Provoz systémových IT služeb v informačním systému Fakultní nemocnice Olomouc

Jaromír Berka

Bakalářská práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jaromír Berka**
Osobní číslo:	**A11768**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Provoz systémových IT služeb v informačním systému Fakultní nemocnice Olomouc**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Analyzujte současný stav IT služeb.**
3. **Popište návrh provozu jednotlivých IT služeb dle požadavku ITIL.**
4. **Navrhněte provozování IT služeb v režimu vysoké dostupnosti.**
5. **Popište technologie nového datového centra.**
6. **Navrhněte design datové sítě pro potřeby provozu ve dvou datových centrech.**
7. **Vypracujte návrh zabezpečení datové sítě před vnitřními útoky.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BRUCKNER, Tomáš, Jiří VOŘÍŠEK a Alena BUCHALCEVOVÁ. Tvorba informačních systémů: principy, metodiky, architektury. 1. vyd. Praha: Grada, 2012, 357 s. Management v informační společnosti. ISBN 978-80-247-4153-6.**
2. **BUCKSTEEG, Martin, Ebel NADIN a Frank EGGERT. ITIL 2011. 1. vyd. Brno: Computer Press, 2012, 216 s. ISBN 978-80-251-3732-1.**
3. **BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. 1. vyd. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.**
4. **MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. Hacking bez záhad. 1. vyd. Praha: Grada, 2007. ISBN 978-80-247-1502-5.**
5. **LUKÁČ, Ľubomír. IT management. 1. vyd. Brno: Computer Press, 2011, 208 s. ISBN 978-80-251-3378-1.**
6. **MICROSOFT. Microsoft TechNet [online]. [cit. 2014-01-27]. Dostupné z: http://technet.microsoft.com/en-US/**

Vedoucí bakalářské práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **7. března 2014**

Termín odevzdání bakalářské práce: **10. června 2014**

Ve Zlíně dne 7. března 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové/bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

ABSTRAKT

Práce reflektuje problematiku provozování systémových IT služeb v prostředí Fakultní nemocnice Olomouc. Prochází postupně celou problematikou zajištění vysoké dostupnosti systémových IT služeb, a to od úrovně vybavení datového centra, až po způsob zajištění systémových IT služeb. Významná část práce je věnována nejmodernějším technologiím společnosti Microsoft, pomocí nichž je vysoká dostupnost zajištěna. Veškeré návrhy vysoké dostupnosti byly ověřeny v testovacím prostředí Fakultní nemocnice Olomouc a mohou být využity v produkčním prostředí.

Práce seznamuje se základními pojmy řízení kontinuity organizace, včetně vysvětlení procesu zajišťující obnovu ICT služeb podniku po havárii. Důležitou částí práce je objasnění zásad vrstvení informačního systému od HW zdrojů po samotnou provozovanou podnikovou aplikaci.

Klíčová slova: Vysoká dostupnost, Hyper-V, Zotavení po havárii, ITIL, Datové centrum, Datové sítě

ABSTRACT

This work reflects problems of running of systematic IT services in the environment of the University Hospital of Olomouc. Step by step it goes through the whole topic of arranging the high availability of systematic IT services varying from the level of equipping of the data centre to the way of procuring of systematic IT services. Great part of the work is dedicated to the state-of-the-art technologies of the Microsoft company with which help the high availability is guaranteed. All proposals for the high accessibility were verified in the testing environment of the University Hospital of Olomouc and these can be further used in the production environment.

The work acquaints with the basic terminology of managing the continuity of an organization, including explanation of the process of securing the renowal of the IT services of the organisation after an emergency accident. A very important part of the work is clarifying the principles of layering of the IT system from the HW sources to the running organisation application itself.

Keywords: High availability, Hyper-V, Disaster recovery, ITIL, Data center, Data network

PODĚKOVÁNÍ

Děkuji Ing. Miroslavu Matýskovi, Ph.D. za cenné rady při vedení bakalářské práce. Mé poděkování patří též kolektivu pracovníků Fakultní nemocnice Olomouc za umožnění zpracovat bakalářskou práci z reálného informačního prostředí nemocnice.

Děkuji rodině, manželce a svému synovi, za podporu a trpělivost, kterou mi během studia poskytovali.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Cílem práce je zpracovat problematiku poskytování IT služeb v prostředí informačního systému Fakultní nemocnice Olomouc s důrazem na vysokou dostupnost služeb a disaster recovery infrastruktury.

Informační systémy byly za několik posledních desítek let vyprofilovány globálně k dominantnímu postavení na poli pořizování, vyhodnocování a nakládání s informacemi. Veškeré agendy jsou postupně transformovány do elektronické podoby, podstatná většina mediální komunikace je tvořena elektronickou formou, rovněž rozmach různorodých sociálních sítí je globálně významný.

Trendu rozmachu informačních technologií není ubráněna ani sféra zdravotnictví, kde probíhá zpracování informací podobného charakteru jako v komerční sféře a expanze specializovaných zdravotnických systémů. Jedná se o systémy sloužící ke zvyšování kvality poskytované zdravotní péče. Pod pojmem kvalita je nutné si představit obsáhlou množinu příznaků, které stojí za úspěšným léčebným procesem se snahou o co nejekonomičtější finanční náročnost.

Oddělení informačních technologií Fakultní nemocnice si uvědomuje důležitost dostupnosti informačních systémů provozovaných v organizaci, z této příčiny probíhají činnosti, které mají za cíl naplnit požadavky budoucího rozvoje informačních systémů využívaných ve zdravotnictví.

Významným krokem z pohledu zajištění výše zmíněných aspektů je výstavba nového datového centra, včetně prvků kritické infrastruktury, návrh modernizace části datové sítě, včetně požadavku připojení nově budovaného datového centra a zabezpečení datové sítě. Dalším významným krokem je budování IT služeb v režimu vysoké dostupnosti s požadavkem na zachování stávajících HW zdrojů z důvodu ochrany předešlých investic do IT.

Návrh provozování jednotlivých IT služeb vychází z konceptu doporučení provozování IT služeb dle metodiky ITIL. Problematika metodiky ITIL je vypracována z důvodu seznámení pracovníků oddělení informatiky a ostatních řídících zaměstnanců nemocnice o vazbách mezi IT a businessem.

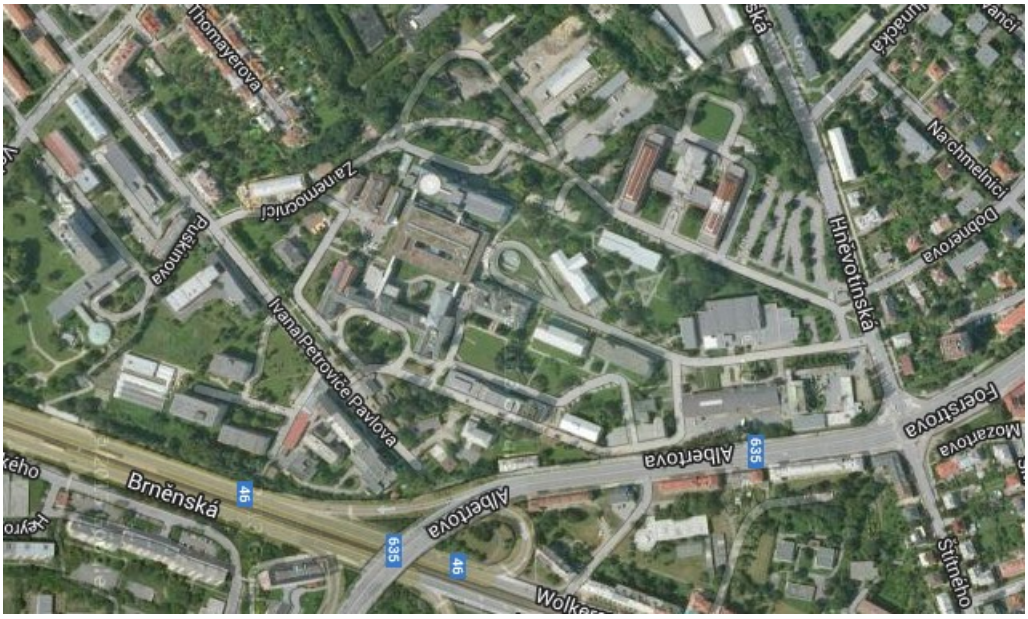
Veškeré zpracovávané návrhy a implementace jsou prováděny a optimalizovány výhradně pro potřeby Fakultní nemocnice Olomouc.

I. TEORETICKÁ ČÁST

1 FAKULTNÍ NEMOCNICE OLOMOUC

1.1 Základní informace

Fakultní nemocnice Olomouc je státní příspěvkovou organizací v přímé řídící působnosti Ministerstva zdravotnictví. Je největším zdravotnickým zařízením v Olomouckém kraji a šestou největší nemocnicí na území České republiky. Areál nemocnice se rozkládá v městské části Nová ulice a je obklopen ulicemi Hněvotínská, Albertova, Brněnská, Vojanova a I. P. Pavlova.



Obr. 1. Areál Fakultní nemocnice Olomouc – upraveno autorem [15].

Fakultní nemocnice Olomouc je významným centrem v mnoha odvětvích moderní medicíny. Ve spolupráci s Univerzitou Palackého významně působí i v oblasti vědy, výzkumu a vzdělávání budoucích zdravotníků.

FAKULTNÍ NEMOCNICE OLOMOUC

Obr. 2. Logo Fakultní nemocnice Olomouc [14].

1.2 Historie vzniku Fakultní nemocnice Olomouc

Historie nemocnice sahá až do roku 1892, kdy císař František Josef 1. společně se Zemským sněmem v Brně dal souhlas s výstavbou někdejších Zemských ústavů v Olomouci. O dva roky později byla zahájena kompozice areálu nemocnice, která průběžně probíhala výstavbou jednotlivých klinik a oddělení až do roku 1930.

Další etapa rozšíření nemocnice probíhala v rozmezí let 1950 – 1984, kdy byla provedena kompozice nových, případně rozšíření již provozovaných klinik a oddělení.

Současný charakter nemocnice byl dotvořen projektem „Modernizace a dostavba Fakultní nemocnice v Olomouci“ realizovaným v rozmezí let 1989 – 2004, kdy byla provedena výstavba centrálního objektu operačních oborů – takzvaného chirurgického monobloku se čtrnácti chirurgickými sály s nejmodernějším technologickým vybavením [12].

1.3 Poskytovaná zdravotnická péče

Fakultní nemocnice Olomouc poskytuje základní, specializovanou a superspecializovanou zdravotní péči o děti i dospělé v celé šíři spektra lékařských oborů. Pacientům poskytuje ambulantní i lůžkovou péči v souladu se současnými dostupnými poznatky lékařské vědy [13].

Tab. 1. Souhrn základních informací o nemocnici za rok 2013 [13].

Počet pracovišť.	52
Počet lůžek.	1 184
Počet zaměstnanců.	3 350
Ambulantně ošetřených pacientů za rok.	776 000
Hospitalizovaných pacientů za rok.	50 000
Průměrná ošetřovací doba ve dnech.	7,4
Počet provedených operací za rok.	16 600

FNOL (Fakultní nemocnice Olomouc) poskytuje zdravotní péči prostřednictvím klinik, oddělení, ústavů a léčebných center. Aktuální seznam provozovaných klinik, oddělení, ústavů a léčebních center je k dispozici na webové prezentaci nemocnice www.fnol.cz v sekci kliniky, ústavy a oddělení.

2 ANALÝZA SOUČASNÉHO STAVU IT SLUŽEB

2.1 Vrstvená systémová infrastruktura

Z pohledu pracovníků nemocnice je pohled na informační systém organizace jednotvárný. Koncový uživatel používá různorodé aplikační vybavení typu např. NIS (nemocniční informační systém), personální agendu, tabulkový procesor, atd. Není zatížen problematikou, kde a jak se aplikace provozuje. Dá se hovořit, že z pohledu uživatele se jedná o konzumaci nějaké IT (informační technologie) služby.

Z pohledu provozovatele infrastruktury je náhled na informační systém komplexní od nejnižší vrstvy, kterou představují služby kritické infrastruktury, až po nejvyšší vrstvu aplikační. V rámci jednotlivých vrstev provozujeme singulární služby související s danou úrovní. Spolehlivost informačního systému se odvíjí od spolehlivosti nejslabšího článku řetězce provozu informačního systému. Během návrhu informačního systému je nutné přihlížet k požadavkům na míru dostupnosti samotné aplikační služby a volit odpovídající způsob zajištění veškerých podřízených služeb aplikační služby. Např. z pohledu spolehlivosti aplikace je rizikové v rámci datového centra opomenout instalaci prvků zajišťující dodávku nepřetržitého zdroje elektrické energie.

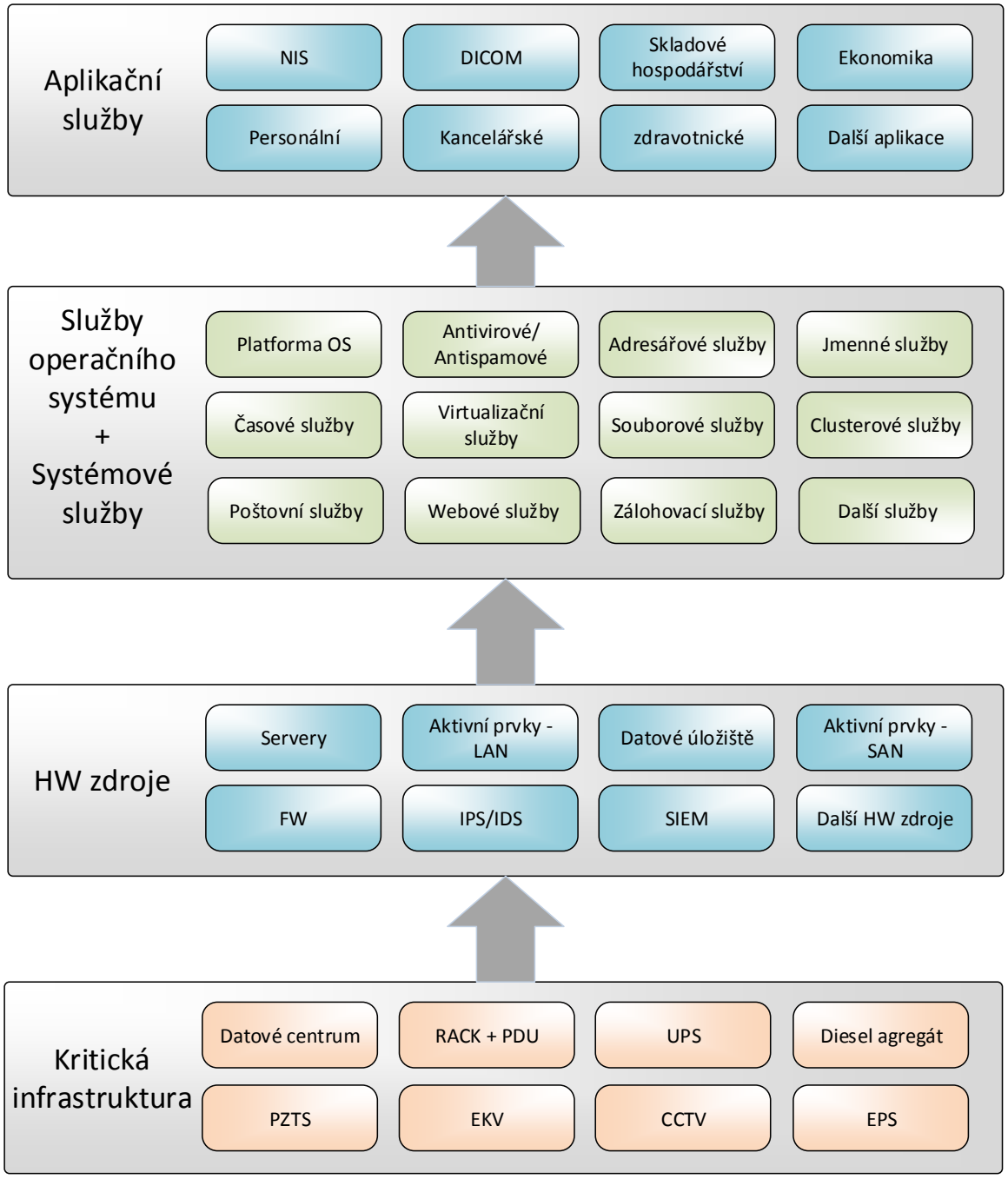
Nejnižší vrstvu tvoří prvky kritické infrastruktury. Jedná se primárně o technologické prostory, serverové rozvaděče tzv. racky, prvky zajišťující nepřetržitou dodávku elektrické energie pomocí UPS (Uninterruptible Power Supply) a diesel agregátu. Doplňkové technologie zajišťující bezpečnost datových center jako je PZS (poplachové zabezpečovací systémy), EKV (elektrická kontrola vstupu), CCTV (Closed Circuit Television), EPS (elektrická požární signalizace), stabilní hasicí zařízení.

Druhou úroveň nazývanou HW (hardware) zdroje tvoří samotné hardwarové vybavení sloužící k provozu informačního systému. Například se jedná o servery, diskové pole, aktivní prvky – LAN (Local Area Network), aktivní prvky – SAN (Storage Area Network), bezpečnostní zařízení – FW (firewall), IPS (Intrusion Prevention System), IDS (Intrusion Detection System), SIEM (Security Information and Event Management), zálohovací zařízení, atd.

Třetí úroveň zprostředkovávají služby operačního systému a systémové služby. Primární službou v této úrovni tvoří instance operačního systému a virtualizační služby. Dále zde spadají veškeré možné systémové služby dostupné na IT trhu např. adresářové služby,

jmenné služby, souborové služby, webové služby, poštovní služby, antivirové / antispamové služby atd.

Čtvrtá finální úroveň je tvořena samotnými aplikacemi např. NIS, DICOM (Digital Imaging and Communications in Medicine), mzdový systém, atd.



Obr. 3. Grafický přehled vrstev systémové infrastruktury.

Práce pojednává o prvních třech nejnižších vrstvách: Kritická infrastruktura, HW zdroje, Služby operačního systému + Systémové služby. Aplikační služby tematicky nespadají do dispozice práce a současně většina provozovaných aplikačních služeb je částečně

outsourcovaná dodavateli aplikačních služeb. Z prostředků FNOL jsou dodavateli využívány služby Kritické infrastruktury, v některých případech HW zdroje a Systémové služby.

2.2 Současný stav služeb Kritické infrastruktury

V současné době jsou v prostředí nemocnice provozována dvě datová centra. Primární lokalita, kde jsou v současnosti instalovány veškeré produkční HW zdroje, se nachází v budově chirurgického monobloku. Chirurgický monoblok byl vystavěn v roce 2004 a během následujících let zde byly přestěhovány a doplněny veškeré informační technologie využívané v organizaci. Moderní označení datové centrum je částečně zavádějící, spíše se jedná o místnost s minimem plášťových otvorů, doplněnou dvěma celoročními klimatizacemi a zdrojem nepřetržité energie. Serverovna je trvale připojena k nemocničnímu diesel agregátu, který zajišťuje elektrickou energii pro celý areál nemocnice. Postupem času byla serverovna dovybavena systémem stabilního hasicího zařízení. Fyzická ochrana prostor serverovny je zajištěna mechanickým zábranným systémem, který je doplněn PZS. Dohled PZS je zajištěn ve spolupráci se soukromou bezpečnostní agenturou, která má své sídlo v areálu nemocnice. V místnosti je umístěno 6 rackových skříní, kde jsou umístěny HW zdroje. Napájení elektrickou energií je realizováno prostřednictvím PDU (Power Distribution Unit) panelů, které jsou vyvedeny ze zdroje UPS.

Záložní serverovna, která byla do roku 2004 jediným místem sdružování informačních technologií, aktuálně slouží pouze k umístění testovacího prostředí. V místnosti chybí klimatizační jednotka a systém stabilního hasicího zařízení. Fyzická ochrana je tvořena stejným způsobem jako primární serverovna.

