ale používají systémy, které vytvořili profesionálové, osvědčily se a mají certifikaci. Všichni se naučili, že se za to platí nemalé peníze, nejčastěji formou roční licence. To, co platí o aplikacích, ale už neplatí o infrastruktuře. Jak je zaručeno, že instalovaný operační systém je bezpečný? Jsou v něm opraveny všechny bezpečnostní díry? Má nějakou certifikaci nebo byl testován před tím, než se na něm spustil IS? Zatím se jen důsledně trvá na tom, že IS musí běžet na serverech, které jsou instalovány v nemocnici. Už dnes však existují případy, kdy tomu tak není a kdy může jeden server pracovat v nemocnici ve městě X a sloužit i pro nemocnici ve městě Y. Pravda, jedná se o případ provozu v rámci téže organizace nebo komerční skupiny.

Jeden z kroků blízké budoucnosti bude i sjednocování software. To už dnes probíhá v souvislosti s koncentrací a komer-

cializací zdravotnických služeb. Nemocnice v kraji se spojí do jedné, viz KZ a. s. v Severočeském kraji nebo se odpovědní zástupci kraje rozhodnou (jako orgán, který nemocnice financuje), že všechny nemocnice v kraji budou používat jednotný systém a vypíší v tomto směru nové výběrové řízení. Vznikají komerční skupiny nemocnic (AGEL) a další. Ty mají také snahu provozovat všechny nemocnice stejně. Poslední léta ukazují, že výběrová řízení vyhrávají silní hráči se systémy, které se osvědčily. O tom svědčí, že v nemocnicích pracuje stále menší počet různých typů systémů, viz příklad PACSů nebo IS typu FONS Enterprise.

Další krok integrace IT služeb může být posun v oblasti infrastruktury. Jak už bylo naznačeno výše, ve skupině nemocnic nebo v kraji nemusí mít každá nemocnice své informační centrum, ale mohou použít jedno centrální, které bude sloužit všem. Propojovací sítě jsou dnes tak dokonalé, že propojení členů není otázkou techniky, ale je jen otázkou rozhodnutí. Ukazuje se několik možností řešení této integrace. Jednou z nich je vybudování silnějších regionálních center s tím, že se vybaví novou infrastrukturou. Druhá možnost je použití cloudového řešení. Tedy případ, kdy IS poběží na serverech, které nepatří nemocnicím, ale profesionální IT firmě.

3 Cloudové řešení

3.1 Datová centra

Trh s výpočetní technikou je dnes přesycen. Na každé vypsané výběrové řízení dostanete množství nabídek. Provozovatel informačního systému nebo jiného IT systému tak má mnoho možností, jak si pořídit konfiguraci, kterou potřebuje pro své aplikace. Půjde o to, jaké řešení zvolí, zda klasické, kdy si chce pořídit vlastní novou infrastrukturu, nebo se bude snažit použít pro některé části svého IS virtuální infrastrukturu uvnitř nějakého existujícího DC.

DC jsou zřizována velkými IT společnostmi obvykle v místech, kde k tomu byly vhodné podmínky (levná energie, nízké náklady na klimatizaci, rychlý internet do mnoha sítí, levná pracovní síla). Tyto přednosti pak využívají ke svému podnikání v oblasti IT, které je velice efektivní. Budoucí uživatelé DC ani nemusí vědět detaily o tom, kde je lokalizováno, musí být jen dobře dostupné přes Internet. Každé takové centrum má stovky nebo tisíce fyzických serverů, a tak v něm lze paralelně zpracovávat ohromné množství úloh od různých uživatelů. Lze v něm vytvářet virtuální stroje s potřebným operačním systémem nebo konfigurace složitých infrastruktur s desítkami nebo stovkami různých VM, které jsou určeny pro specializované aplikace