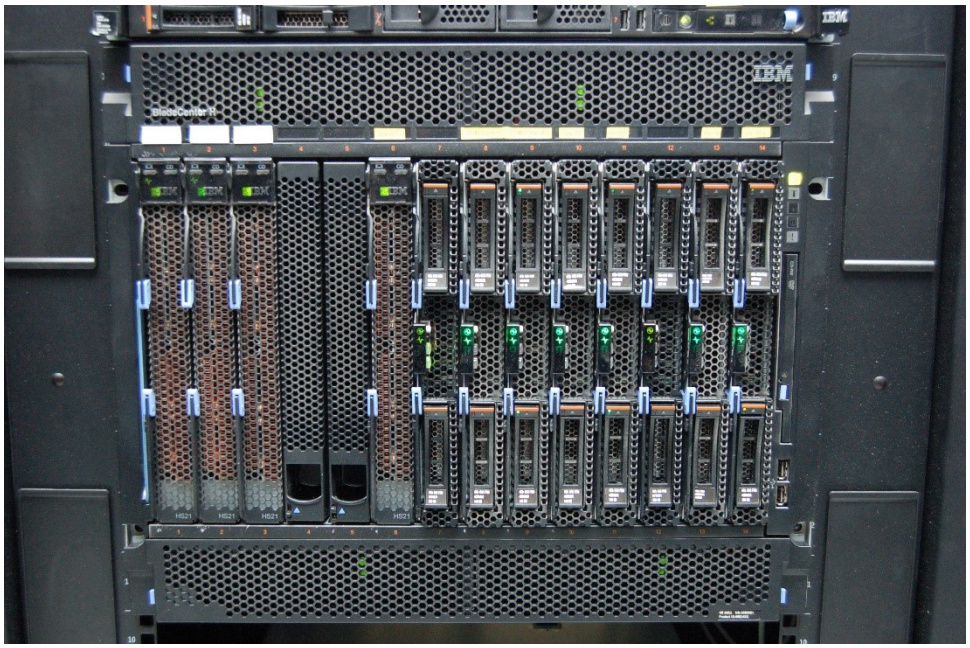
2.3 Současný stav HW zdrojů

Vrstva HW zdrojů představuje veškeré fyzické technologie, které je možné umístit do datového centra. V prostředí FNOL se jedná o fyzické servery, diskové pole, aktivní prvky – LAN, SAN.

2.3.1 Servery

V nemocnici jsou od roku 2004 provozovány servery společnosti IBM. Díky vysoké spolehlivosti produktů IBM byly servery po ukončení servisní podpory v pravidelných intervalech obměňovány. V současnosti jsou nemocnicí využívány servery řady xSeries. Jedná se o typ založený na platformě x86. Většina serverů je ve dvou procesorovém

provedení s různým počtem logických procesorů v závislosti na typu a stáří procesoru. Velikost operační paměti RAM (Random Access Memmory) je v rozsahu 8 – 128 GB RAM v závislosti na provozované službě. Připojení do sítě LAN je realizováno síťovými adaptéry s rychlostí 1 GbE (Gigabit Ethernet). Diskový prostor je dělen na interní / externí. Interní je zajištěn dvojicí pevných disků, které jsou proti výpadku chráněny systémem RAID 1 (Redundant Array of Independent Disks). Interní disk je vyčleněn pro potřeby operačního systému, případně pro služby, které nemají vysoce kapacitní požadavky pro ukládání dat. Externí diskový prostor je realizován pomocí sítě SAN, která zprostředkovává jednotlivé datové oblasti diskového pole konkrétním serverům.



Obr. 4. IBM bladecenter H.

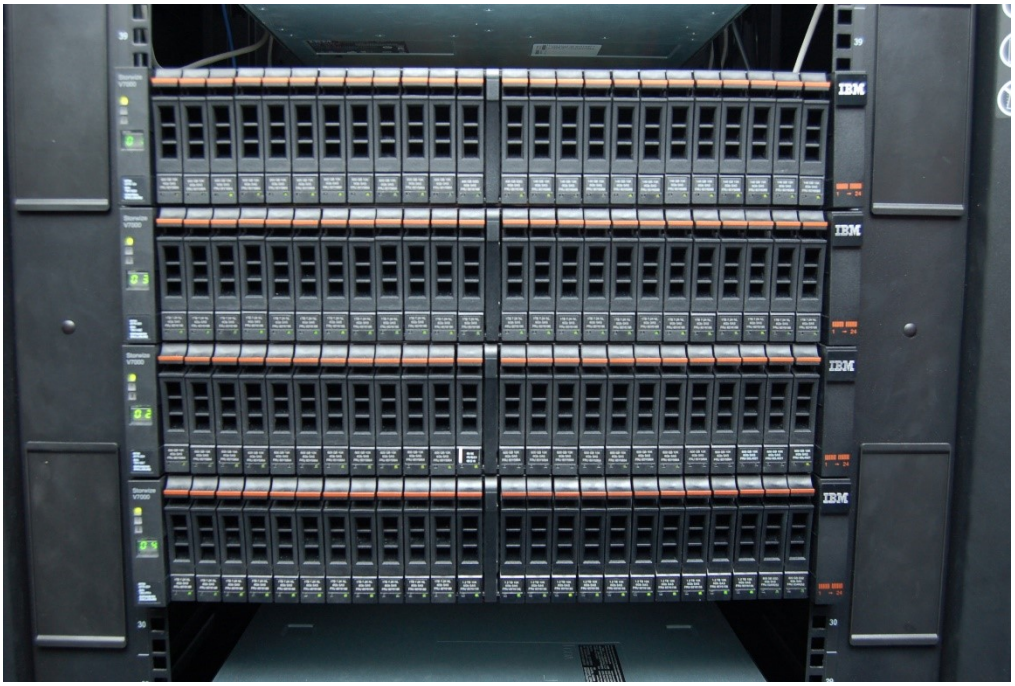
Z důvodu nedostatku volného prostoru v rackových skříních byla provedena změna v konceptu nákupu samostatných serverů na řešení typu blade. Jedná se o řešení IBM bladecenter H, které na prostoru cca 4 fyzických serverů s velikostí 2U (Unit) umožní provozovat až 14 fyzických serverů. Bladecenter obsahuje samostatný agregační LAN / SAN aktivní prvek. V případě přidání dalších serverů do bladecenter se již neprovádí složité připojení veškeré kabeláže nutné pro provoz serveru. Připojení nových serverů může v případě neopatrné manipulace s kabeláží zapříčinit neočekávané výpadky IT služeb [17].

Obr. 5. Stávající datové centrum.

Veškeré servery disponují mechanismy napomáhajícími zajistit nepřetržitý provoz serveru. Jedná se o redundantní napájecí zdroje, systém ochrany diskového prostoru RAID, operační paměti s funkcí ECC (Error Correcting Code), proaktivní monitoring komponent serveru.

2.3.2 Diskové pole

Provozovaná disková pole jsou výrobky společnosti IBM. Provozovány jsou dvě disková pole s různými rolemi souvisejícími s charakterem ukládaných dat. Jedná se o produkční data, která jsou ukládána na novějším diskovém poli IBM Storwize V7000. Zařízení má k dispozici skupinu rychlých disků s 10 000 otáčkami, které jsou výkonově podporovány SSD (Solid State Disk) disky v režimu rychlé vyrovnávací paměti, kdy jednotlivé bloky nejvíce využívaných dat jsou automatizovaně přesunuty na oblast tvořenou SSD disky. Oblast rychlých disků je využívána k ukládání dat generovaných databázovými systémy, virtualizační platformy a služeb, které vyžadují maximální výkon diskového subsystému. Systémy požadující velkokapacitní úložiště mají k dispozici oblast tvořenou levnými vysokokapacitními disky se 7 200 otáčkami. Jedná se o struktury ukládající značné množství informací, např. souborové služby, případně systémy, které nemají požadavek na rychlou odezvu diskového subsystému [18].



Obr. 6. Diskové pole IBM Storwize V7000.

Druhé diskové pole IBM DS 5100 zajišťuje roli ukládání záloh dat z produkčního diskového pole. V případě havárie primárního diskového pole jsou k dispozici data, ze kterých je možné provést zpětnou obnovu ukládaných informací. Je tedy primárně tvořeno nízkootáčkovými vysokokapacitními disky.

Diskové pole je zařízení, které je koncipováno k zajištění bezvýpadkového provozu diskových oddílů. Vysoká dostupnost je zaručena navzájem nezávislou dvojicí řadičů diskového systému, pomocí nichž jsou serverům publikovány diskové oblasti. Diskové oblasti jsou chráněny systémem RAID 5, který je doplněn o několik disků čekajících na poruchu jednoho z využívaných disků. Napájení elektrickým proudem je zajištěno redundantními napájecími zdroji.

2.3.3 Aktivní prvky – SAN

SAN aktivní prvky v prostředí nemocnice slouží k dedikovanému datovému propojení serverů, zálohovacích knihoven a diskových polí. Fyzické propojení mezi zařízeními je provedeno pomocí multimodových optických kabelů a HBA (Host Bus Adapter). Aktivní prvky jsou vybaveny porty umožňujícími zajistit přenos dat mezi dvěma zařízeními rychlostí 8 Gbit/s. Některé servery disponují staršími HBA, které podporují pouze rychlost 4 Gbit/s. Propojení jednotlivých zařízení skrz SAN je zajištěno pomocí zónování, kde jsou definovány matice serverů, diskových polí a zálohovací knihovny. Jeden server ve většině případů

obsahuje jednu dvouportovou HBA kartu, která je pomocí zónování spojena s diskovým polem, který má vždy dva řadiče diskového subsystému. Z důvodu zajištění vysoké spolehlivosti připojení datových oblastí je každý HBA port připojen k oběma řadičům diskového pole. Řadiče diskových polí mají v závislosti na typu diskového pole 2 – 4 porty sloužící k připojení do SAN. Každá datová oblast je k serveru připojena pomocí minimálně čtyř nezávislých cest. V operačním systému se takhle publikovaný disk tváří jako čtyři nezávislé disky. Z důvodu zajištění konzistence dat, je v operačním systému nahrán MPIO (Multipath Input Output) ovladač, který čtyři cesty sjednotí do jedné virtuální. V případě výpadku dílčí části SAN (optický kabel, port na SAN – aktivním prvku, optický převodník, řadič diskového pole) nedochází k výpadku diskových oblastí.

2.3.4 Aktivní prvky – LAN

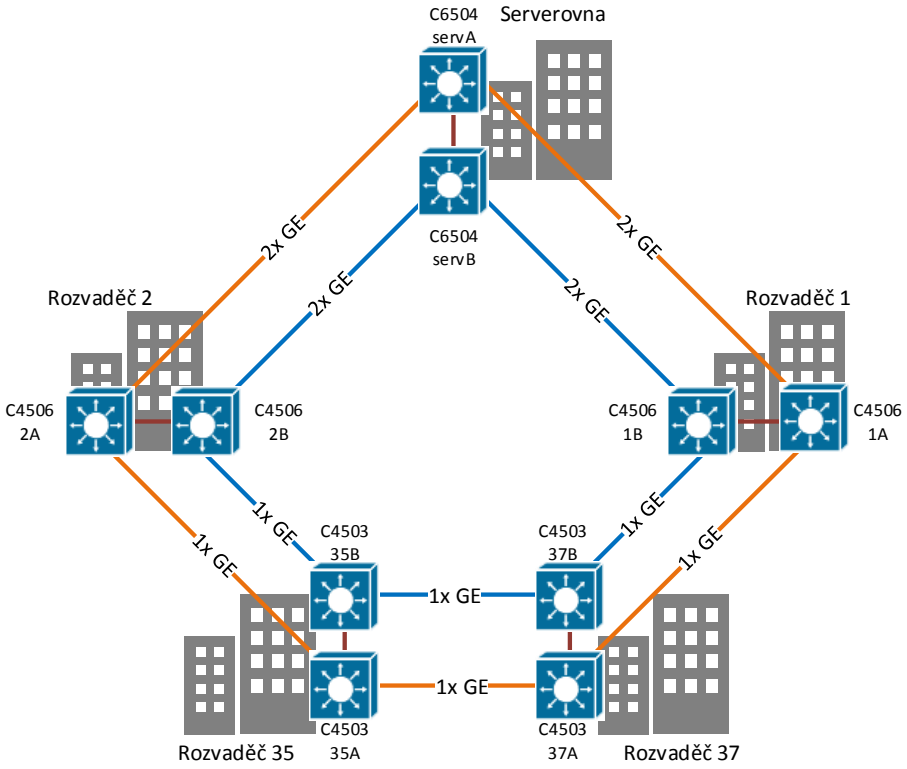
Struktura sítě LAN je tvořena pěti hlavními uzly propojenými do fyzického a logického kruhu. V hlavních uzlech se nachází modulární páteřní L3 přepínače typu Cisco řady 6500 a 4500, které slouží také jako agregační zařízení pro další přepínače, které jsou provozovány v jednotlivých budovách klinik a oddělení. Připojení serverů do LAN je zajištěno pomocí přístupových přepínačů, které jsou zapojeny do hlavních přepínačů Cisco řady 6500. IBM blade chassis je vybaveno 10GE přístupovým přepínačem, který je zapojen do modulárního přepínače Cisco 6500, který je rozšířen o 8x 10GE kartu.

Fyzické propojení jednotlivých uzlů je provedeno pomocí dvou okruhů. Každý okruh tvoří dvojice optických vláken vedoucích z jedné dvojice páteřních přepínačů. Tím je docílena redundance v případě poruchy některého z propojení.

Každá dvojice páteřních přepínačů tvoří samostatnou LAN síť. Síť tvoří dvouvrstvou hierarchii. První vrstva je přístupová, sloužící k připojení koncových zařízení do LAN. Druhá vrstva je distribuční, která propojuje jednotlivé přístupové přepínače v daném uzlu. Páteřní vrstva propojuje jednotlivé páteřní přepínače.

Nad fyzickou lokální sítí je provozováno několik VLAN (Virtual Local Area Network) s lokální působností v jednotlivých uzlech. Jednotlivé uzly jsou odděleny na úrovni třetí vrstvy ISO/OSI (International Standards Organization/Open Systen Interconnection) modelu.

Směrování datové komunikace je zajištěno pomocí protokolu RIP (Routing Information Protocol) verze 1. Úlohou RIP protokolu je předávat informace o jednotlivých sítích přes celou topologii sítě.



Obr. 7. Fyzické zapojení uzlů LAN.

2.4 Současný stav systémových služeb

V prostředí fakultní nemocnice je většina systémových služeb provozovaných na operačních systémech společnosti Microsoft. Rozsah edic je od Windows Server 2003 po Windows server 2008 R2. Dále se vyskytují operační systémy založené na různých edicích Linuxu. Tyto systémy jsou pod správou dodavatelů aplikačních služeb, které v nemocnici provozují.

K autentizaci uživatelů je využívána adresářová služba Active Directory. Adresářové služby jsou společně se jmennými a časovými službami provozovány na třech instancích operačního systému Windows Server 2008 R2.

Již v minulosti byla část fyzických serverů převedena do virtuálního prostředí Microsoft Hyper-V. Virtuální prostředí je konfigurováno v režimu vysoké dostupnosti na úrovni jedné lokality pomocí služby Microsoft FailOver Cluster.

Služba FailOver Cluster je využívána k zajištění vysoké dostupnosti souborových, databázových, DHCP (Dynamic Host Configuration Protocol) a poštovních služeb.

Dále jsou provozovány webové služby prostřednictvím služby IIS (Internet Information Services) a terminálové služby, které jsou rozděleny do dvou terminálových farem s rozdílným operačním systémem, a to Windows Server 2003 a Windows Server 2008 R2.

Zálohování infrastruktury je zajištěno pomocí nástroje IBM Tivoli data protection manager. Virtualizované prostředí je automatizovaně zálohováno pomocí exportu instance operačního systému na souborový systém.

3 NÁVRH PROVOZU JEDNOTLIVÝCH IT SLUŽEB DLE POŽADAVKŮ ITIL

„ITIL (Information Technology Infrastructure Library) představuje ve formě sbírky knih rozsáhlý a všeobecně dostupný návod pro správu služeb IT“ [3]. ITIL slouží ke zvyšování kvality služeb a může se tím stát podstatou pro vyšší uspokojení zákazníků. ITIL zavádí jednotnou terminologii do správy služeb IT, tím dochází ke zvýšení kvality komunikace mezi lidmi pohybující se v IT sektoru. Vznikl a dodnes je postaven na principu nejlepších praktik vycházejících z reálných implementací IT projektů. Historie rámce spadá do počátku 80. let, kdy zaměstnanci veřejné správy Velké Británie hledali možnosti, jak ve státním sektoru snížit náklady na IT. Agentura CCTA (Central Computer and Telecommunications Agency) pokračovala v řešení úkolu a koncem 80. let vydala dokumentaci ITIL. V současnosti je aktuální edicí ITIL verze 3, někdy též označovaná jako ITIL edice 2011. Dle vyjádření Ľubomíra Lukáče je nejznámější a nejpoužívanější verze 2 [6].

3.1 Přínosy ITIL

ITIL zastává názor, že IT služby musí být v souladu s potřebami podniku a musí podpořit klíčové podnikové procesy. Poskytuje podniku informace k využití IT jako nástroj k usnadnění podnikání, reakce na změny trhu, transformaci a růstu společnosti.

Implementace ITIL přináší následující výhody:

- kvalitnější IT služby,
- nižší náklady,
- zlepšení spokojenosti zákazníků díky profesionálnímu přístupu k poskytování služeb,
- zvýšení produktivity,
- lepší využití znalostí a zkušeností,
- zlepšení poskytovaných služeb třetími stranami.

ITIL přináší obecný rámec, jeho procesy je možné / nutné přizpůsobit potřebám konkrétní organizace [20].

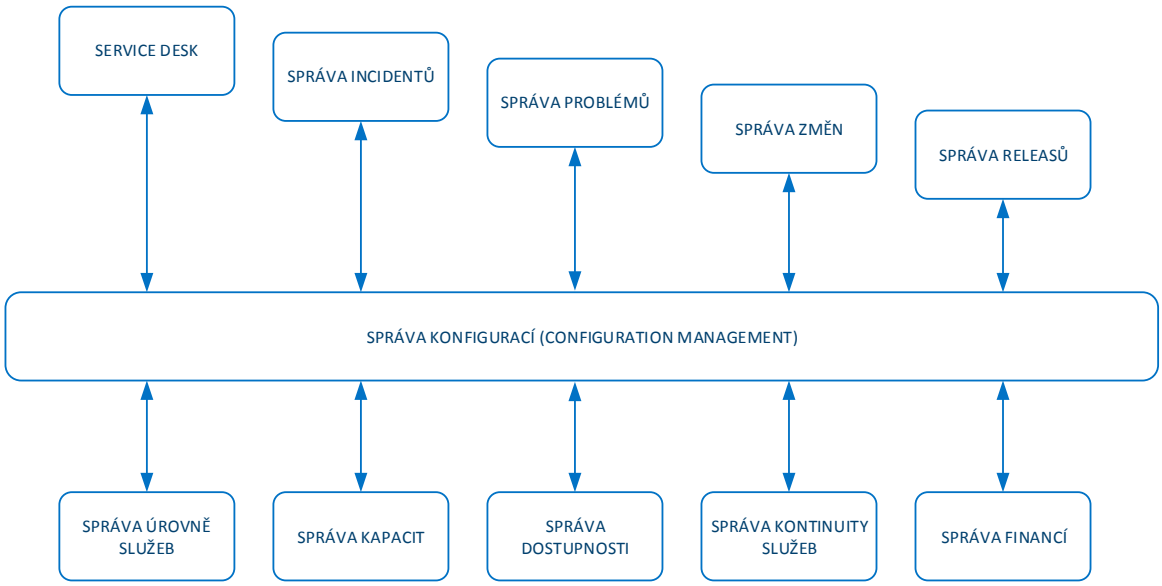
3.2 Procesy ITIL

„Proces lze chápat jako koordinovanou množinu činností, které probíhají za účelem dosažení určitého cíle opakovatelným a měřitelným způsobem“ [3].

Proces je charakterizován určitými příznaky:

- skládá se z množství prostředků (lidé, finanční zdroje, zařízení, technologie, atd.) a činností,
- vyžaduje vstupy a bývá zahájen konkrétními externími aktivitami,
- má výstupy, které představují přidanou hodnotu,
- představuje předlohu jednání pro neustále se opakující činnosti.

Nejvíce důležité části ITIL jsou publikace pojednávající o podpoře služeb a dodávce služeb [6].



Obr. 8. Procesy a funkce dle ITIL verze 2 – upraveno autorem [6].

Procesy podpory služeb jsou:

- správa incidentů,
- správa problémů,
- správa změn,
- správa releasů,
- správa konfigurací.

Dále podpora služeb vystihuje funkci Service desk.

Procesy dodávky služeb jsou:

- správa úrovně služeb,
- správa financí pro IT služby,
- správa kontinuity služeb IT,
- správa kapacit,
- správa dostupnosti.

ITIL verze 3 přináší pohled na řízení IT z pohledu služeb. Rozvinul seznam procesů a funkcí, které obsahuje. Komplexně mění přístup k procesům, které již nejsou centrem dění, ale do popředí se dostává služba. Je rozvržen na části podle fází životního cyklu služby.

	SPRÁVA DOSTUPNOSTI	SPRÁVA MAJETKU A KONFIGURACÍ		
	SPRÁVA KAPACIT	SPRÁVA ZNALOSTÍ		
	SPRÁVA ÚROVNĚ SLUŽEB	VYHODNOCENÍ	SPRÁVA UDÁLOSTÍ	
SPRÁVA FINANCÍ	SPRÁVA DODAVATELŮ	VALIDACE A TESTOVÁNÍ	SPRÁVA PŘÍSTUPŮ	
SPRÁVA POŽADAVKŮ	SPRÁVA BEZPEČNOSTI INF.	SPRÁVA RELEASŮ A NASAZENÍ	SPRÁVA PROBLÉMŮ	MĚŘENÍ SLUŽBY
SPRÁVA PORTFOLIA SLUŽEB	SPRÁVA KONTINUITY SLUŽEB	SPRÁVA ZMĚN	PLNĚNÍ POŽADAVKŮ	REPORTING SLUŽEB
VYTVOŘENÍ STRATEGIE	SPRÁVA KATALOGU SLUŽEB	PLÁNOVÁNÍ A PODPORA PŘECHODŮ	SPRÁVA INCIDENTŮ	NEUSTÁLÉ ZLEPŠOVÁNÍ V 7 KROCÍCH
STRATEGIE SLIŽEB	NÁVRH SLUŽEB	PŘECHOD SLUŽBY	PROVOZ SLUŽBY	NEUSTÁLÉ ZLEPŠOVÁNÍ SLUŽEB

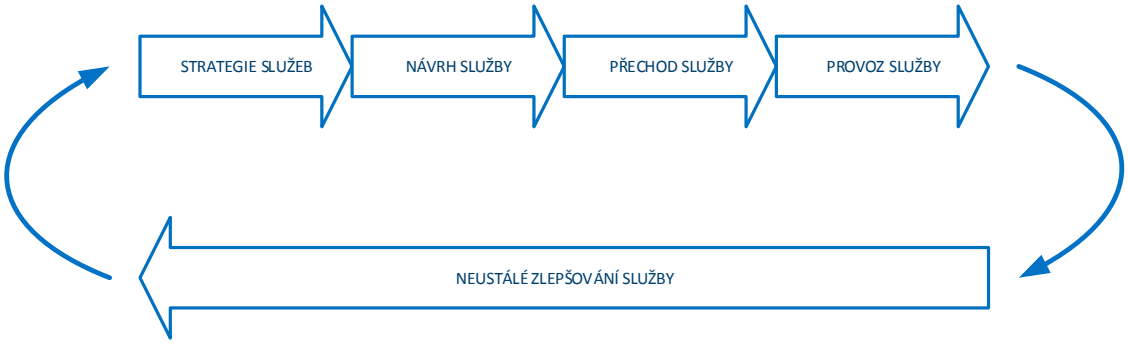
Obr. 9. Procesy dle ITIL verze 3 – upraveno autorem [6].

Fáze služby jsou:

- strategie služeb,
- návrh služby,
- přechod služby,
- provoz služby,

- neustálé zlepšování služby.

Strategii služeb lze interpretovat jako návod, jak se navrhuje, vyvíjí a implementuje správa služeb. Vztahuje se např. k vývoji na domácích a mezinárodních trzích, aktivům služby a implementaci strategie pro celý životní cyklus služby.



Obr. 10. Životní cyklus služby – upraveno autorem [6].

Návrh služby nabízí doporučení pro návrh a vývoj služeb a procesů. Představuje designové metody a zásady, pomocí kterých lze přesunout strategické cíle do portfolia služeb a aktiv služby.

Přechod služby zodpovídá za zavádění nových nebo pozměněných služeb do produkčního prostředí.

Provoz služby se zabývá aktivitami s ohledem na účinnost a efektivitu dodávky a provozu služeb.

Neustálé zlepšování služby poskytuje prostředky a návody pro neustálé zlepšování služeb a všech dříve zmíněných aspektů jako je návrh, zavádění a provoz služeb IT [3].

Nejběžnější metodou, která se na neustálé zlepšování uplatňuje, je takzvaný Demingův cyklus. Často je v odborných kruzích označován jako PDCA - Plan, Do, Check, Act.

Demingův cyklus má 4 kroky:

- plánování,
- implementace,
- kontrola,
- analýza.

Ve fázi plánování, na základě zkušeností s procesem, probíhá výběr naplánovaných akcí, které mají chod procesu zefektivnit. Implementace obnáší nasazení naplánovaných kroků.

V etapě kontroly probíhá monitoring efektivnosti vylepšení. Analýza vyhodnotí úspěšnost navrhnutých akcí. Výsledek vyhodnocení změní definici zadání do PDCA cyklu a vrátí proces do bodu plánování. PDCA cyklus je nikdy nekončící proces [6].

3.3 Služby IT

Služba je nástroj produkce hodnot pro zákazníky. Poskytuje zákazníkům vyjednané výsledky, aniž by tito museli nést zodpovědnost za specifické výdaje a rizika sloučená se službami.

Služba IT je poskytovatelem služeb IT poskytována internímu nebo externímu zákazníkovi. Sestává ze sdružování informačních technologií, personálu a procesů.

Služba IT orientovaná na konzumenta přímo zohledňuje podnikové procesy jednoho či více zákazníků a ve smlouvě o úrovni služeb SLA (Service Level Agreement) by měly být definovány cíle úrovní služeb. Další služby IT, nazývané jako podpůrné, nejsou podnikáním bezprostředně využívány, ale pro provoz služeb orientovaných na zákazníka jsou nepostradatelné.

Klíčová služba poskytuje zákazníkovi relevantní výsledky ve formě žádaného přínosu. Toto je základní část poskytování služeb. Přitom v pozadí poskytují podporu další technické služby IT. Subvenční práce je realizována pomocí služeb, které klíčovou službu rozšiřují či vůbec umožňují, tedy umožňují základní funkčnost. Za tuto funkčnost neplatí konzumenti přímo, ale náklady mohou být poměrně rozděleny [3].

V rámci návrhu IT služeb provozovaných v prostředí FNOL bylo z rozsáhlého množství doporučení ITIL, po konzultaci se zástupci vedení nemocnice a poskytovatelem IT služeb (oddělení informatiky), rozhodnuto, inspirovat se částí ITIL - návrh služeb a jejími procesy správa úrovně služeb a správa kontinuity služeb. Rozhodnutí vychází z cíle nemocnice, který je zvýšení dostupnosti IT služeb s využitím dvou datových center.

3.4 Návrh SLA

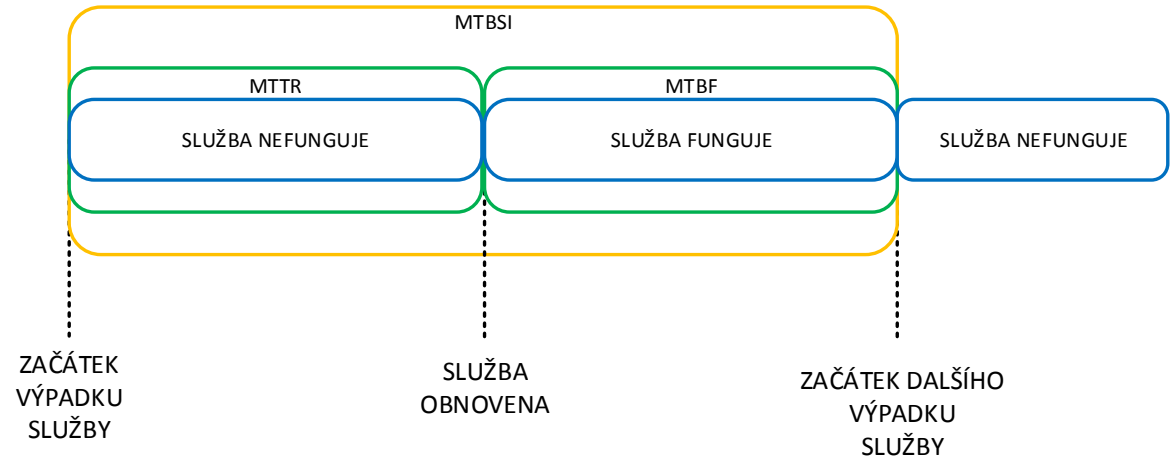
Návrh úrovně služeb přichází ze strany zákazníka v podobě dokumentu, který je pojmenován „požadavky na úrovně služby“, neboli SLR (Service Level Requirement). Nad návrhem probíhá diskuze obou stran a z jejího závěru je vytvořen dokument „dohoda o úrovni služeb“.

Obsahem dokumentu může být následující:

- Přesná definice předmětu SLA.

- Datum zahájení platnosti SLA, datum vypršení a termíny pravidelných revizí.
- Otevírací doby služby – čas, kdy konzument může žádat o změny služby, domluvené reporty a obdobně.
- Otevírací doba podpory služby – čas, ve kterém je dodavatel připraven řešit incidenty vzniklé na službě. Tyto doby můžou být v závislosti na závažnosti incidentu rozděleny na dílčí časová okna. Úplné výpadky služby mohou být např. řešeny v režimu 24x7 a méně závažné incidenty v režimu 8x5 (tedy pouze v pracovních dnech po běžnou 8 hodinovou pracovní dobu).
- Speciální otevírací doba – například dny pracovního klidu.
- Přesná definice dostupnosti služby. V jakých dnech a dobách musí být služba dostupná a na kolik procent. 100% dostupnost nelze v žádném případě dosáhnout. Vždy musí existovat domluvený čas na servisní odstavení služby z důvodu aktualizací, konfiguračních změn atd. Dále je nutné mít rezervu na neočekávané výpadky služby.
- Spolehlivost služby – v rámci SLA je žádoucí měřit dohodnuté veličiny.
    - Průměrná doba mezi poruchami MTBF (Mean Time Between Failures), tj. doba mezi posledním uvedením do provozu po poruše a dalším výpadkem služby.
    - Průměrná doba mezi incidenty MTBSI (Mean Time Between Service Incident), tj. doba od počátku jednoho výpadku služby po začátek dalšího výpadku.
    - Průměrná doba opravy MTTR (Mean Time To Repair), tj. čas potřebný na opravu incidentu. Obvykle se začíná měřit od nahlášení incidentu, ale je přípustná možnost měření incidentu bezprostředně po jeho vzniku.
    - Veškeré zmíněné veličiny je nutné měřit v pravidelných dohodnutých intervalech. Většinou se veličiny vyhodnocují v období jednoho měsíce.
- Podpora uživatelů.
    - Telefonní číslo, e-mailová adresa, odkaz na Service desk.
    - Otevírací doba Service desku.

  - Čas dohodnutý na zvednutí telefonu.
  - Reakční čas.
  - Čas opravy rozdělený dle závažnosti incidentu.
- Výkonnost běhu služby.
  - Reakce systému na různé transakce.
  - Počet transakcí – průměrné hodiny a špičky.
- Výkonnost v provozu dávek – doba trvání zpracování dávky nebo maximální čas jejího dokončení.
- Záložní plány.
- Bezpečnost.
- Platební podmínky.
  - Výpočet platby.
  - Výpočet penále.
  - Období placení.
- Správa změn dokumentu SLA.
- Definice termínů pro revize SLA.



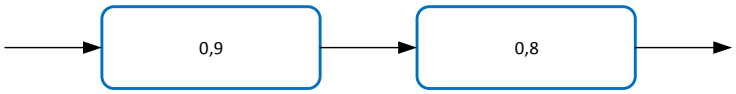
Obr. 11. Průměrná doba mezi poruchami, Průměrná doba mezi incidenty, Průměrná doba opravy – upraveno autorem [6].

Výpočet SLA je závislý na počtu zařízení, které se podílí na zajištění funkčnosti služby a podle varianty závislosti.

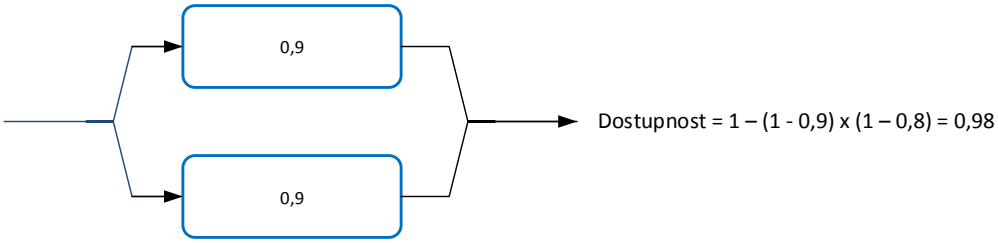
- Varianta A SOUČASNĚ - Služba je závislá na všech zařízeních, v případně výpadku jednoho prvku dochází k výpadku služby.
- Varianta NEBO – Služba je závislá na jednom zařízení, v případě výpadku jednoho prvku nedochází k výpadku služby [6].

$$Skutečná\ dostupnost = \frac{DDDS - DVS}{DDDS}$$

DDDS = Domluvená doba dostupnosti služeb DVS = Doba výpadku služby



Dostupnost = 0,9 x 0,8 = 0,72



Obr. 12. Výpočet dostupnosti – upraveno autorem [6].

3.5 Řízení kontinuity služeb

Řízení kontinuity se rozumí soubor opatření, postihující celou oblast řízení kontinuity procesů organizace pro případ výpadku podpory procesů ze strany ICT. Oblast řízení vychází z britského standardu řady norem BS 25999, které jsou pro specifika řízení kontinuity oblasti ICT doplněny normou BS 25777.

Řízení kontinuity činností profiluje na následujících 6 zásadách:

- Chránit – spočívá v budování robustnosti a odolnosti ICT služeb s cílem zajistit definované dostupnosti služeb.

- Odhalovat – spočívá v proaktivním monitoringu ICT služeb a diagnostice problémů v počáteční fázi vzniku incidentu.
- Reagovat – volba nejvhodnějšího postupu reakce i na méně závažný incident významným způsobem snižuje rozsah výpadku ICT služeb.
- Obnovit – využitím správné strategie při obnově ICT služeb a dat může být zkrácena doba nedostupnosti na minimální časový rámec. Stěžejním faktorem při oživování ICT služeb je přednostní zprovoznění kritických služeb a odložení méně důležitých činností na pozdější období.
- Provozovat – zajistit funkčnost ICT v nouzovém režimu z důvodu provozu kritických služeb s omezením výkonových parametrů.
- Navrátit – definování postupu pro zabezpečení chodu ICT v běžném provozním režimu.

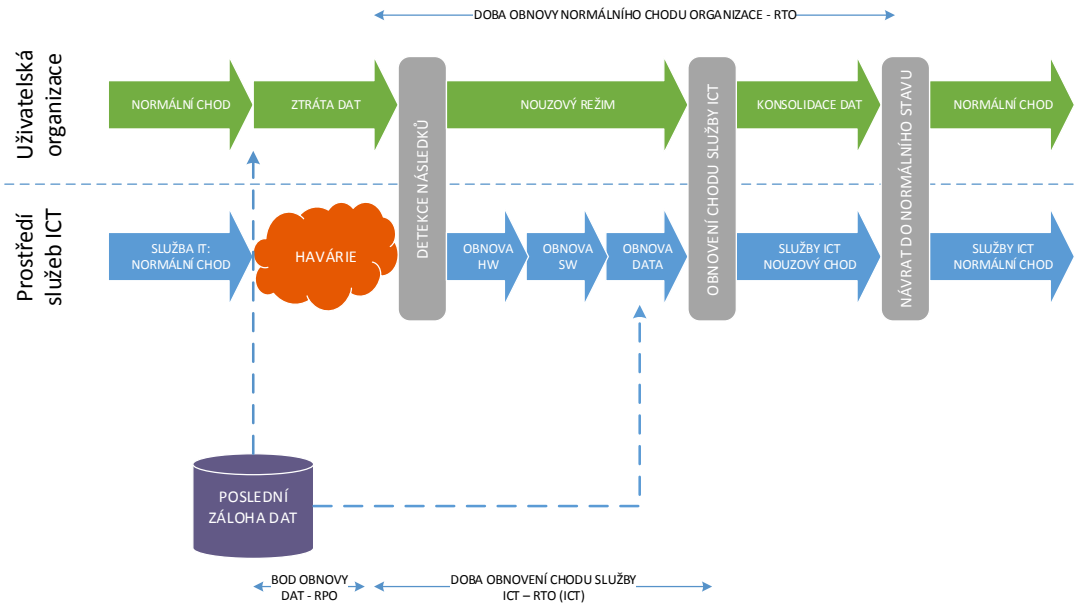
Výše zmíněné zásady je nezbytně nutné zohlednit při provozování ICT služeb. Proces řízení kontinuity je postaven na principu tzv. PDCA, kdy je nutné jednotlivé fáze podrobit procesu neustálého zlepšování [4].

3.6 Postup obnovy chodu organizace

Metoda obnovy chodu organizace je pevně stanovený postup dílčích procesů, které společně zajišťují návrat organizace do normálního chodu.

Z obr. 13 plyne rozdělení nedostupnosti na dvě samostatné úrovně. Uživatelský pohled na nedostupnost se odráží ve snížení komfortu, případně v některých odvětvích až nemožnost zaměstnanců společnosti vykonávat pracovní povinnosti. V procesu obnovy chodu jsou pro uživatele informačních systémů důležité 3 milníky, které rozdělují proces na fázi nouzový režim, konsolidace dat a normální chod.

Nouzový režim chodu organizace předpokládá využití manuálního zpracování procesů bez prvků automatizace poskytující ICT.



Obr. 13. Model metody obnovy chodu ICT [4].

Během konsolidace dat společnosti probíhá zpětný import generovaných dat, během doby běhu organizace v nouzové režimu, do obnoveného systému. Po dokončení konsolidace přechází chod organizace plynule do normálního chodu.

Z pohledu provozovatele ICT služeb je normální chod organizace přerušen havárií, která může být zapříčiněna různorodými událostmi. Rozsah nedostupnosti ICT služeb je v rámci detekce následků diagnostikován. Dle zjištěných skutečností dochází k volbě správného havarijního plánu, popisující chronologicky kroky při obnově HW, obnově SW (software) a obnově dat až po komplexní obnovení normálního chodu ICT služeb v organizaci.

Metodika principu obnovy chodu organizace je značně ovlivněna z definovaných časů položek RPO (Recovery Point Objective) a RTO (Recovery Time Objective). Tyto položky definuje řídící vertikála podniku z důvodu zajištění chodu podniku.

Zkratka RPO skrývá dle tvrzení online verze magazínu IBM Systems [19] význam pro definování maximálně možné ztráty dat organizace v případě vzniku jakékoliv události. Může se pohybovat v intervalu od nuly až nekonečno. V běžných reálných podmínkách se hodnoty definované RPO pohybují v rozmezí minut až několika dní, v závislosti na hloubce integrace ICT v podniku.

RTO dle výše zmíněného magazínu pojem definuje jako maximálně přípustnou dobu od počátku havárie po komplexní obnovení normálního chodu organizace. Může se pohybovat v intervalu od nuly až nekonečno. V běžných reálných podmínkách se hodnoty definované

RPO pohybují v rozmezí minut až několika dní, v závislosti na hloubce integrace ICT v podniku.

Pro správné nadefinování jednotlivých časů RTO a RPO provádí top management podniku hloubkovou analýzu dopadu nedostupnosti business procesů podniku. Dle požadovaných hodnot RPO a RTO provádí provozovatel ICT služeb konkrétní technologické zajištění business procesů organizace. Na trhu ICT je nepřeberné množství způsobů jak technologicky zajistit podporu podnikových procesů systémy s garantovanou dostupností služeb. Na druhé straně, v době hospodářské recese, sílí tlak managementu šetřit finanční prostředky místo investování do složitých IT technologií [19].

4 PROVOZ IT SLUŽEB V REŽIMU VYSOKÉ DOTUPNOSTI

Zajistit provoz IT služeb v režimu vysoké dostupnosti klade na provozovatele IT služeb nemalé vědomostní požadavky. Jak již bylo zmíněno, celková dostupnost IT služeb se degraduje na úroveň nejslabšího článku v řetězci poskytování služby. Vysokou dostupnost je tedy nutné zajistit přes všechny vrstvy infrastruktury.

4.1 Vysoká dostupnost kritické infrastruktury

Fyzické umístění datového centra je důležité kritérium k zajištění vysoké dostupnosti. Ztotožňuji se s názory publikované na odborném portálu SystemOnLine.cz [28].

Není vhodné provádět výstavbu datového centra v následujících lokalitách:

- v lokalitách postižených v minulosti přírodními vlivy (povodně, vichřice, zásahy bleskem, atd.),
- v lokalitách, v nichž hrozí rizika vyplívající z událostí v blízkém okolí (požáry, výbuchy, pád stromu atd.),
- v lokalitách, v nichž hrozí rizika úmyslného poškození vyplívající z blízkosti veřejných prostor.