nebo uživatele. Virtuální stroje jsou vzájemně zcela separovány, takže uživatel má k dispozici vše, co potřebuje, stejně jako na svém fyzickém stroji. Nikdo se do jeho zpracování nevměšuje a i jeho data jsou zcela separována od jiných uživatelů. Organizace, která bude DC používat, tam nebude vlastnit žádný HW, ale bude si ho jen dynamicky pronajímat. V každém případě bude organizace potřebovat lidi, kteří umí s takovou virtuální infrastrukturou pracovat a budou na ní umět postavit aplikaci, kterou organizace potřebuje. Virtuální infrastruktura je nejen VM s patřičným operačním systémem, ale i vzájemné propojení VM virtuální sítí v rámci DC. Tak může mít i v těchto případech celou infrastrukturu zcela pod vlastní kontrolou. Otázkou je, jak bude organizace důvěřovat provozovateli DC. Ta otázka je však podobná tomu, jak dnes důvěřuje firmě, která mu dodala IS a instaluje ho na jeho vlastním serveru.

Otázka používání DC není aktuální jen pro zdravotnické systémy, ale pro mnoho dalších oblastí nejen nekomerční sféry, která je závislá na centrálním financování. Informatika by se měla začít chápat jako služba, kterou jim někdo profesionálně poskytne. To se může odehrávat na různých úrovních. Třeba tím, že poskytne funkční infrastrukturu, na které si uživatelé budou sami provozovat své systémy. Což se dnes nazývá IaaS (Infrastructure as a Service). Je však možné očekávat stále častější poskytování servisu pro webové systémy, databázové systémy, statistické softwary atd., což se zobecňuje jako PaaS (Platform as a Service) nebo SaaS (Software as a Service). Každá úroveň přináší určité rozšíření spektra služeb. Velmi dobře tuto hierarchii znázorňuje obrázek č. 3. Z něho je i patrné, jakou roli v něm hrají správci data centra (DC), správci jednotlivých VM, vývojáři a uživatelé. Na levé straně obrázku je prodejce služeb ve všech úrovních. To může být např. Microsoft nebo Amazon, tedy společnosti, které nabízejí jak fyzickou infrastrukturu, tak velké množství obecných služeb, které na ní běží. Na pravé straně jsou odběratelé těchto služeb, což mohou být různé IT firmy, které spravují VM, dodávají a instalují speciální aplikační software na vytvořené VM. Zcela nahoře je pak finální uživatel, což vyjadřuje, že se nemusí starat o to, jak a kým je jeho aplikace v systému implementována. Avšak může si zvolit, kterou úroveň si pokryje vlastními lidmi a bude jí mít zcela pod kontrolou. Např. tvorbu a správu VM.

3.2 Jací hráči jsou ve hře

Z firem, které nabízejí takové služby v ČR, můžeme jmenovat např. O2, Radiokomunikace, Zoner Cloud, CloudSigma a jistě

i další firmy. I CESNET nabízí svým uživatelům cloudové řešení na bázi OpenNebula. Před několika lety CESNET spustil také speciální službu datových úložišť (DU), kam si uživatelé mohou ukládat svá data. Původní tři DÚ v Plzni, Brně a Jihlavě budou posílána o další 2 DÚ, protože původní DÚ jsou již zcela plná. Potvrzuje se skutečnost, že uložení dat a jejich archivování je velký problém, který není často správně chápán. Je zcela odlišný od jiných aktivit z oblasti IT, jako je např. komunikace nebo výpočetní kapacita. Komunikace může být rychlá nebo pomalá, výpočty se dají odložit, ale data jsou po prvotním zpracování buď bezpečně uložena nebo mazána. No a právě to rozhodnutí, co s daty a jak dlouho je uchovávat, je na uživatelích. Speciální problém pak nastává, když existuje archiv dat na mediích, která jsou nepodporovaná novou infrastrukturou.

Vedle těchto menších DC jsou k dispozici i prostředky od velkých mezinárodních společností, jako jsou Google, Amazon, Microsoft atd. Jejich velkou předností je také to, že nabízejí prostředky, které jsou v národním prostředí nedosažitelné. Mimo to, že nabízejí možnosti vytvořit rozsáhlé infrastruktury, které mohou být rozloženy teritoriálně po celém světě a využívat tak tuto službu pro nadnárodní společnosti, které působí také v globálním měřítku. Mimo to nabízejí i software a aplikace, které jsou již uzpůsobeny tak, aby mohly efektivně pracovat na VM v těchto DC, což také zjednodušuje práci finálním uživatelům. Cenově jsou jejich služby také často mnohem nižší než služby tuzemských společností. CESNET je partnerem v projektu „Geant cloud Platform“, který nabízí možnost používat přední světové cloudy. O tom bude detailněji pojednávat další odstavce.

3.3 Proces zřízení VM

Mnoho lidí má dnes zkušenosti s VMware, který umožňuje již dlouhá léta vytvářet virtualizované infrastruktury. Řídící software cloudu pracuje se stejnou filosofií jako VMware. Hlavní rozdíl je v tom, že VMware používáme na vlastním HW, zatímco při práci v cloudu pracují s cizím HW a prostředky, které byly vytvořeny předem podle zkušeností, doporučení nebo oblíbenosti.

Vlastnímu vytvoření virtuálního stroje (VM) předchází několik fází a kroků, které vidíme ve všech typech cloudů, i když každý poskytovatel této služby je implementuje trochu jinak. První fáze je přihlášení uživatele k odběru služby. To se obvykle děje přes webovou stránku poskytovatele, kde uživatel vyplní svojí žádost o přístup. Protože se vesměs jedná o placenou službu, je požadován i souhlas s tím, že náklady budou kryty např. kreditní kartou. Pokud je uživatel přijat, dostane do emailu přihlašovací

**) Jest žalostné, jak nejen širší publikum, ale bohužel i samotní vědci se někdy dívají na knihovníka. Knihovník je jim v knihovně asi tím, čím je řekneme ve škole — školník; anebo ani to ne. Prostě zřízenec sázející knihy do polic. Slyšeli jsme nedávno, jak se jeden učenec s úsměškem pozastavil nad tím, že knihovníci potřebují chodit do té své školy dva roky! Když mají i jinak skutečně vzdělaní lidé takovýto názor na poslání a funkci tak důležitého kulturního a pro organizaci vědecké práce významného činitele, jakým je vědecký knihovník, nelze se diviti, že ztrácíme občas odborné bibliotékaře, kteří mají opravdové nadšení pro vědecké knihovnictví, tím spíše, že i o hmotné zabezpečení těchto pracovníků není dobře postaráno.*

Obrázek 3 – Vazby mezi subjekty v rámci cloudu

údaje (uživatelské jméno a heslo). Druhým krokem této úvodní fáze je přihlášení uživatele do vlastního cloudu. I tento krok znamená přístup přes webovou stránku, a to s údaji, které dostal uživatel emailem. Přihlášením se dostane do řídicího panelu (Dashboardu) cloudu. To je opět webová stránka, která obsahuje funkční tlačítka, rolovací menu nebo vyskakovací panely (podle implementace) a s těmi pak uživatel pracuje. Druhou fází je výběr konfigurace budoucího VM. Obvykle má uživatel na výběr počet procesorů a velikost paměti, kterou bude potřebovat. Definiuje si i velikost a typ diskového prostoru, typ a verzi operačního systému. Forma výběru těchto parametrů je různá. Někdy to je dlouhý seznam specifikovaných položek, někdy menu, do kterého se dají napsat potřebné údaje.

Další důležitou fází specifikace je pak definice síťových parametrů a bezpečnostních politik. Tedy pravidel, jak se bude dít k novému stroji přistupovat. Jde o typ IP adresy a definice používaných protokolů, zda to bude přístup jen přes ssh nebo to bude web server, atd. Součástí této fáze je i generace ssh klíčů nebo předání svého obvyklého veřejného ssh klíče centru, které bude zřizovat VM. Pokud je vše hotovo, může uživatel stisknout tlačítko „vytvoř VM“. Pokud byly všechny požadavky v pořádku, řídicí systém začne vytvářet VM a bude informovat uživatele, v jaké je fázi. V několika desítkách sekund je vše hotovo a uživatel se může připojit do VM. To je přeci báječný přístup. Nemusí nic kupovat, nic instalovat a za chvíli práce na svém PC má k dispozici funkční systém v potřebné velikosti. Pro zahájení práce stačí mít jen pár desítek dolarů na kreditní kartě.