Samotná budova musí být pro potřeby datového centra projektována, jedná se především o požadavek na dostatečnou nosnost podlahy a střechy, vodovodní instalaci v objektu a instalaci zpětných klapek na potrubí kanalizace povrchové vody vně objektu.

Nepřetržitý zdroj elektrické energie a zálohované napájení pomocí motorgenerátoru musí být bezpodmínečně součástí datového centra v případě, že je kladen požadavek na vysokou dostupnost.

Z důvodu zajištění optimálních provozních teplot systémů je prostor datového centra nutné ochlazovat klimatizačními jednotkami. Běžné kancelářské klimatizace, i s celoročním provozem, nejsou do datového centra vhodné. Dále z důvodu energetických, není žádoucí chladit celou oblast datového centra, ale optimalizovat výdechy klimatizačních jednotek do oblasti, kde technologie nasávají vzduch do svých útrob. Systémy studené a teplé uličky jsou vhodné způsoby chlazení datového centra.

Stabilní hasicí zařízení nemá přímý vliv na dostupnost IT služeb, ale v případě nenadálého požáru může dojít k uhašení ohniska požáru dříve, než dojde k výpadku služby. Z tohoto důvodu by stabilní hasicí zařízení mělo být součástí datového centra.

Napájecí napětí a chlazení mají přímý vliv na spolehlivost a tím i dostupnost infrastruktury. Je nutné minimálně tyto dva klíčové aspekty podstoupit nepřetržitému monitorování funkčnosti. Monitoring musí být doplněn o rozhraní umožňující napojení na operativní dohled datového centra a zasílání oznámení v podobě emailových a SMS (Short Message Service) zpráv. Z důvodu sledování reálné dostupnosti je vhodné integrovat monitoring s aplikací typu Service desk. Jednotlivé výpadky klimatizací, napájecího napětí, atd., jsou formou incidentů zpracovávány a dlouhodobě vyhodnocovány [28].

Datová centra je možné certifikovat. Pro komerční poskytovatele datových center je nutnost certifikaci zajistit z důvodu úspěchu na obchodním trhu. Certifikovaná komerční datová centra vytvářejí zázemí pro informační systémy s určitou garantovanou dostupností.

Standardy datového centra jsou klasifikovány do 4 certifikačních úrovní. Jejich cílem je rozlišit infrastrukturu a topologii certifikovaného datového centra. Uptime Institut je certifikačním orgánem úrovní. Tento americký systém porovnává funkčnost a kompatibilitu datových center. Každá úroveň definuje vyspělost datového centra.

Úroveň 1 - datové centrum s jediným napájecím a chladícím distribučním procesem, bez redundantních prvků, poskytuje 99,6 % dostupnost.

Úroveň 2 - datové centrum s jediným napájecím a chladícím distribučním procesem, ale s podporou redundantních prvků, poskytuje 99,7 % dostupnost.

Úroveň 3 - datové centrum se záložním bezpečnostním systémem, resp. disponujícím více aktivními napájecími a chladícími prvky, včetně redundantních komponent, jehož dostupnost dosahuje minimálně 99,98 %.

Úroveň 4 - maximálně zabezpečené datové centrum, které obsahuje více aktivních napájecích a chladících prvků, včetně redundantních komponent a systémem prevence výpadků s dostupností 99,99 % [10], [34].

4.2 Vysoká dostupnost HW zdrojů

Pojem HW zdroje obsahuje obsáhlou množinu zařízení, které je možné umístit do rackových skříní v datovém centru. Při návrhu vysoké dostupnosti IT služeb je nutné přesně analyzovat

potřeby podniku a poté rozhodnout, které služby budou v režimu vysoké dostupnosti konfigurovány a na kterých zařízeních budou provozovány. Dle poskytované role dělíme HW zařízení na primární a podpůrné. Zařízení ze skupiny primárních zdrojů má na funkčnost IT služeb principiální vliv. V případě selhání kteréhokoliv zařízení, dochází k okamžité nedostupnosti poskytované IT služby. Již při výběru konkrétních komponent je nutné zohlednit požadavek na vysokou dostupnost celého IS (informační systém). Základním požadavkem jsou redundantní napájecí zdroje všech primárních HW zdrojů a redundantní připojení serverů a diskových polí k sítím LAN a SAN.

V případě selhání zařízení zajišťující provoz podpůrných IT služeb nedochází k nedostupnosti IS, ale pouze ke snížení kvality poskytované služby. Jedná se většinou o zařízení provádějící monitoring provozu toku dat v LAN sítích, bezpečnostní monitoring, atd. U těchto zařízení není nutné brát významný zřetel na vysokou dostupnost, nicméně najdou se IS, kde je kladen enormní význam na bezpečnost a v případě nedostupnosti IPS systému, může dojít k odstavení určité části IS.

HW zdroje pro provoz primárních podnikových IT služeb:

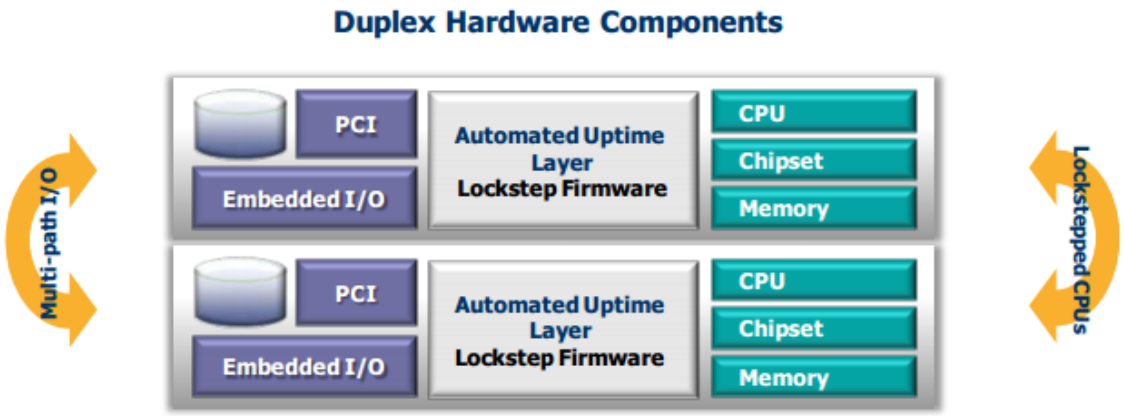
- servery,
- aktivní prvky – LAN,
- aktivní prvky – SAN,
- diskové pole.

HW zdroje pro provoz podpůrných IT služeb:

- SIEM,
- IPS,
- IDS,
- pásková knihovna.

Významný vliv k zajištění vysoké dostupnosti serverové platformy má využití virtualizace. Standartní servery disponují většinou redundantními prvky typu napájecí zdroj, LAN adaptér HBA adaptér. Disponují s proaktivním monitoringem jednotlivých komponent, které v případě problémů mohou vyřadit z provozu např. část paměti RAM.

Na trhu jsou i specializovaná serverová řešení, kde jsou veškeré komponenty zdvojeny. Jedná se o produkty společnosti Stratus řada serverů ftServer Systems. V případě poruchy logické výpočetní jednotky systém automatizovaně odstaví vadnou jednotku. Řešení je vhodné do prostředí, kde je vyžadována dostupnost řádu 99,999 % [31].



Obr. 14. Stratus redundance komponent [31].

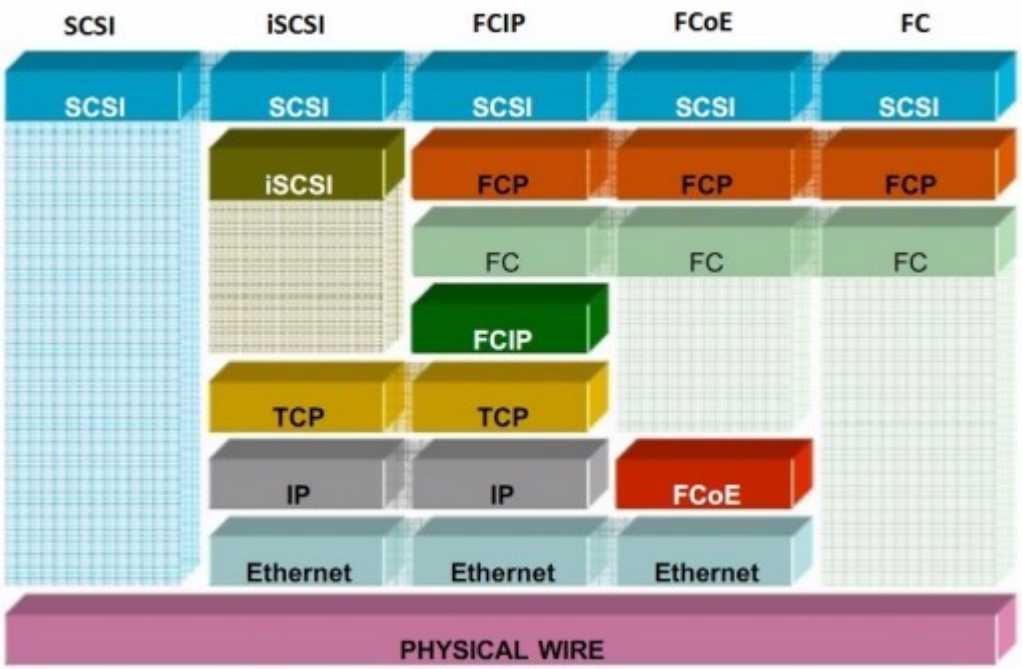
Diskové pole je zařízení sloužící k centrálnímu ukládání dat. Jsou uzpůsobeny pro snadné rozšíření diskového prostoru bez přerušení funkcionality. Obsahují desítky až stovky pevných disků různé technické specifikace. Pro požadované zajištění dostupnosti jsou disky zařazeny do jednotlivých skupin, které jsou chráněny technologii RAID. V případě poruchy fyzického disku jsou přes jednotlivé diskové police vyčleněny pevné disky, které plní funkci rezervního disku, který automatizovaně nahradí chybný disk. Dochází tím ke zvýšení spolehlivosti systému RAID a celkové dostupnosti diskového prostoru. O zápis / čtení dat se stará řadič diskového pole. V závislosti na typu pole jsou řadiče redundantní.

Publikování diskových oddílů serverům je zajištěno pomoci sítě SAN, NAS (Network Attached Storage) a eventuálně díky přímému připojení pomocí SCSI (Small Computer System Interface) řadiče. Přímé připojení má limitující rys v počtu současně připojených serverů k diskovému poli, z tohoto důvodu se v rozšířených instalacích využívá připojení diskových oddílů pomocí sítě SAN.

Diskové pole typu NAS využívá k funkci přenosu dat sdílení na úrovni operačního systému pomocí protokolu NFS (Network File System) nebo CIFS (Common Internet File System). V instalacích vysoce dostupných systémů se využívá omezeně pouze pro potřeby zálohování.

Dle použité technologie může být SAN realizována pomocí FC a iSCSI (internet Small Computer System Interface). Protokol iSCSI se šíří prostřednictvím sítě LAN. Protokol FC

(Fibre Channel) je šířen pomocí dedikované optické sítě v době rozmachu 10 gigabitového ethernetu byl FC protokol modifikován do podoby FCoE (Fibre Channel over Ethernet). Důvodem evoluce je snížení finančních nákladů na stavbu infomačních systémů, díky sdílení sítě LAN pro komunikaci a přenos dat [32].



Obr. 15. Srovnání protokolů typu SCSI [32].

4.3 Vysoká dostupnost systémových služeb

Operační systémy společnosti Microsoft jsou již od verze Windows Server 2000 vybaveny funkcionalitou převzetí služby při selhání. Jedná se o skupinu nezávislých počítačů, které spolupracují na zvýšení dostupnosti aplikací a služeb. Jednotlivé počítače mají přístup k jednotnému úložišti, které je umístěno na diskovém poli. Jsou spojeny interní komunikační linkou, pomocí ní se jednotlivé uzly clusteru vzájemně kontaktují za účelem ujištění, že jednotliví členové jsou funkční. V případě chyby jednoho z uzlů dochází k automatizovanému přesunu služby na funkční uzel. Během přesunu služby dochází ke krátkodobému výpadku služby.

Funkcionalita služeb provozovaných v clusteru je zajištěna pomocí prostředků, které mají svůj vlastní objekt typu počítače v doméně, obdrží svoji vyhraněnou IP (Internet Protocol) adresu. Konfigurace služby je umístěna na sdíleném disku, který je společný pro všechny uzly clusteru. Clusterová služba uzlu, který aktuálně poskytuje vysoce dostupnou službu,

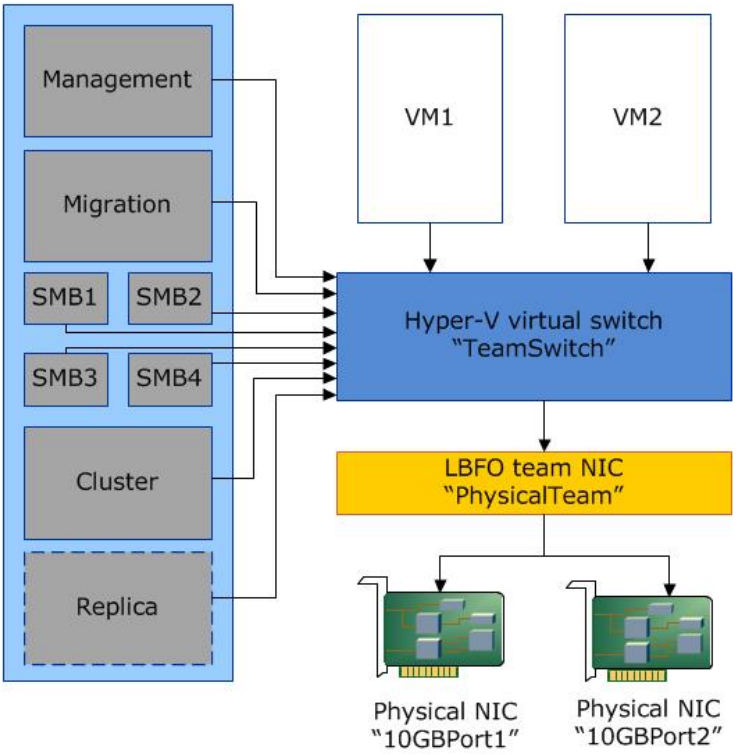
musí zajistit rezervaci a uzamčení disku pro ostatní členy clusteru. Funkcionalitu uzamčení disku musí podporovat diskové pole.

Servery tvořící cluster musí projít validačním testem, který vyhodnocuje HW a SW kompatibilitu. Jednotlivé uzly musí být identické, včetně instalovaných aktualizací operačního systému. V rámci jednoho clustru je možné provozovat až 64 fyzických serverů.

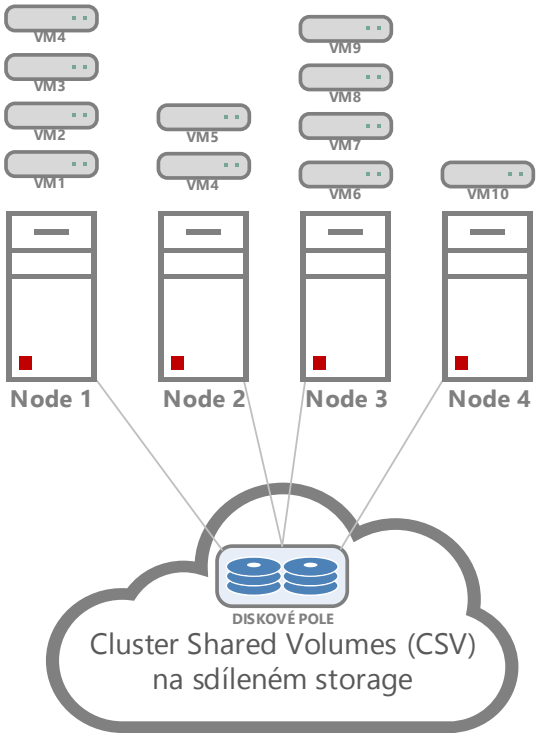
Jednotlivé systémové služby podporují do různé míry nativní provoz ve vysoké dostupnosti, např. poštovní systém Microsoft Exchange Server 2010 provádí rozložení provozu na více instancí poštovního serveru, mezi kterými probíhá neustálá synchronizace dat. Úskalím této metody jsou vyšší náklady vynaložené na licenční pokrytí více instancí poštovního systému. Obdobná situace je u systému řízení báze dat Microsoft SQL Server.

Díky virtualizaci a službě Windows FailOver Cluster je provozován jednodušší způsob zajištění vysoké dostupnosti. Samotná ICT služba je zprovozněna v jedné instanci virtuálního počítače, který je díky FailOver Clusteru vysoce dostupný přes několik fyzických uzlů. Dochází k eliminaci rizika nedostupnosti služby z důvodu selhání hardwarových komponent serveru. V rámci clustru je teoreticky možné provozovat až 8000 virtuálních instancí v závislosti na dostupných hardwarových zdrojích, síťové propustnosti a performance diskového subsystému.

Virtuální instance je možné flexibilně přesouvat mezi uzly clustru bez výpadku informačního systému díky funkcionalitě Live Migration. Díky tomu je možné provádět dynamicky údržbu a patch management fyzických serverů. Zajištění vysoké dostupnosti na úrovni síťové vrstvy obstarává nativní možnost týmu síťových adaptérů. Funkcionalita Hyper-V clusteru je závislá na přítomnosti sdíleného úložiště, které je dostupné všemi nody clustru. V prostředí Windows Serveru 2012 R2 je nově implementovaná možnost použít sdílený diskový prostor formou samba protokolu verze 3.0 [22].



Obr. 16. Přehled principu Hyper-V síťová konfigurace [23].



Obr. 17. Windows FailOver Cluster Hyper-V.

5 VIRTUALIZACE

Za posledních cca 13 let se stala virtualizace intel platformy nezbytnou službou každé implementace systémového prostředí. Díky ní se zásadním způsobem změnil způsob provozování IT služeb. Do té doby běžný informační systém tvořily desítky serverů, ve kterých byly provozované jednotlivé IT služby. Z důvodu nepřizpůsobení jednotlivých IT služeb sdílet společnou instanci operačního systému, se informační systém postupně rozšiřuje o nově implementované servery. Tento trend nese zvýšení nákladů na pořízení, energetický provoz a správu serverů.

Postupem času přichází na trh edice multi-core procesorů, které mají nadbytek reálně nevyužitých výpočetních prostředků. V této době přichází boom virtualizačních technologií. Pohled na provoz informačních systémů se otočil opačným směrem a dochází k postupné konsolidaci serverů. Již není nutné z důvodu nekompatibility IT služeb nakupovat nové servery, ale vytvořit server virtuální, který využívá výpočetního výkonu své „matky“. V závislosti na výpočetním výkonu „matky“ je možné na jednom fyzickém serveru provozovat kolem 10 – 20 virtuálních instancí.

Pojem serverové virtualizace není výjev moderní doby, počátky serverové virtualizace se datují k roku 1961, kdy společnost IBM představila Compatible Time Sharing System umožňující sdílení procesorového času. V počítačích typu Mainframes byl provoz virtuálních instancí umožněn již v roce 1980. Počítače typu Mainframe jsou schopné hostovat množství virtuálních instancí, které jsou označovány názvem partitions [5].

5.1 Motivace proč virtualizovat

Hlavním motivačním faktorem je:

- Úspora finančních prostředků vynakládaných na provoz informačních systémů. Výdaje jsou optimalizovány díky konsolidaci serverů a snížení spotřeby elektrické energie.
- Zjednodušení řízení kontinuity organizace a obnovení normálního chodu podniku po havárii.
- Současný běh více typů operačních systémů na jednom serveru. V rámci provozu jednoho fyzického serveru je zabezpečen provoz různých operačních systémů.
- Striktní vzájemná izolace jednotlivých instancí virtuálních serverů.

- Možnost automatizovaného přenosu již provozovaného informačního systému v rámci fyzického serveru do virtuálního prostředí.
- Správa testovacího prostředí, během pár minut je možné provést otisk produkčního informačního systému do testovacího prostředí a provádět testování různorodých scénářů [5].

5.2 Virtualizační architektury

V prvotní fázi vzniku virtualizace pracovaly virtualizační produkty přímo pod operačním systémem. Během postupné evoluce byl tento režim, z důvodu velké výkonové režie, opuštěn a nahrazen odlehčeným operačním systémem pro potřeby virtualizace tzv. hypervisorem. Někdy též označován jako Virtual Machine Management. Hypervisor obhospodařuje správu paměti, přiřazení výpočetního výkonu procesoru, obsluhuje vstupně/výstupní operace jednotlivých virtuálních serverů.

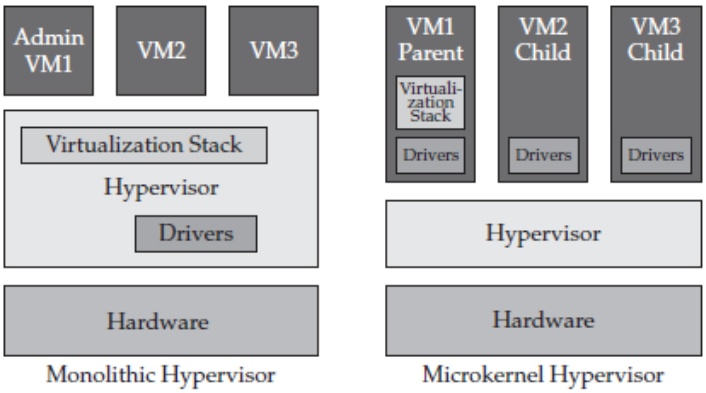
Běžně se využívají tři způsoby provozování hypervisoru:

- Softwarová emulace hardwaru – výhodou této metody je absolutní nezávislost na hardwaru. Nevýhodou velká výkonová režie hypervisoru.
- Virtualizace s hardwarovou asistencí – s rozmachem virtualizačních technologií jednotliví výrobci hardwarových prostředků cílí své zájmy nabídnout podporu virtualizace na úrovni některého typu hardwaru např. procesory, chipsety, paměti, síťové karty a host bus adaptéry. To má dopad na zvýšení výkonnosti hypervisoru z důvodu minimalizace režie.
- Paravirtualizace – způsob vyžaduje zásah do operačního systému provozovaného ve virtuálním prostředí. Do jádra systému se zanesou rutiny, které přesměrovávají určité instrukce do hypervisoru.

Hypervisory můžeme rozdělit na dva hlavní typy dle architektury provedení jádra hypervisoru.

- Monolitický – je instalován přímo na hardwarovou vrstvu. Do vrstvy hypervisoru jsou integrovány nástroje třetích stran a ovladače potřebné pro běh virtuálního počítače.
- Mikrojádro – stejně jako u monolitického je hypervisor instalován přímo na hardwarovou vrstvu. Změna je ve způsobu práce s nástroji třetích stran a ovladači,

které jsou přesměrovány do jednotlivých virtuálních serverů. Výhodou je vyšší úroveň stability virtualizační vrstvy [5].



Obr. 18. Architektura provedení jádra hypervisoru [5].

5.3 Přehled na trhu serverové virtualizace

V současné době je na trhu k dispozici nepřeberné množství produktů nabízející řešení serverové virtualizace. V podnikové sféře českých firem jsou nejčastěji využívané produkty společnosti VMware, Microsoft a Citrix. Jediná společnost VMware se zcela koncentruje pouze na produkty týkající se virtualizace. Společnosti Microsoft a Citrix nabízí virtualizace jako podporný nástroj svých primárních produktů.

Produkt společnosti VMware vSphere je na poli enterprise virtualizace považován za obecný standard. Vůči svým konkurentům má technologický náskok pramenící z prvotního uvedení svého produktu na trh již v roce 2001. V současné době náskok významně dotahuje společnost Microsoft. Enterprise verze virtualizačního nástroje vSphere je licenčně zpoplatněna. Konkurence v podobě korporací Microsoft a Citrix nabízí enterprise virtualizační technologii zdarma. VMware v rámci produktu vSphere dává k dispozici nástroje sloužící k monitoringu a ke správě virtualizovaného prostředí. Dále jako jediný podporuje všechny tři virtualizační architektury.

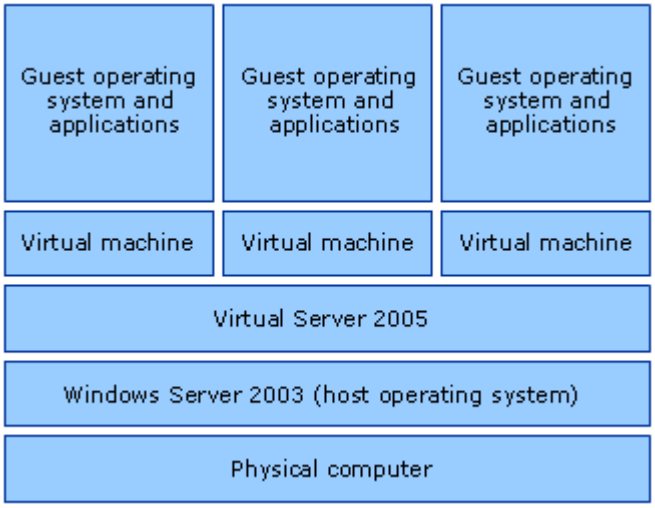
Společnost Microsoft k zajištění monitoringu a komplexní správy virtualizovaného prostředí využívá samostatný produkt System Center. Společnost Citrix svůj produkt XenServer postavila na volně dostupném řešení Xen. Jedná se o open source virtualizaci vyvíjenou na půdě Cambridge univerzity. Stejné řešení využívá i společnost Oracle pro svůj OracleVM. Microsoft a Citrix podporují pouze architekturu virtualizace s hardwarovou asistencí a paravirtualizace. Z tohoto důvodu je nutné využívat pouze servery nativně podporující virtualizaci [29].

6 MICROSOFT HYPERVISOR

6.1 Virtual Server 2005

Virtualizační platforma společnosti Microsoft byla prvotně uvedena na trh v roce 2004 produktem Virtual Server 2005. Produkt využíval pouze prostředků emulace HW zdrojů a neměl přímý přístup k hardwarové vrstvě. Nativně neumožňoval provoz virtuálních serverů v režimu vysoké dostupnosti pomocí služby převzetí služby při výpadku.

Z důvodu spolupráce s hostovaným operačním systémem Windows Server 2003, jsou jednotlivé virtuální instance serverů limitovány velikostí operační paměti na 3,6 GB RAM. Celkový počet virtuálních serverů je v rámci Virtual Serveru 2005 omezen na 64 instancí. Architektura virtuálních strojů je pouze 32-bitová [26].



Obr. 19. Architekura Virtual Server 2005 [25].

6.2 Hyper-V

S příchodem operačního systému Windows Server 2008 společnost uvádí nový virtualizační produkt Microsoft Hyper-V. Hypervisor je v rámci licence operačního systému k dispozici zdarma. V dnešní době je aktuální verze Hyper-V 3.0 v rámci serverového produktu Windows Server 2012 R2.

Hyper-V oproti Virtual Serveru má již přímý přístup k hardwarové vrstvě. Problematika výkonových omezení je v současnosti odstraněna. Definované limity Hyper-V jsou pro potřeby dnešních implementací informačních systémů reálně nedosažitelné.

Hypervisor umožňuje spravovat 320 logických procesorů, umí adresovat 4 TB operační paměti. V případě nasazení v režimu vysoké dostupnosti umožňuje vytvořit Cluster o celkovém počtu 64 uzlů.

Samotná instance virtuálního serveru je omezena na 64 virtuálních procesorů a 1 TB operační paměti. Možnost připojit až 255 virtuálních disků každý o velikosti až 64 TB. To je dostatek výpočetního výkonu i pro Enterprise databázové řešení.

Pro potřeby síťové komunikace je možné využít až 12 virtuálních síťových adaptérů. Z důvodu zajištění různorodých scénářů implementace je možné přesměrování fyzických FC adaptérů do virtuálního prostředí. Tím dochází k přímému přístupu do fyzické SAN architektury.

Virtualizace Hyper-V využívá funkcionalit systému Windows Server 2012 R2, který zohledňuje rostoucí poptávku trhu po uživatelsky dostupném řešení vysoké dostupnosti informačních systémů. Společnost Microsoft v nedávné době spustila cloudovou službu Windows Azure, která ke svému běhu primárně využívá funkcionalit Windows Server 2012 R2 a Hyper-V.

V rámci řešení virtualizace Microsoft Hyper-V jsou v následující tabulce uvedeny podporované klientské operační systémy.

Struktura virtuálního počítače je na diskovém oddílu uložena v podobě XML (Extensible Markup Language) souboru, který popisuje technickou specifikaci virtuálního počítače. Datová část virtuálního počítače je uložena v souboru VHD/VHDX (Virtual Hard Disk) [21].

Tab. 2. Přehled podporovaných hostovaných operačních systémů – upraveno autorem [21].

Hostovaný operační systém	**Maximální počet virtuálních procesorů**
Windows Server 2012 R2	64
Windows Server 2012	64
Windows Server 2008 R2 (SP1)	64
Windows Server 2008 (SP2)	4
Windows Home Server 2011	4
Windows Small Business Server 2011 Essentials edition	2
Windows Small Business Server 2011 Standard edition	4
Windows Server 2003 R2	2
Linux (CentOS, Debian, Oracle, SUSE, Ubuntu)	64
Windows 8.1	32
Windows 8	32
Windows 7 (SP1)	4
Windows Vista (SP2)	2
Windows XP (SP3)	2
Windows XP x64 (SP2)	2

7 ZPŮSOB ZAJIŠTĚNÍ DISASTER RECOVERY IT SLUŽEB

Problematika disaster recovery je pro podniky, které jsou ve svých výrobních procesech závislé na informačních systémech důležitou záležitostí. Hlavní myšlenkou disaster recovery je, mít aktuální otisk primárního prostředí nebo primárních dat v geograficky oddělené lokalitě. V případě zničení primární lokality z důvodu živelné pohromy je možné „jednoduchým“ způsobem provést kompletní obnovu infrastruktury v řádu několika minut až hodin.

V případě chybějícího řešení disaster recovery dochází ke kompletnímu zániku informačního systému podniku. Je možné infrastrukturu znovu vystavět v řádu několika týdnů, ale ztráta informací v podobě uložených dat může mít pro podnik zničující důsledky. Nejjednodušším typem řešení disaster recovery je zálohování dat na páskové zařízení. Magnetické nosiče dat jsou, po ukončení offline zálohy, vynášeny z prostor datového centra a bezpečně uloženy v chráněném prostoru. V případě zničení datového centra dochází opět k několika týdenní nedostupnosti poskytovaných služeb, ale ztráta dat je redukována na hodnotu od poslední offline zálohy infrastruktury.

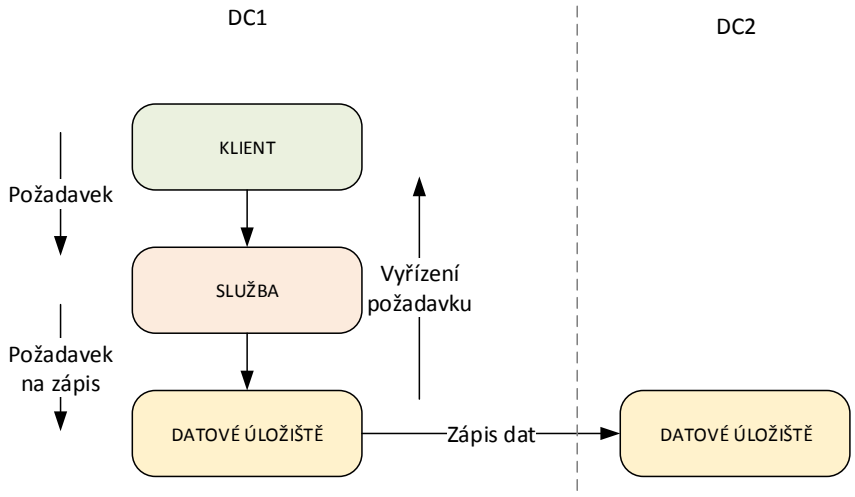
7.1 Replikace dat

Sofistikovanější řešení disaster recovery je pomocí replikace dat z primárního datového centra do sekundárního datového centra. Replikace dat může být zajištěna na úrovni diskových polí, které vlastnost replikace podporují v závislosti na typu diskového pole. Funkce zrcadlení dat není běžně dostupná a je nutné u většiny výrobců zakoupit aktivační licenci. Licencuje se většinou na fyzický box nebo na velikost replikovaných dat. V případě zápisu dat na primární diskové pole dochází k okamžité replikaci dat do sekundární lokality. Replikace dat probíhá pomocí SAN, LAN, WAN (Wide Area Network) sítě. Kvalita a propustnost přenosové linky mezi lokalitami má vliv na režim replikace.

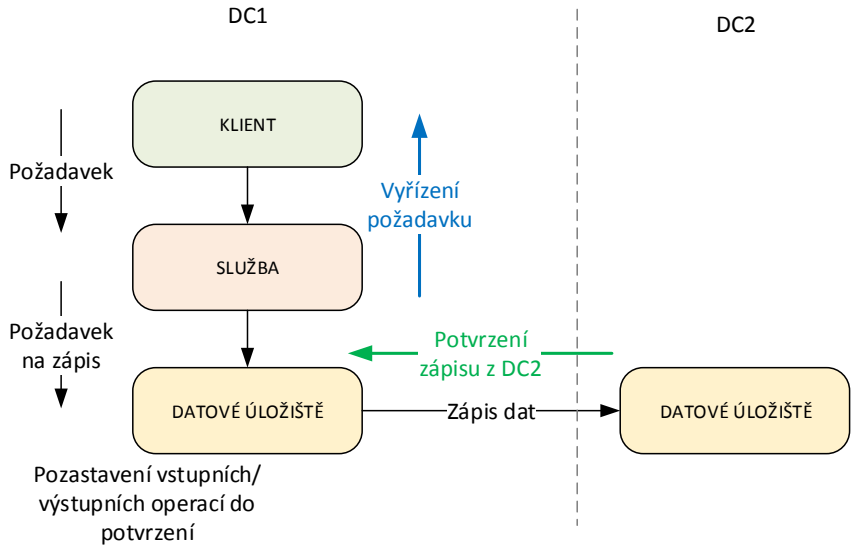
Při analýze rizik, které scénáře má disaster recovery zajistit, je nutné počítat s ochranou zónou kolem centra působení katastrofy. Dle zkušeností společnosti IBM byl akční rádius hurikánu Katrina 250 km. V případě řešení disaster recovery je tedy nutné přihlédnout, které vlivy mohou na sekundární datové centrum působit. Limit technologií pro synchronní replikaci dat je 300 km v podobě tzv. Metro mirroru a 8000 km pro asynchronní replikaci v případě tzv. Global Mirroru [33].

Synchronní režim garantuje nulovou ztrátu dat. V případě vzniku požadavku na zápis dat do primárního diskového pole dochází k pozastavení transakce a čeká se na potvrzení zápisu dat ze sekundární lokality. Po přijetí potvrzení je dokončena čekající transakce.

Asynchronní režim negarantuje nulovou ztrátu dat. V případě vzniku požadavku na zápis dat do primárního diskového pole dochází k okamžité replikaci dat do sekundární lokality. Transakce zpracování není pozastavena a nečeká se na potvrzení zápisu z druhé lokality [33].



Obr. 20. Asynchronní replikace dat.



Obr. 21. Synchronní replikace dat.

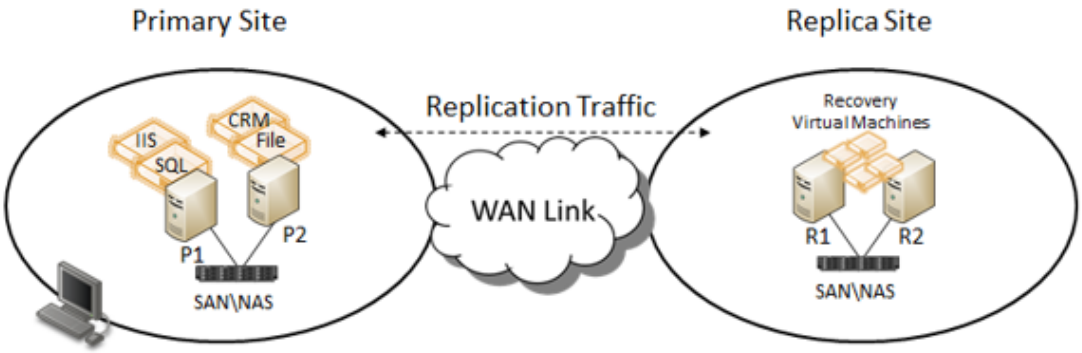
Většina technologií společnosti Microsoft, které umožňují provádět replikaci dat (Exchange server, SQL server, Hyper-V, atd.) využívají asynchronní režim. Možnost přepnutí do garantovaného módu je umožněna pomocí aplikačního rozšíření výrobců třetích stran [16].

7.2 Hyper-V replikace

Z důvodu sílících požadavků podniků na řešení disaster recovery v případě neočekávané havárie, výpadku primární lokality a zajištění co nejkratší doby obnovy chodu organizace, společnost Microsoft v rámci svého virtualizačního řešení přináší možnost replikace virtuálních serverů do jiné geograficky odlišné lokality.

V prvotní fázi konfigurace replikace virtuálního prostředí dochází k volbě, co a kam se bude replikovat. Počáteční replika spočívá v přenesení celého obsahu virtuálního počítače do vzdálené lokality. Může se jednat i o několik TB dat, z tohoto důvodu je možné provést export dat na přenosné médium a poslat médium pomocí kurýra do druhé lokality. Po nahrání exportovaných dat dojde pouze k rozdílové replikaci, která je už v řádu desítek MB. Této funkcionality je využíváno v prostředích, kde mezi lokalitami je pouze pomalá WAN linka, případně jsou vyžadovány FUP (Fair User Policy) politiky pro přenos dat.

Během provozu virtuálního serveru se v pravidelných intervalech, minimálně 30 sekund, provádí delta replikace virtuálních počítačů, včetně jejich virtuálních disků do cílového replikačního cíle. Replikovaný virtuální počítač má pro záložní lokalitu alternativní síťovou konfiguraci, která se v případě aktivace disaster recovery nastaví jakou defaultní síťová konfigurace TCP/IP (Transmission Control Protocol/Internet Protocol) [22], [24].



Obr. 22 Hyper-V replikace [24].

7.3 Replikace do veřejného cloudu

Zajistit vysokou dostupnost a disaster recovery je složitý proces, který vyžaduje nemalé investiční náklady do technologií a lidských zdrojů. V případě menších firem je výstavba datového centra zajišťující vysokou dostupnost a disaster recovery nereálnou záležitostí.

Z tohoto důvodu je možné si infrastrukturu a požadovaný výkon pronajmout u poskytovatelů cloudových služeb. Microsoft nabízí možnost pronájmu virtuálního prostředí pomocí služby Windows Azuze, která může být využívána jako replikační cíl primárního prostředí zákazníka. Disaster recovery je tedy dostupná pro široké spektrum podniků [27].

II. PRAKTICKÁ ČÁST

8 TECHNOLOGIE NOVÉHO DATOVÉHO CENTRA

Z důvodu zvýšení kvality poskytovaných IT služeb bylo vedením oddělení informatiky a řídící vertikálou Fakultní nemocnice schválena výstavba nového datového centra.

Zvýšením kvality bylo zamýšleno následující:

- Nezávislost na údržbě elektrického napájení v budově chirurgického monobloku.
- Bezpečné uchování dat v jiné lokalitě.
- Možnost manuálního překlopení IT služeb do jiné lokality v případě údržby primární lokality.
- Nastartovat budování vysoce dostupného informačního systému.
- Řešení problematiky disaster recovery.

V roce 2011 byla započata stavba nového energobloku Fakultní nemocnice. V rámci stavby bylo umožněno ujmout část nových prostor pro potřeby nového datového centra. Budova nového energobloku byla napojena na stávající kabelové šachty sloužící k vedení optických tras po areálu nemocnice. Po dokončení stavebních prací bylo zahájeno osazení nového datového centra novými technologiemi kritické infrastruktury.

8.1 Technologie kritické infrastruktury

8.1.1 Serverové rozvaděče

Datové rozvaděče pro servery byly zvoleny od společnosti Rittal typ DK-TS8 v rozměrech 800x2000x1200 mm (šířka x výška x hloubka). Rozměry byly zvoleny v závislosti na instalovaných zařízeních, která jsou hluboká cca 1000 mm. Nosnost rozvaděče byla kalkulována na hodnotu 1000 kg statické zatížitelnosti. Vstup do rozvaděče je umožněn pomocí dělených předních a zadních dveří s více bodovým uzamykáním, které je možné v případě potřeby doplnit o bezpečnostní mechanické zábranné systémy. Útroby rozvaděče byly doplněny příslušenstvím pro kabelový management. Krajní rozvaděče byly vybaveny uzamykatelnou bočnicí bránící vstup do prostoru rozvaděče. Mezi sousedícími rozvaděči byly instalovány dělící příčky z důvodu zamezení vzájemného tepelného ovlivňování. Ve všech rozvaděčích byly vloženy kabelové trasy a vzduchové přepážky. Vstup kabelových tras do rozvaděčů byl zvolen pomocí střešního prostupu vybaveným kartáčovou vložkou.

Obr. 23. Datový rozvaděč.