VM má IP adresu podle zvolených parametrů na síti, kterou si uživatel také předem vybral. Do nové VM se uživatel připojí některým ze svých terminálů, které má k dispozici. Pro uživatele PC to je obvykle PUTTY nebo MobaXterm. Pro připojení do VM na bázi Microsoftu použije VNC. Ve VM pak operuje stejně jako na stroji, který by měl na stole nebo v nejbližším racku svého domácího centra. Není to nijak složité a drahé, takže to snad za zkoušku stojí. No a pokud už máte běžící funkční VM někde v cloudu, je zase jednoduché tam nainstalovat svoji oblíbenou aplikaci a zkusit si tam pustit i nějaký cvičný provoz. Za měsíc vám poskytovatel pošle fakturu. Já to udělal s aplikací, která používá Linux, databázi mysql a web a měsíčně platím kolem 15 US.

Často je odůvodňováno zachování existujícího stavu bezpečnosti. Vedení organizací věří, že jejich IT specialisté dokáží nejlépe ochránit své systémy. Většina systémů se ale dnes neobejde bez internetu, a tak je jen otázkou, jak jsou tyto systémy provozované s internetem chráněny. Nakolik jsou v systémech opraveny známé bezpečnostní chyby, kolik je v systému bočních vrátek atd. Data se dnes nekradou tím, že se odnese magnetická páska nebo se nahrají na flash paměť, ale přes internet. Pokud je odpovědný pracovník schopen zajistit bezpečný přístup na domácím serveru, pak má stejné prostředky k tomu, aby stejnou úroveň zajistil na virtuálním stroji v DC. CESNET se touto problematikou již léta zabývá a provádí tzv. forenzní testy. Ty ukazují, že jen málo organizací má vše v pořádku. Nejde ale jen o zcizení dat, ale i o zajištění stability chodu systému jako takového, tedy otázky bezpečné dodávky energie atd., což často reprezentuje další náklady. Velmi významným faktem je např. existence záložní infrastruktury pro zpracování v případě havárie.

4 Závěr

Nasazení aplikací do cloudu není možné realizovat paušálně. Použití aplikací v cloudu je spojeno s mnoha aspekty, které je nutné individuálně vyhodnotit pro každý případ. Jde jak o ryze technické parametry, jako jsou požadovaná rychlost zpracování, celkový objem zpracovávaných dat, doba nutná pro přístup k datům nebo doba jejich uchovávání. Ve hře je i reakce systému na požadavky uživatele. Také parametry spojené s bezpečností

rutinního zpracování mají svůj význam. Každý dílčí požadavek má svoji cenu, a tak nakonec i výsledná cena řešení může mít vliv na celkové rozhodnutí, zda řešit problém v cloudu nebo tradičním způsobem, tedy vlastní infrastrukturou nebo třeba jejich kombinací.

Literatura

- [1.] <https://clouds.geant.org/>
- [2.] <https://wiki.metacentrum.cz/wiki>
- [3.] <https://azure.microsoft.com/cs-cz/>
- [4.] <https://aws.amazon.com/>
- [5.] <https://www.orcz.cz/cs/produkty/marie-pacs>
- [6.] https://www.iczgroup.com/pa-reference_category/zdravotnictvi/

Kontakt

Ing. Jiří Navrátil

CSc. CESNET z.s.p.o.
Zikova 4
16000 Praha 6
tel. 224355209
email: jiri@cesnet.cz
<http://www.cesnet.cz>

Pavel Pečiva

KZ a.s. MNUL
Sociální péče 3316 /12A
401 13 Ústí nad Labem
email: Pavel.Peciva@KZCR.EU