První serverový rozvaděč byl navrhnut jako datový, je zde zakončena strukturovaná kabeláž do ostatních racků. Druhý rozvaděč byl zvolen k uložení diskových polí. Jsou zde zakončena optická vlákna typu multimode ze staré serverovny.

8.1.2 Napájecí lišty

Serverové rozvaděče byly osazeny dvěma dvouokruhovými modulárními napájecími lištami ve vertikálním provedení. Byly zvoleny 3 fázové napájecí lišty s napájecím přívodem 3x 16 A s pevnou montáží.

Napájecí lišty byly osazeny konektory typu:

- 18x IEC320 C13,
- 4x C19,
- 4x ČSN.

8.1.3 Monitoring vnitřního prostředí rozvaděče

Jako základ systému monitorování rozvaděčů byly zvoleny řídící jednotky připojené do management části datové sítě pomocí ethernet rozhraní. Byly voleny jednotky, které umožňují zasílat funkční stavy pomocí SNMP (Simple Network Management Protocol) protokolu do řídícího centrálního monitoringu informačního systému. Každý rozvaděč byl osazen teplotními detektory, detektory vlhkosti a záplavovými detektory umístěnými ve zdvojené podlaze. Systém monitoringu byl z důvodu zasílání incidentů napojen na GSM (Groupe Spécial Mobile) modul. Systém monitoringu datového centra byl volen s požadavkem na zasílání emailových zpráv a SNMP trapů.

8.1.4 Zavřená studená ulička

Veškeré datové rozvaděče, Rittal LCP (Liquid Cooling Package) jednotky a Rittal UPS byly poskládány do systému chlazení pomocí uzavřené studené uličky. Šířka studené uličky byla zvolena v šíři 1800 mm, včetně vstupního dveřního prvku a zadního panelu. Vstupní posuvné dveře byly zvoleny v proskleném provedení.

8.1.5 Uzavřený kamerový systém

K zajištění obrazového záznamu přítomnosti osob v datacentru byla instalována barevná IP kamera Siemens s technologií CMOS (Complementary Metal Oxide Semiconductor). Úložiště obrazového záznamu bylo nastaveno na monitoring server sloužící k ovládání technologií.

Obr. 24. Systém studené uličky.

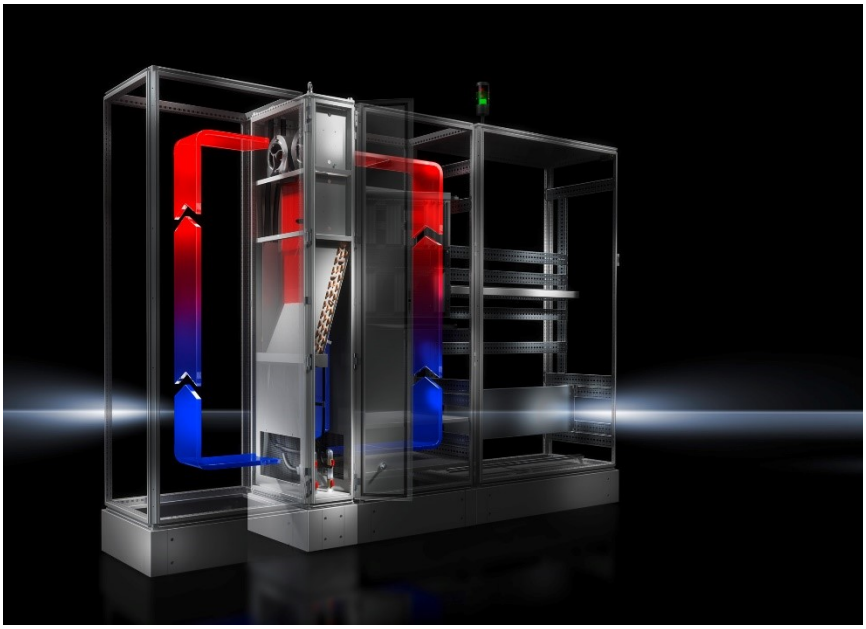
Obr. 25. Systém studené uličky.

8.1.6 Chlazení

Jako zdroj chladu byly navrženy dvě kompaktní vzduchem chlazené jednotky Uniflair model ISAF0921A, každá o chladícím výkonu 106 kW v konfiguraci 1 + 1. Tím bylo zajištěno pokrytí tepelných zisků zařízení i při výpadku jedné z chladících jednotek.

Systém chlazení byl koncipován na celoroční provoz, v případě nízkých venkovních teplot dochází k šeření elektrické energie. Systémy / jednotky byly navrženy za účelem využití příznivých teplotních podmínek a jsou vybaveny jednotkou volného chlazení. V případě dostatečně nízké teploty dochází ke snížení výkonu chladící části, nebo dojde ke kompletnímu odstavení kompresorů. Právě kompresory jsou největšími konzumenty elektrické energie. Po odstavení kompresorů je zajištění tepelné výměny dosaženo pomocí výměníku vzduch / voda.

K zajištění chlazení datového centra byly navrhnuty vnitřní mezi rackové chladící jednotky Rittal LCP inline s uvažovaným výkonem 5x 25 kW. Jednotky byly navrženy s ohledem na dostatečnou rezervu, v případě výpadku jedné z nich jsou zbylé čtyři jednotky schopné uchladit tepelnou zátěž datového centra.



Obr. 26. Systém chlazení Rittal LCP [30].

8.1.7 UPS

V rámci zajištění nepřetržitého zdroje napájení byl instalován modulární redundantní systém Rittal PMC 200 UPS sestávající ze skříně pro výkonové moduly, kterou lze osadit pěti kusy autonomních výkonových modulů s jednotkovým výkonem 40 kVA / 32 kW. UPS byly osazeny systémem bezúdržbových akumulátorů typu VRLA (Valve Regulated Lead Acid). UPS byla vybavena systémem hot-plug z důvodu vkládání a vyjímání výkonových modulů bez nutnosti přepnutí na elektronicky / manuální bypass nebo odstavení UPS. Každý modul byl navržen k samostatné činnosti, včetně kontrolních prvků (blok řízení, ovládací panel s displejem a tlačítky), usměrňovače, střídače, nabíječe a elektronický bypass. Provedení skříně UPS a bateriové skříně bylo navrženo v shodném provedení jako serverové rozvaděče. Z důvodu monitoringu byla UPS vybavena monitorovací jednotkou, která byla zapojena do management části datové sítě. V případě výpadku elektrické energie byla UPS dimenzována na běhový čas 15 min. v případě maximálního zatížení.

Obr. 27. Elektrotechnické rozvaděče.

Prostřednictvím elektrotechnických rozvaděčů bylo datové centrum připojeno k nově budovanému energobloku, který pro část nemocničního areálu poskytuje dodávku elektrické energie včetně náhradního zdroje napětí v podobě motorgenerátoru. Náběh motorgenerátoru byl stanoven na dobu maximálně 5 minut.

Obr. 28. UPS – výkonové moduly.

8.1.8 Zvlhčovač

Z důvodu zajištění optimální vlhkosti v datovém centru byla instalace technologií rozšířena o vnitřní parní zvlhčovač HumiSteam X-plus UE005.

8.1.9 Stabilní hasicí zařízení

Z důvodu ochrany vynaložených finančních prostředků do instalovaných technologií bylo datové centrum vybaveno plynovým stabilním zařízením Novec 1230. Hasivo je uchováváno v tlakových lahvích při tlaku 42 barů v kapalné podobě. Uvolněním hasiva dochází k rozprášení na malé kapičky, které se rychle v prostoru odpaří a dojde k vytvoření požadované hasící koncentrace. Vzniklá homogenní koncentrace hasiva zajistí rozrušení chemických vazeb při hoření a tím rychlé eliminaci plamene [9].

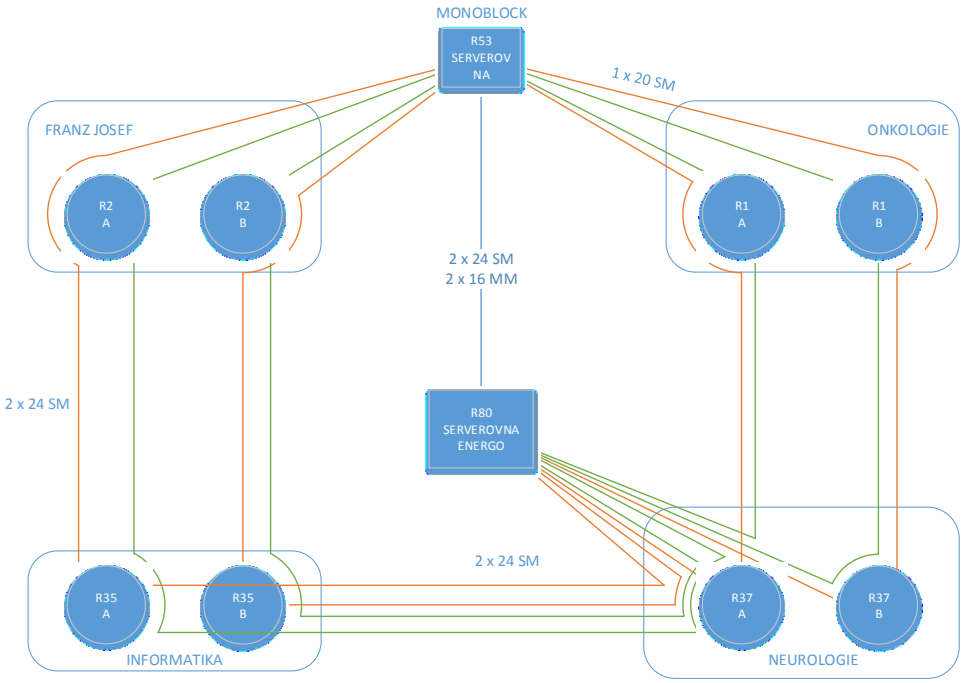
Obr. 29. Stabilní hasicí zařízení s ústřednou.

9 NÁVRH DESIGNU DATOVÉ SÍTĚ PRO POTŘEBY PROVOZU VE DVOU DATOVÝCH CENTRECH

9.1 Fyzická vrstva

Požadavek na vysokou dostupnost přes dvě datová centra byl zapracován v podobě nového návrhu designu datové sítě. Dle doporučení byla změněna fyzická vrstva z kruhu na dvojitou hvězdu [1]. Každý z dvojice páteřních přepínačů byl rozmístěn mezi stávající a nové datové centrum, společně tvořící jeden logický celek. Jako páteřní přepínače byly zvoleny zařízení Cisco Catalyst 6500E. Centrum hvězdy bylo z důvodu redundance zdvojeno, v případě výpadku jednoho z přepínačů nedojde k výpadku služby. Tímto způsobem bylo zajištěno výrazné zvýšení spolehlivosti a dostupnosti důležitých částí LAN infrastruktury.

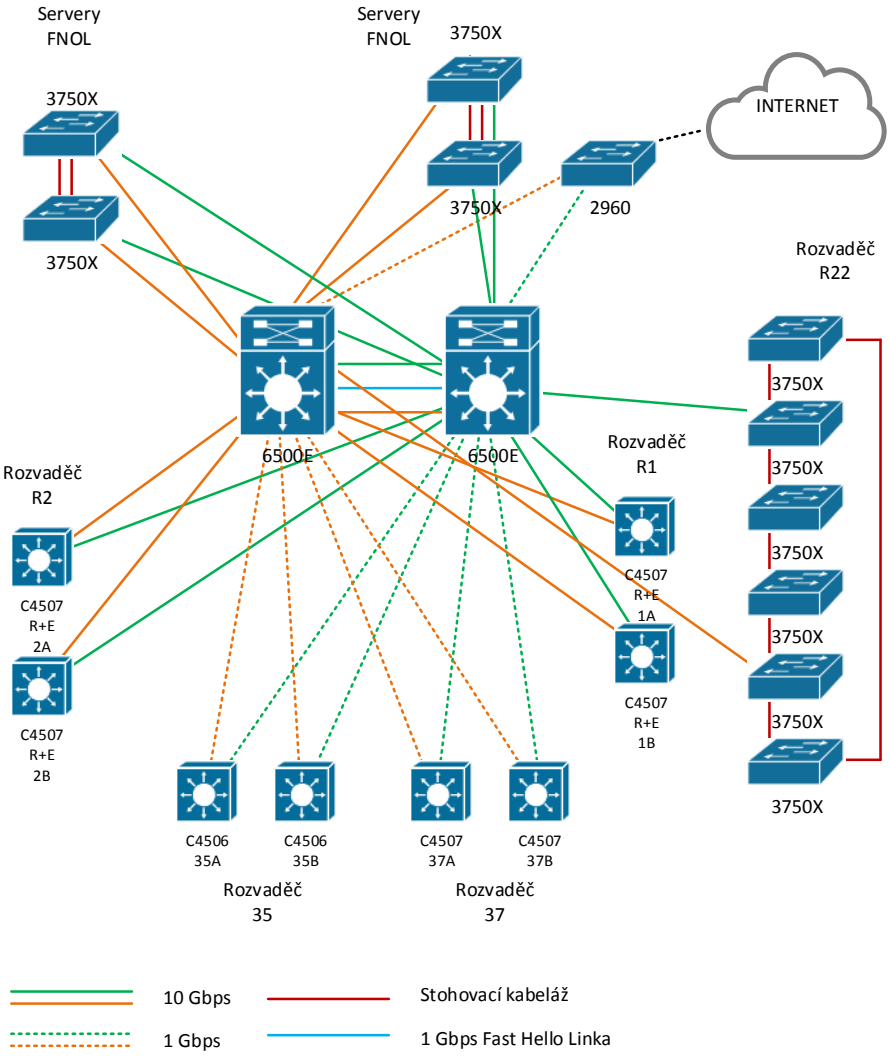
Pro připojení serverových zařízení bylo navrhnuto použít dvakrát dvoupřístupové přepínače Cisco Catalyst 3750-X spojené do dvou stohů. První stoh byl umístěn ve starém a druhý v novém datovém centru. Připojení stohu k páteřním přepínačům bylo navrhnuto pomocí 4x 10GE rozhraní [1].



Obr. 30. Optické trasy v areálu nemocnice.

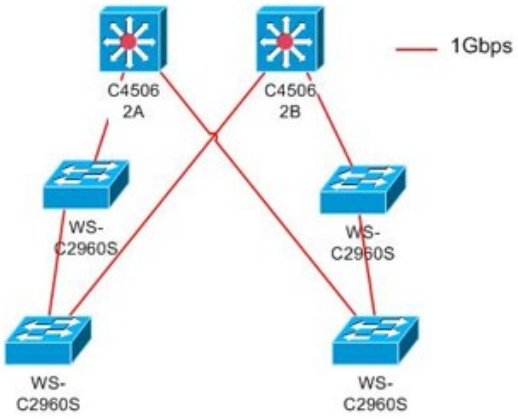
Změna fyzického designu si vyžádala dodělání nových optických vláken kategorie OM3 mezi datovými centry a dále mezi datovými centry a jednotlivými uzly sítě LAN. Přenosová rychlost fyzického propojení mezi páteřními přepínači a přepínači řady Catalyst 4500

v rozvaděčích R1 a R2 bylo použito 10GE. V ostatních rozvaděčích byla ponechána stávající přenosová rychlost 1GE. Mezi páteřními prvky bylo zamýšleno s jedním gigabitovým propojem sloužícím jako Fast Hello linka pro Virtual Switching System.



Obr. 31. Fyzické zapojení aktivních prvků.

Připojení nemodulárních přepínačů bylo provedeno přímo k hlavním přepínačům z důvodu nežádoucí tvorby rozvětvené sítě, která by mohla způsobovat problémy s fyzickými a logickými smyčkami. Pro připojení přístupových přepínačů bylo zamýšleno využít optickou kabeláž a v ojedinělých případech využít kabeláž metalickou vždy s minimální přenosovou rychlostí 1 Gbit/s.



Obr. 32. Zapojení přístupových přepínačů.

9.2 Páteřní přepínače

Na úrovni páteřních přepínačů došlo k nahrazení stávajících Cisco Catalyst 6500 za nové přepínače stejného typu. Se stávajícími přepínači se již nepočítá a budou odprodány v rámci Trade-in programu společnosti Cisco. Jako centrální modul přepínače byl zvolen supervisor SUP2T, který je pro potřeby nemocnice vhodným řešením. Z důvodu připojení distribuční vrstvy přepínačů byly přepínače rozšířeny o jeden 24x 1GE modul a dva 8x 10GE modul.

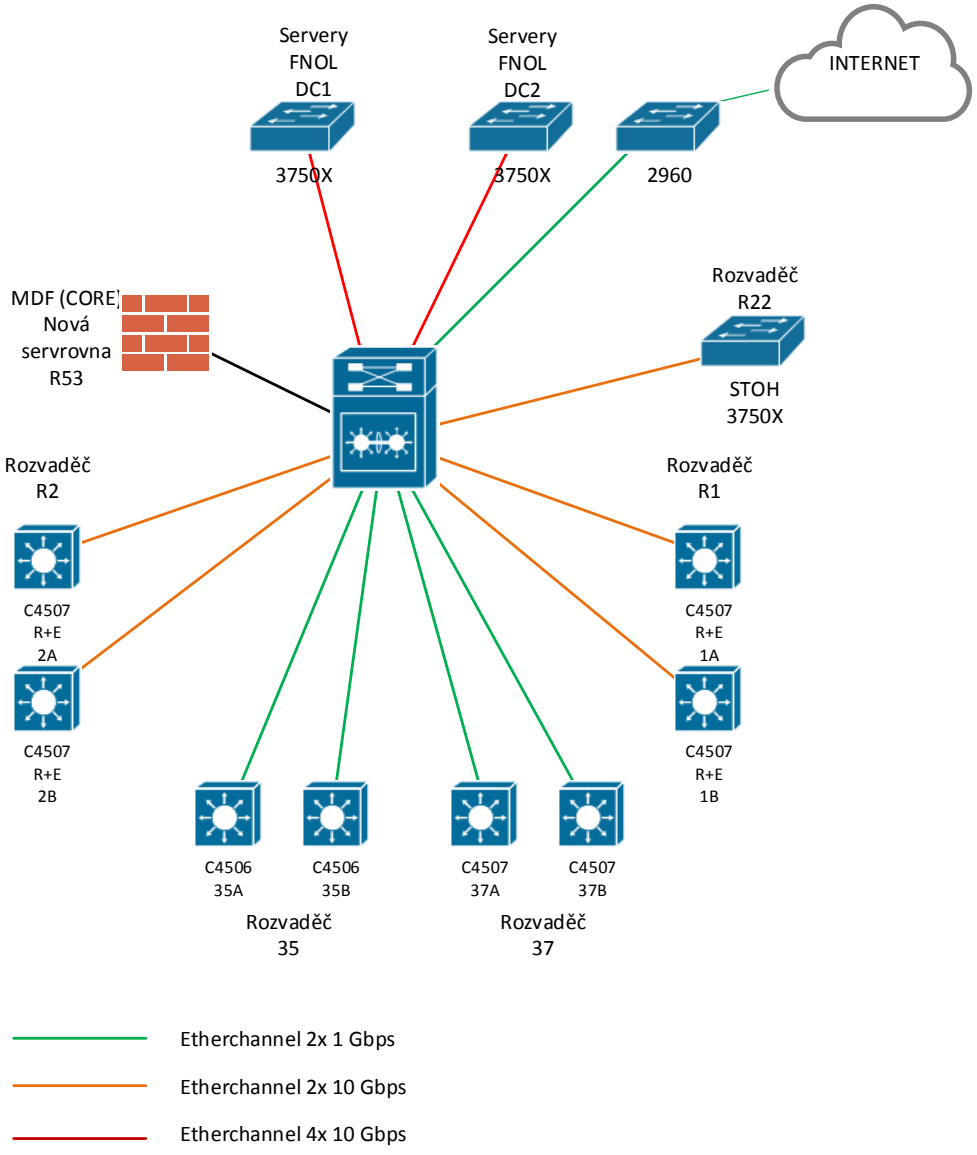
Fyzické propojení datových center bylo navrhnuto realizovat pomocí dvou 10GE rozhraní, které jsou k dispozici na supervisoru. Díky propojení datových center a konfigurace VSS (Virtual Switching System) bylo dosaženo logického spojení přepínačů.

Díky implementaci VSS byly zajištěny následující výhody:

- Dva přepínače sdílejí společný management a vůči síťové infrastruktuře vystupují jako jedno zařízení.
- Eliminuje závislost na FHRP (First Hop Redundancy Protocol) a Spanning tree protokolu.
- Obnova L2 linky v případě výpadku tvá maximálně 200 milisekund a tím poskytuje bezvýpadkovou komunikaci v rámci EtherChannel linky.
- Obsahuje ochranný mechanismus v podobě Fast Hello protokolu, který zabraňuje stavu, kdy přepínače netvoří VSS a pracují samostatně a tím vytváří smyčky v síti [11].

9.3 Logická topologie

Spojová vrstva byla v závislosti na fyzické vrstvě řešena jednoduše. Vychází z hvězdy s páteřními přepínači. Díky sloučení centrálních přepínačů do VSS bylo možné propojení mezi přístupovými a páteřními přepínači sloučit do jednoho EtherChannelu.



Obr. 33. Logická topologie.

9.4 Virtuální sítě

V rámci úpravy topologie byl proveden návrh změny VLAN. Veškeré virtuální sítě byly centralizovány a ukončeny na páteřních přepínačích. Šíření VLAN na jednotlivé přístupové přepínače bylo provedeno s ohlédnutím, kde je nutné jednotlivé virtuální sítě používat.

Jedinou virtuální sítí, která se šíří přes všechny přepínače, je management sítě pro potřeby správy aktivních prvků.

9.5 Spanning tree protokol

Vzhledem k použití technologie VSS byly v páteřní části sítě eliminovány smyčky v síti. Pro případ náhlého rozpadu VSS bylo na přepínačích Catalyst 6500 nastaven PVRST (Per VLAN Rapid Spanning Tree) protokol. Konfiguraci Spanning tree bylo nezbytné provést v přístupové části sítě z důvodu redundantního připojení přístupového přepínače k distribuční vrstvě. Spanning tree protokol byl konfigurován na uplink portech a na všech linkách, kde je použito trunk propojení. Jako spanning tree root bridge byly zvoleny páteřní přepínače Catalyst 6500 [8].

10 NÁVRH ZABEZPEČENÍ DATOVÉ SÍTĚ PŘED VNITŘNÍMI ÚTOKY

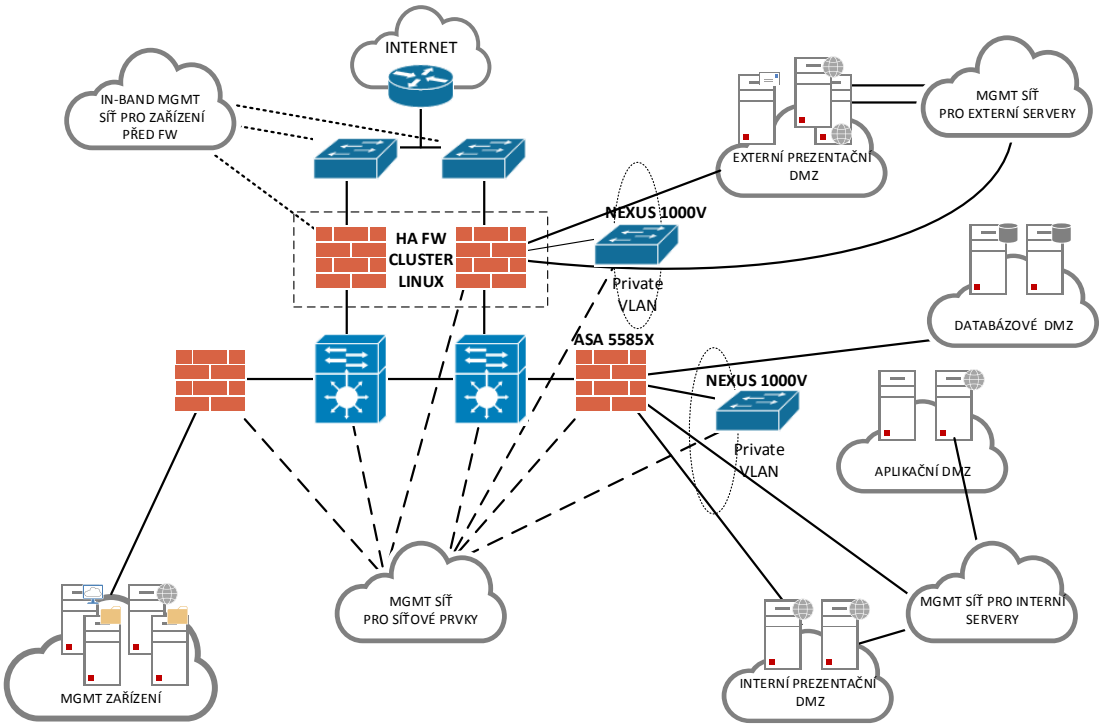
Zabezpečení datové sítě souvisí s novým návrhem datové sítě, kdy součástí konfigurace páteřních přepínačů byl implementován zone base firewall, který byl koncipován k definování komunikačních pravidel mezi jednotlivými virtuálními sítěmi. Úroveň zabezpečení je limitována typem aplikační architektury.

Dle tvrzení odborné literatury je nejvhodnější tzv. třívrstvá architektura, která spočívá v oddělení komunikace do třech různých úrovní [2].

Klient – Prezentační vrstva - Aplikační vrstva, datová vrstva

Představitelem klienta jsou počítače uživatelů, prezentační vrstva může být zajištěna např. pomocí webových služeb a aplikační vrstva může být zajištěna např. databázovým systémem. Komunikace probíhá lineárním způsobem, klient nikdy nekontaktuje databázový server [2].

Pomocí zone base firewallu tedy dochází ke striktnímu oddělení komunikace mezi virtuální sítí sloužící pro klienty a virtuální sítí pro databázové servery.



Obr. 34. Návrh segmentace sítě LAN.

V rámci jednotlivých segmentů musí být uplatněny technologie, které od sebe dílčí systémy oddělují. Důvodem je zamezení útoku z kompromitovaného systému na jiný systém v daném segmentu. Komunikace více systémů uvnitř segmentů byla v návrhu řízena firewallem. Pokud byly servery připojeny k jednomu přepínači, nakonfigurují se jednotlivé porty jako protected. Tyto porty nemohou mezi sebou vzájemně komunikovat. Pokud jsou servery připojeny k více přepínačům, je nutné použít technologii Private VLAN. Z důvodu využívání virtualizační platformy Microsoft Hyper-V bylo v návrhu počítáno s využitím virtuálního přepínače Cisco Nexus 1000.

Z důvodu zvýšení bezpečnosti datové sítě byly pomocí Windows Group Policy aktivovány interní firewall systémy koncových zařízení.

Jednou ze slabých částí zabezpečení sítě je tzv. ARP (Address Resolution Protocol) přesměrování [7]. ARP protokol slouží k převodu IP adres na MAC adresy. V případě kontaktování některého ze svých sousedů (včetně brány sítě), se zeptá všesměrovým ARP dotazem. Pomocí aplikace arpredirect je možné falšovat veškeré ARP odpovědi týkající se brány a komunikace prochází přes zařízení útočníka.

Proti útoku na ARP je možné se chránit pomocí funkce Dynamic ARP inspection, tato funkce využívá aktivovaný DHCP snooping.

Významné zvýšení bezpečnosti na síťové vrstvě pomáhá implementace IEEE (Institute of Electrical and Electronics Engineers) 802.1x [7].

Tab. 3. Komunikační matice.

Odkud	**Zařízení**	**Kdo**	**Autentizace**	**Autorizace**
LAN	PC ve správě IT	-	ok	domovská VLAN
LAN	PC ve správě IT	-	špatné	restricted VLAN
LAN	PC mimo správu IT	-	ok	VLAN s limitovaným přístupem

Implementace ověřování přístupu do sítě LAN byla navrhnuta na platformě CISCO ISE. Autentizace / autorizace byla prováděna prostřednictvím protokolu RADIUS (Remote Authentication Dial In User Service), pomocí kterého budou komunikovat síťové přepínače s ISE. Na základě navrhnuté komunikační matice dochází k dynamickému nastavení VLAN na portu přístupového přepínače. Autentizace stanic byla navržena pomocí certifikátu, který se generuje automaticky v prostředí domény active directory.

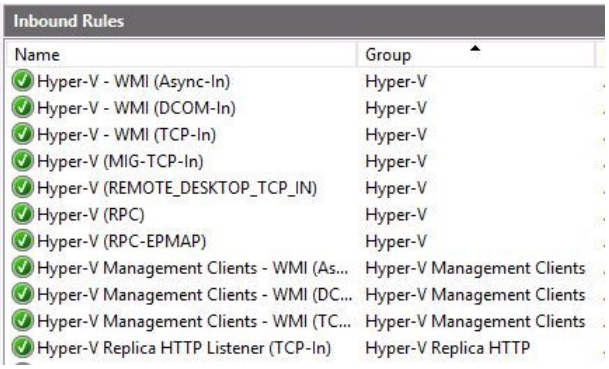
11 NÁVRH PROVOZU IT SLUŽEB V REŽIMU VYSOKÉ DOSTUPNOSTI V PROSTŘEDÍ FNOL

V prostředí FNOL byla již velká část systémů provozována v režimu vysoké dostupnosti. Zajištění provozu mezi dvěma lokalitami bylo provedeno díky kombinaci služeb převzetí po výpadku a Hyper-V replika, případně interními mechanismy produktů společnosti Microsoft.

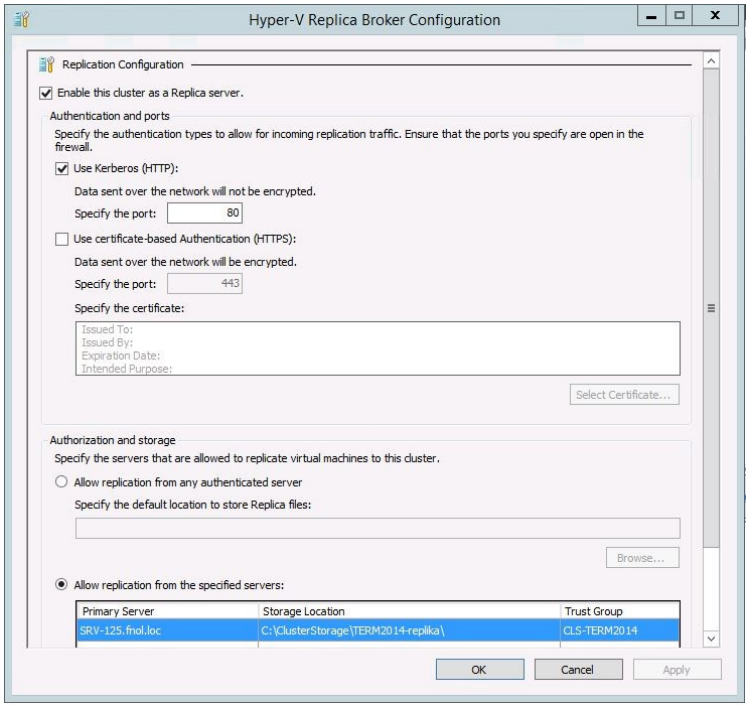
11.1 Vysoká dostupnost virtuální infrastruktury

11.1.1 IT služby provozované pomocí jedné instance

Vysoká dostupnost byla navrhnuta na úrovni primární lokality pomocí služby převzetí po výpadku. Virtualizační cluster byl vystavěn na operačním systému Windows Server 2012 R2. Z důvodu zajištění výkonových rezerv byl zvolen 4 uzlový cluster, v případě výpadku jednoho z uzlů nedojde ke snížení kvality poskytovaných služeb. Zajištění replikace dat do sekundární lokality bylo realizováno pomocí Hyper-V repliky. V sekundární lokalitě byl vystavěn nový cluster sloužící pro příjem replikačních dat. Repliky virtuálních počítačů jsou zde vypnuty a přijímají replikovaná data. V případě plánované odstávky primární lokality dochází ke spuštění replikovaných virtuálních serverů. Na obou clusterech bylo nutné zkonfigurovat clusterový prostředek Replica broker. Replica broker zajišťuje replikaci virtuálních počítačů v clusteru do vzdáleného clusteru. Při konfiguraci bylo nutné specifikovat, ze kterých uzlů je možné přijímat žádost o replikaci.



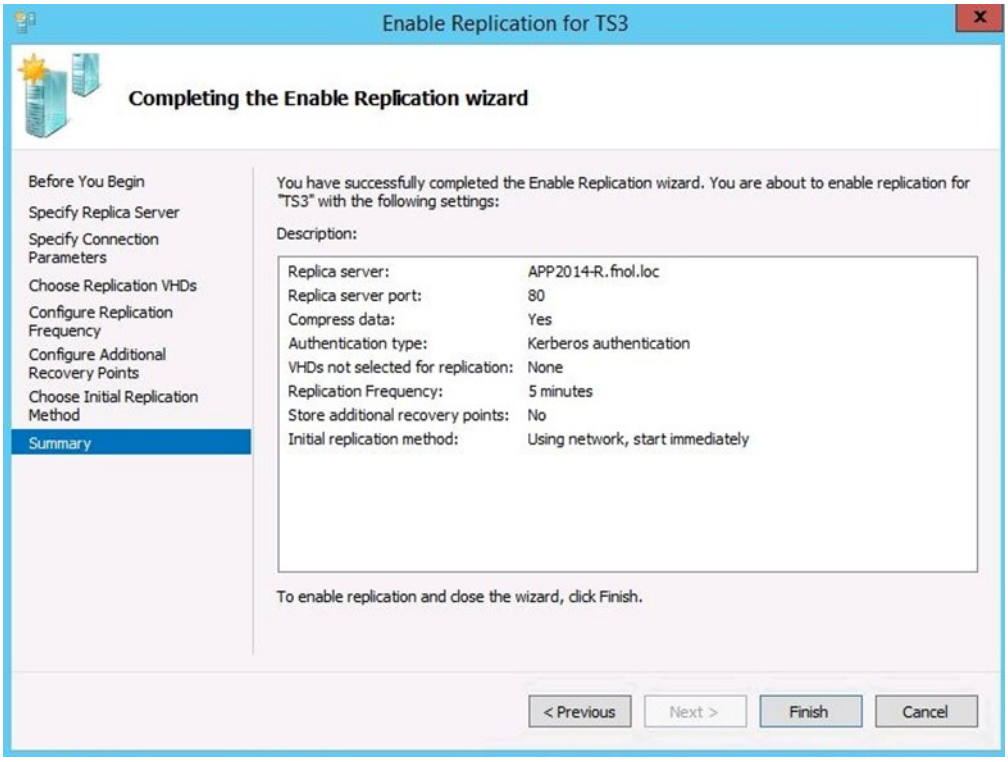
Obr. 35. Nastavení interního FW.



Obr. 36. Konfigurace Hyper-V replica broker.

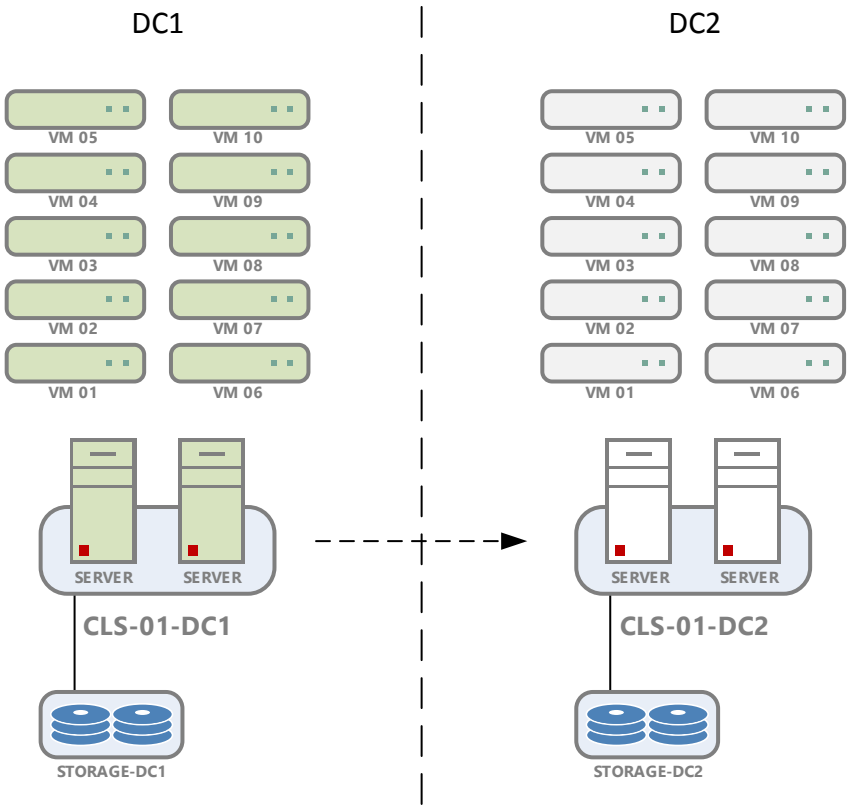
Dále bylo nutné povolit komunikační pravidla na interním firewallu.

Po dokončení konfigurace cílového replikačního clusteru bylo nutné nastavit replikační režim jednotlivých virtuálních počítačů.



Obr. 37. Sumář nastavení replikace.

Bylo nutné nastavit cílový replikační server, kterým byl v clusterovém provedení prostředek replica broker. Přenos dat byl proveden pomocí HTTP (Hypertext Transfer Protocol) protokolu. Kdyby byla komunikace šířena mimo prostředí FNOL, bylo by možné využít zabezpečené komunikace pomocí HTTPS (Hypertext Transfer Protocol Secure) protokolu. Důležitým nastavením byla doba frekvence replikace. Bylo možné nastavit tři úrovně 30 sekund, 5 minut, 15 minut.

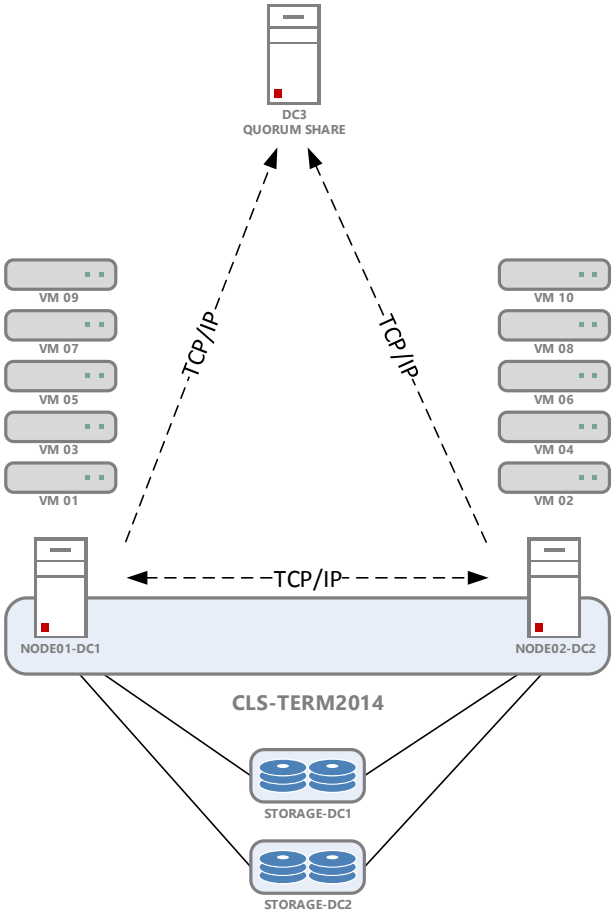


Obr. 38. Princip fungování Hyper-V repliky.

11.1.2 IT služby provozované pomocí několika instancí

U služeb, které se v prostředí FNOL vyskytují ve více instancích, byl navrhnutý režim smíšeného rozmístění. Původní cluster byl rozdělen mezi obě datová centra. Z tohoto důvodu bylo nutné změnit konfiguraci clusteru. Funkcionalita clusteru spočívá v počtu aktivních hlasů. Pokud je počet aktivních hlasů menší než polovina všech dostupných hlasů clusteru, dochází k zastavení funkce clusteru. V případě počtu dvou uzlů je v rámci clusteru doporučeno zprovoznit svědka (sdílený diskový prostor, který je přepínatelný mezi uzly), a to z důvodu prohlášení, který uzel bude dále poskytovat hostované služby. Z důvodu rozdělení na dvě lokality nebylo možné svědka v podobě fyzického disku použít. Bylo tedy využito sdíleného souborového sdílení. Server, který poskytuje sdílenou složku, byl umístěn

v datovém centru v budově informatiky. V případě poruchy na komunikační vrstvě mezi jednotlivými uzly rozhodne svědek, který uzel bude v clusteru aktivní. Pokud je výpadek komunikace důsledkem havárie datového centra, předá svědek informaci zbylému uzlu a zajistí dodání požadovaného hlasu k provozu clusteru [22].



Obr. 39. Komunikace mezi uzly a svědkem.

Logika smíšeného rozřazení se spoléhá na interní mechanismus zajištění vysoké dostupnosti služby. Pro aplikace typu Microsoft Exchange Server nebo Microsoft SQL Server bylo v návrhu počítáno s mechanismem DAG (Database Availability Group) nebo Always on. V rámci ověření smíšeného rozřazení bylo využito terminálových služeb, kdy liché názvy instance byly umístěny v datovém centru 1 na diskovém poli 1 a sudé instance byly umístěny v datovém centru 2 na diskovém poli 2.

Disks (8)

Search

Name	Status	Assigned To	Owner Node
Physical Disk VM SRV-22 (DC2)	Online	Cluster Shared Volume	SRV-126
Physical Disk VM TERM-11 (DC1)	Online	Cluster Shared Volume	SRV-125
Physical Disk VM TERM-17 (DC1)	Online	Cluster Shared Volume	SRV-125
Physical Disk VM TERM-18 (DC2)	Online	Cluster Shared Volume	SRV-126
Physical Disk VM TERM-19 (DC1)	Online	Cluster Shared Volume	SRV-125
Physical Disk VM TERM-20 (DC2)	Online	Cluster Shared Volume	SRV-126
Physical Disk VM TERM-21 (DC1)	Online	Cluster Shared Volume	SRV-125
Physical Disk VM TS3 (DC1)	Online	Cluster Shared Volume	SRV-126

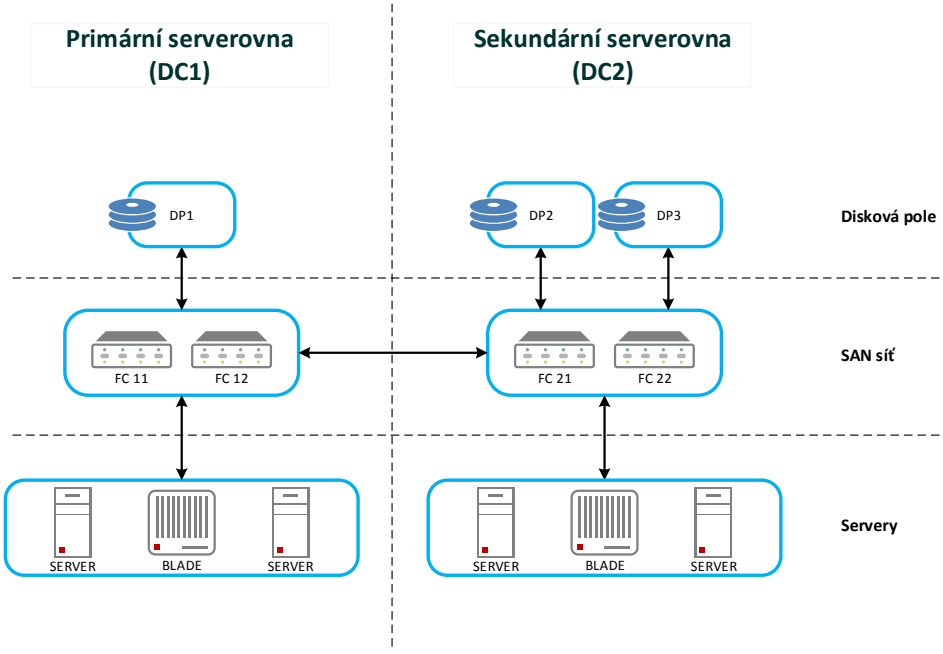
Obr. 40. Rozmístění fyzických disků přes disková pole.

11.2 IT služby mimo správu oddělení informatiky Fakultní nemocnice

U služeb, které nejsou ve správě oddělení informatiky FNOL, bylo navrhnuto využít funkcionality zrcadlení dat na úrovni diskových polí IBM Storwize V7000. Tyto IT služby nebyly původně koncipovány pro provoz ve vysoké dostupnosti. Zrcadlením bylo alespoň zajištěno disaster recovery IT služby.

11.3 Změna topologie SAN sítě

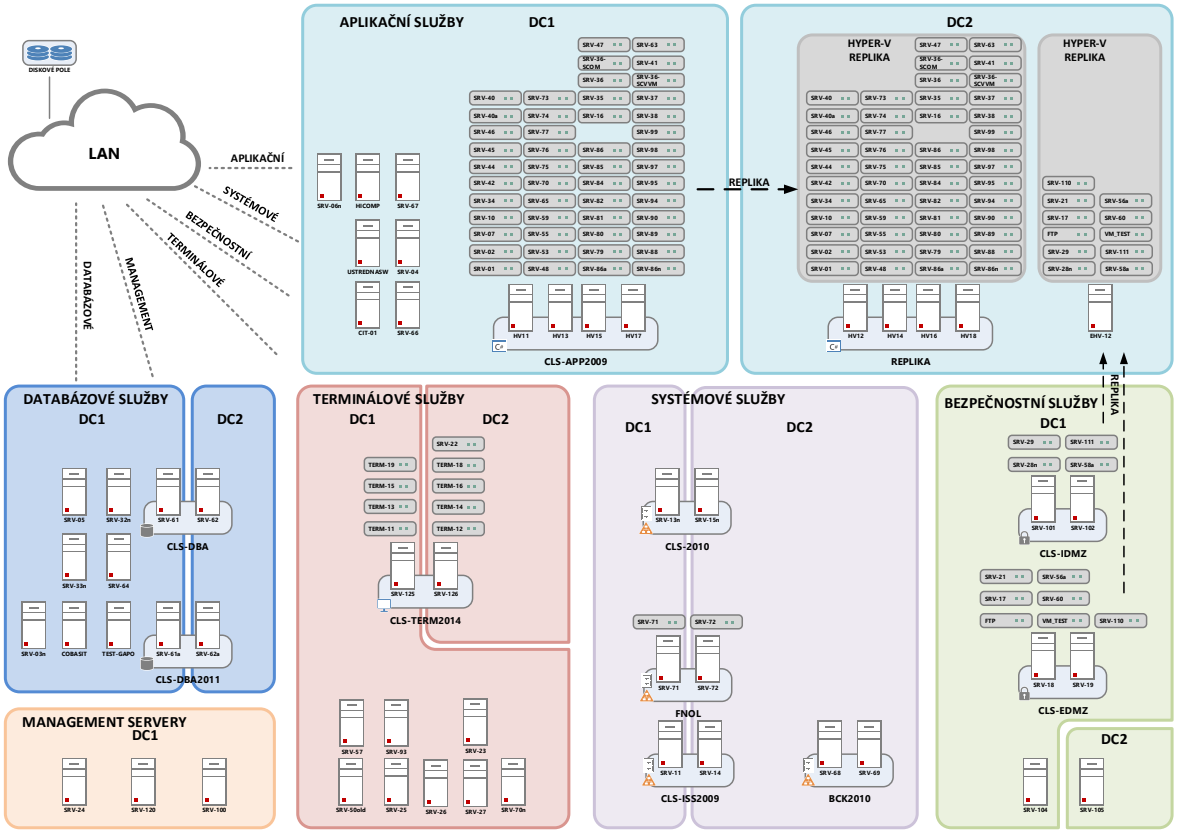
Z důvodu změny návrhu zajištění vysoké dostupnosti v návaznosti na provoz ve dvou datových centrech byl proveden návrh změny topologie SAN sítí. Změna reflektuje požadavky na nové rozmístění diskových polí a serverů.



Obr. 41. Změna topologie SAN.

11.4 Testovací prostředí

Veškeré návrhy poskytování IT služeb byly ověřeny v reálném prostředí Fakultní nemocnice Olomouc. Pro potřeby návrhu bylo vytvořeno testovací prostředí pomocí čtyř serverů IBM bladecenter HS23 s 256 GB RAM. Servery byly rozmístěny mezi dvě IBM bladecenter řešení. Tím došlo k nasimulování prostředí dvou datových center. Pro potřeby diskových oddílů bylo využito dvou diskových polí IBM Storwize V7000. Připojení fyzických hostů k diskovému poli bylo provedeno s ohlédnutím na rozmístěním diskových polí v rámci obou datových center.



Obr. 42. Globální návrh provozování infrastruktury.

ZÁVĚR

Bylo vypracováno vypořádání požadavku vedení Fakultní nemocnice Olomouc na zajištění informačních a komunikačních služeb v režimu vysoké dostupnosti, včetně disaster recovery celého informačního systému Fakultní nemocnice Olomouc.

Byly navrhnuty technologické komponenty kritické infrastruktury nově budovaného datového centra s důrazem na zajištění požadovaných potřeb vysoké dostupnosti informačního systému nemocnice.

V části č. 9 věnované datové síti nemocnice byl proveden návrh modernizace stávající datové sítě s přihlédnutím k potřebám zajistit homogenní síťovou infrastrukturu napříč oběma datovými centry. Design návrhu datové sítě odráží požadavky oddělení informatiky zajistit v části datové sítě vyšší propustnost dat.

Na návrh designu sítě navazuje kapitola týkající se zabezpečení datové komunikace. Z důvodu diskrétnosti byla problematika zabezpečení stažena pouze na vnitřní segment sítě. Návrh zohledňuje požadavek oddělení informatiky zamezit fyzickému přístupu do datové sítě zařízením, které nejsou pod správou oddělení informatiky. V rámci bezpečnosti byla zmíněna závislost aplikační architektury a jejím vrstvením na celkovém zabezpečení síťové infrastruktury.

V rámci návrhu realizace zajištění vysoké dostupnosti IT služeb s ohledem na využití stávajících infrastrukturních zdrojů, bylo navrženo využití funkcionalit operačního systému Microsoft Windows Server 2012 R2. Byla provedena úprava rozmístění stávajících zařízení mezi obě datová centra tak, aby bylo možné provozovat maximální množství IT služeb v režimu vysoké dostupnosti. U služeb, které nejsou přizpůsobeny k provozu v režimu vysoké dostupnosti, bylo navrhnuto využít funkcionalit zrcadlení dat na úrovni diskového pole.

Návrhy scénářů zajištění vysoké dostupnosti byly v prostředí Fakultní nemocnice Olomouc nasazeny do testovacího prostředí. Část scénářů byla nasazena do produkčního prostředí, kde probíhá ověřování funkčnosti a spolehlivosti řešení. Z důvodu chybějících licencí zrcadlení dat prostřednictvím diskových polí, nebylo možné tento scénář zrealizovat v prostředí nemocnice.

Práce má potenciál dalšího rozvoje ve formě modernizace zálohovacího řešení s úzkou vazbou na virtualizační platformu a specifické nastavení způsobu disaster recovery. V rámci

modernizace datové sítě má práce potenciál v samotné implementaci dle navrhnutého designu.

SEZNAM POUŽITÉ LITERATURY

[1] BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. 1. vyd. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.

[2] BRUCKNER, Tomáš, Jiří VOŘÍŠEK a Alena BUCHALCEVOVÁ. *Tvorba informačních systémů: principy, metodiky, architektury*. 1. vyd. Praha: Grada, 2012, 357 s. Management v informační společnosti. ISBN 978-80-247-4153-6.

[3] BUCKSTEEG, Martin, Ebel NADIN a Frank EGGERT. *ITIL 2011*. 1. vyd. Brno: Computer Press, 2012, 216 s. ISBN 978-80-251-3732-1.

[4] DOUCEK, Petr, Luděk NOVÁK, Lea NEDOMOVÁ a Vlasta SVATÁ. *Řízení bezpečnosti informací: 2. rozšíření vydání o BCM*. 2. přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[5] KAPPEL, Jason, Toby J. VELTE a Anthony T. VELTE. *Microsoft Virtualization with Hyper-V*. The McGraw-Hill Companies, 2009. ISBN 978-0-07-161404-7.

[6] LUKÁČ, Ľubomír. *IT management*. 1.vyd. Brno: Computer Press, 2011, 208 s. ISBN 978-80-251-3378-1.

[7] MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. *Hacking bez záhad*. 1. vyd. Praha: Grada, 2007. ISBN 978-80-247-1502-5.

[8] FAKULTNÍ NEMOCNICE OLOMOUC. *Analýza stávajícího stavu lokální sítě Fakultní nemocnice Olomouc*. 2013

[9] FAKULTNÍ NEMOCNICE OLOMOUC. *Datové centrum pro Fakultní nemocnici Olomouc*. 2012

[10] BELL, A. Michael. Use Best Practices to Design Data Center Facilities. *Gartner* [online]. April 22, 2005 [cit. 2014-03-20]. Dostupné z: http://it.northwestern.edu/bin/docs/DesignBestPractices_127434.pdf

[11] CISCO. Virtual Switching Systems (VSS). *Cisco.com* [online]. [cit. 2014-03-19]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vss.html

[12] FAKULTNÍ NEMOCNICE OLOMOUC. Historie. *Fakultní nemocnice Olomouc* [online]. [cit. 2014-01-27]. Dostupné z: http://www.fnol.cz/historie.asp

[13] FAKULTNÍ NEMOCNICE OLOMOUC. O nás. *Fakultní nemocnice Olomouc* [online]. [cit. 2014-01-27]. Dostupné z: http://fnol.cz/o-nas.asp

[14] FAKULTNÍ NEMOCNICE OLOMOUC. Loga ke stažení. *Fakultní nemocnice Olomouc* [online]. [cit. 2014-01-27]. Dostupné z: http://www.fnol.cz/loga-ke-stazeni.asp

[15] GOOGLE. Olomouc – Mapy Google. *Google.cz* [online]. [cit. 2014-01-27]. Dostupné z: https://www.google.com/maps/place/Olomouc/@49.6013662,17.2649871,14z/data=!4m2!3m1!1s0x47124e8311181853:0x400af0f66159470

[16] GOWANS, Doug. *Asynchronous or Synchronous Replication..?* [online]. [cit. 2014-05-02]. Dostupné z: http://blogs.msdn.com/b/douggowans/archive/2008/12/12/asynchronous-or-synchronous-replication.aspx

[17] IBM. BladeCenter H Chassis. *IBM.com* [online]. [cit. 2014-02-02]. Dostupné z: http://www-03.ibm.com/systems/bladecenter/hardware/chassis/bladeh/

[18] IBM. IBM Storwize V7000 Information Center. *IBM.com* [online]. Feb 14, 2014 [cit. 2014-03-02]. Dostupné z: http://pic.dhe.ibm.com/infocenter/storwize/ic/index.jsp?topic=%2Fcom.ibm.storwize.v7000.720.doc%2Fsvc_easy_tier.html

[19] IBM SYSTEMS MAGAZINE. RPO/RTO Defined. *IBM Systems magazine* [online]. [cit. 2014-03-23]. Dostupné z: http://www.ibmsystemsmag.com/mainframe/administrator/highavailability/backups_on_file/RPO-RTO-Defined/

[20] ITIL. WHAT IS ITIL®?. *Itil-officialsite.com* [online]. [cit. 2014-03-30]. Dostupné z: http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx

[21] MICROSOFT. Hyper-V Overview. *Microsoft.com* [online]. [cit. 2014-03-25]. Dostupné z: http://technet.microsoft.com/en-us/library/hh831531.aspx

[22] MICROSOFT. Microsoft TechNet. *Microsoft.com* [online]. [cit. 2014-01-27]. Dostupné z: http://technet.microsoft.com/en-US/

[23] MICROSOFT. Network Recommendations for a Hyper-V Cluster in Windows Server 2012. *Microsoft.com* [online]. [cit. 2014-03-25]. Dostupné z: http://technet.microsoft.com/en-us/library/dn550728.aspx

[24] MICROSOFT. Understand and Troubleshoot Hyper-V Replica in Windows Server "8" Beta. *Microsoft.com* [online]. [cit. 2014-03-25]. Dostupné z: http://www.microsoft.com/en-us/download/details.aspx?id=29016

[25] MICROSOFT. Virtual Server architecture. *Microsoft.com* [online]. [cit. 2014-03-25]. Dostupné z: http://technet.microsoft.com/en-us/library/cc708365(v=ws.10).aspx

[26] MICROSOFT. Virtual Server feautures. *Microsoft.com* [online]. [cit. 2014-03-25]. Dostupné z: http://technet.microsoft.com/en-us/library/cc720335(v=ws.10).aspx

[27] MICROSOFT AZURE. Hyper-V Recovery Manager. *Azure.microsoft.com* [online]. [cit. 2014-05-05]. Dostupné z: http://azure.microsoft.com/en-us/services/recovery-manager/

[28] MOLÍK, Václav. Datová centra realisticky. *Systemonline.cz* [online]. [cit. 2014-03-20]. Dostupné z: http://www.systemonline.cz/sprava-it/datova-centra-realisticky.htm

[29] PAŠEK, David. Tři z nejsilnějších - srovnání serverové virtualizace VMware vs. Citrix vs. Microsoft. V*mwarenews.cz* [online]. [cit. 2014-03-23]. Dostupné z: http://www.vmwarenews.cz/vmw/vmwnews.nsf/0/53BB1B111BE5A818C12575E5005F83A6

[30] RITTAL. RITTAL LCP Liquid Cooling Package pour l'industrie. *Rittal.com* [online]. [cit. 2014-04-21]. Dostupné z: http://www.rittal.com/fr-fr/content/fr/unternehmen/presse/pressemeldungen/pressemeldung_detail_25921.jsp

[31] STRATUS TECHNOLOGIES. Stratus ftServer Architecture. *Stratus.com* [online]. [cit. 2014-02-02]. Dostupné z: http://stratus.com/Products/Platforms/ftServerSystems/ftServerArchitecture

[32] TATE, Jon, Pall Beck, Hector Hugo Ibarra, Shanmuganathan Kumaravel a Libor Miklas. *Introduction to Storage Area Networks and System Networking* [online]. 3. vyd. IBM Redbooks, 2013. [cit. 2014-03-28]. Dostupné z: http:// redbooks.ibm.com/redbooks/pdfs/sg245470.pdf

[33] TATE, Jon, Rafael Vilela Dias, Ivaylo Dikanarov, Jim Kelly a Peter Meschler. *IBM System Storage SAN Volume Controller and Storwize V7000 Replication*

Family Services [online]. 5. vyd. IBM Redbooks, 2012. [cit. 2014-03-25]. Dostupné z: http://www.redbooks.ibm.com/redbooks/pdfs/sg247574.pdf

[34] TAYLLORCOX. Certifikace Datacentra. Tayllorcox.com [online]. [cit. 2014-03-20]. Dostupné z: http://www.tcox.cz/tier-certifikace-datova-centra.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ARP	Address Resolution Protocol
Atd.	A tak dále
BS	British Standards
CCTA	Central Computer and Telecommunications Agency
CCTV	Closed Circuit Television
CIFS	Common Internet File System
CMOS	Complementary Metal Oxide Semiconductor
ČSN	Česká státní norma
DAG	Database Availability Group
DDDS	Domluvená doba dostupnosti služeb
DHCP	Dynamic Host Configuration Protocol
DICOM	Digital Imaging and Communications in Medicine
DVS	Doba výpadku služby
ECC	Error Correcting Code
EPS	Elektrická požární signalizace
FC	Fibre Channel
FCoE	Fibre Channel over Ethernet
FHRP	First Hop Redundancy Protocol
FUP	Fair User Policy
FW	Firewall
GB	Giga Byte
GE	Gigabit Ethernet
GSM	Groupe Spécial Mobile
HBA	Host Bus Adapter

HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
FNOL	Fakultní nemocnice Olomouc
IBM	Výrobce informačních technologiích
ICT	Informační a komunikační technologie
IDS	Intrusion Detection System
IEEE	Institute of Eelectrical and Electronics Engineers
IIS	Internet Information Services
IP	Internet Protocol
IPS	Intrusion Prevention System
iSCSI	Internet Small Computer System Interface
IT	Informační technologie
ISO/OSI	International Standards Organization / Open Systen Interconnection
ITIL	Information Technology Infrastructure Library
NIS	Nemocniční informační systém
kVA	Kilo Volt Amper
kW	Kilo watt
LAN	Local Area Network
LCP	Liquid Cooling Package
MB	Mega Byte
MPIO	Multipath Input Output
MTBF	Mean Time Between Failures
MTBSI	Mean Time Between Service Incident
MTTR	Mean Time To Repair
NAS	Network Attached Storage

NFS	Network File System
Obr.	Obrázek
PDCA	Plan, Do, Check, Act
PDU	Power Distribution Unit
PVRST	Per VLAN Rapid Spanning Tree
PZS	Poplachové zabezpečovací systémy
RACK	Uzamykatelný rozvaděč pro informační technologie
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memmory
RIP	Routing Information Protocol
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAN	Storage Area Network
SCSI	Small Computer System Interface
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SLR	Service Level Requirement
SNMP	Simple Network Management Protocol
SSD	Solid State Disk
SW	Software
Tab.	Tabulka
TB	Tera Byte
TCP/IP	Transmission Control Protocol/Internet Protocol
U	Unit
UPS	Uninterruptible Power Supply
VHD	Virtual Hard Disk

VHDX	Virtual Hard Disk
VLAN	Virtual Local Area Network
VM	Virtual Machine
VRLA	Valve Regulated Lead Acid
VSS	Virtual Switching System
WAN	Wide Area Network
XML	Extensible Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK