Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Centralizace prostředků IT vybrané firmy prostřednictvím virtualizace

Bc. Pavel Frass

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Pavel Frass

Informatika

Název práce

Centralizace prostředků IT vybrané firmy prostřednicrvím virtualizace

Název anglicky

IT centralization of selected company using virtualization

Cíle práce

Diplomová práce je zaměřena na problematiku centralizace současných IT prostředků. Hlavním cílem diplomové práce je demonstrovat využití technologie virtualizace na platformě VMware pro centralizaci IT infrastruktury vybrané firmy.
Dílčí cíle jsou:
- představení produktů VMware
- analýza stávajícího prostředí
- návrh a realizace nového řešení
- správa a monitoring
- závěry a doporučení

Metodika

Teoretickáí část diplomové práce klade důraz na teoretické seznámení s problematikou virtualizace a stručně představuje produkty firmy VMware. Obsažené informace autor čerpá z uvedené literatury a internetových zdrojů. Praktická část práce je zaměřena na analýzu stávajícího prostředí, návrh a realizaci nové infrastruktury. Uvádí jednotlivé kroky od volby vhodného serverového hardware, přípravy síťové infrastruktury, implementace produktů VMware až po migraci stávajících prostředků. Samostatná část diplomové práce se zabývá možnostmi správy a monitoringu nového prostředí. Poslední kapitola je věnována závěrům a doporučením.

Doporučený rozsah práce

60 – 70 stran

Klíčová slova

virtualizace, vmware, esxi, hypervisor, cisco, LAN, monitoring, mobilní aplikace

---

Doporučené zdroje informací

KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.

RUEST, Danielle a Nelson RUEST. Virtualizace: podrobný průvodce. Vyd. 1. Brno: Computer Press, 2010. ISBN 978-80-251-2676-9.

VMware(r) Education Services, VMware, Inc., VMware vSphere: Install, Configure, Manage, ESXi 5.0 and vCenter Server 5.0, Student Manual Volume 1, Part Number EDU-ENG-ICM5-LEC1-STU

VMware(r) Education Services, VMware, Inc., VMware vSphere: Install, Configure, Manage, ESXi 5.0 and vCenter Server 5.0, Student Manual Volume 2, Part Number EDU-ENG-ICM5-LEC2-STU

Předběžný termín obhajoby

2015/06 (červen)

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Elektronicky schváleno dne 31. 10. 2014

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2014

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 23. 03. 2015

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Centralizace prostředků IT vybrané firmy prostřednictvím virtualizace" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.3.2015 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi Ph.D., za cenné rady, připomínky a odborné vedení této diplomové práce. Dále děkuji společnosti První novinová společnost a.s. za možnost realizace praktické části.

Centralizace prostředků IT vybrané firmy prostřednictvím virtualizace

---

IT centralization of selected company using virtualization

Souhrn

Diplomová práce je zaměřena na problematiku centralizace současných IT prostředků pomocí virtualizace. První část práce je věnována představení technologie virtualizace v obecné rovině a seznámení s konkrétními produkty firmy VMware, které budou implementovány v praktické části.

Praktická část práce je zaměřena na analýzu stávajícího firemního IT prostředí, návrh a realizaci nového řešení postaveného na virtualizačních technologiích společnosti VMware. Realizace řešení pokrývá výběr serverového hardware, instalaci, konfiguraci a migraci stávajících IT prostředků do nového prostředí. Samostatná kapitola je věnována správě a monitoringu virtuálního prostředí.

Summary

This thesis is focused to the centralization of current IT resources through virtualization. The first part focuses on the introduction of virtualization technology in general and familiarity with specific products of VMware, which will be implemented in the practical part.

The practical part is focused to the analysis of existing corporate IT environment, design and implement a new solution built on VMware technologies. Implementation of solutions covers selection of server hardware, installation, configuration and migration of existing IT resources into a new environment. A separate chapter is devoted to managing and monitoring virtual environments.

Klíčová slova: Virtualizace, VMware, ESXi, Hypervisor, Cisco, LAN, Monitoring, Mobilní aplikace

Keywords: Virtualization, VMware, ESXi, Hypervisor, Cisco, LAN, Monitoring, Mobile application

OBSAH

1 Úvod

Virtualizace je ve světě IT fenomén již několik let. Počátky sahají až do 60. let 20. století, kdy s tímto konceptem přišla firma IBM u svých sálových počítačů. Jedná se o revoluční technologii, která přináší nový pohled na problematiku IT infrastruktury jako celku. Základní myšlenka virtualizace je taková, že na jednom fyzickém serveru je provozováno několik od sebe navzájem oddělených virtuálních strojů s různými operačními systémy, z nichž každý využívá společný hardware fyzického serveru. O řízení a přidělování zdrojů se stará mezivrstva VMM, označovaná jako hypervisor. Dnešní moderní serverové systémy jsou schopny poskytnout prostředky pro několik desítek až stovek virtuálních strojů. To má následně dopad na další součásti infrastruktury jako jsou datová úložiště, sítě, zabezpečení, zálohování a obnovu dat apod.

V době, kdy je kladen důraz na snižování provozních nákladů na IT, vysokou dostupnost, škálovatelnost a snadnou administraci, je virtualizace vhodný prostředek k dosažení těchto cílů. Díky ní je možná konsolidace fyzických serverů, které představují náklady v podobě pořizovací ceny, maintanance, elektrické energie, potřeby odpovídajících prostor, chlazení apod.

Nové technologie přináší i nové hrozby, které je potřeba si uvědomit a v co největší míře eliminovat. V případě virtualizace se jedná o zcela nový pohled na řadu oblastí, které s virtualizací zdánlivě nesouvisejí. Jako příklad může posloužit otázka systémového zabezpečení, kdy odcizení serveru s daty a jeho vynesení mimo firmu je záležitost zkopírování několika souborů s virtuálním strojem na přenosné médium.

Nasazení virtualizace výrazně zasahuje do chodu podnikového IT a vyžaduje nejednu změnu zaběhnutých procesů, což však zpravidla není na škodu. Poslední léta tuto technologii dostatečně prověřila a dnes již není otázka zda virtualizovat, ale spíše co a jakou cestou.

2 Cíl práce a metodika

2.1 Cíl práce

Diplomová práce je tematicky zaměřena na problematiku virtualizace serverů. Hlavním cílem práce je demonstrovat využití technologie virtualizace na platformě VMware pro centralizaci IT infrastruktury vybrané firmy. Dílčí cíle jsou:

- představení produktů firmy VMware, zejména těch, se kterými bude dále pracováno v praktické části
- analýza stávajícího firemního prostředí, posouzení vhodnosti virtualizace jednotlivých serverů
- návrh a realizace nového řešení vychází z výsledků analýzy. Zahrnuje zejména návrh fyzické a logické topologie, výběr a nákup nového HW (servery a disková pole), přípravu a konfiguraci prostředí, migraci fyzických serverů do virtuálního prostředí
- samostatná kapitola je věnována možnostem správy a monitoringu celého prostředí s využitím nativních nástrojů, dohledových a monitorovacích systémů třetích stran a aplikací pro chytré telefony a tablety.

2.2 Metodika

Teoretická část diplomové práce klade důraz na teoretické seznámení s problematikou virtualizace a stručně představuje produkty firmy VMware. Obsažené informace autor čerpá z uvedené literatury a internetových zdrojů.

Praktická část práce se zabývá analýzou stávajícího firemního IT prostředí společnosti První novinová společnost a.s., ve které je autor této diplomové práce zaměstnán na pozici Manažer oddělení IT infrastruktury. Je zodpovědný za projekt virtualizace v rozsahu od úvodní analýzy až po technickou realizaci.

Jsou vybrány fyzické servery vhodné pro virtualizaci a jsou odhadnuty potřebné parametry nového prostředí z hlediska výpočetního výkonu, kapacity operační paměti, síťové propustnosti a nároků na datové úložiště. Podrobně je zdokumentována příprava síťového prostředí, zejména konfigurace přepínačů a síťového subsystému na straně VMware. Předvedena je instalace a konfigurace jednoho fyzického serveru, který bude hostovat virtuální stroje a jeho začlenění do virtuální infrastruktury. Migrace stávajících fyzických serverů je řešena pomocí nástroje VMware Converter, který je detailněji

představen. Téma správy a monitoringu je prozkoumáno z několika pohledů. Prvním z nich je správa a monitoring hardwaru fyzických serverů. Druhým je správa a monitoring virtuální infrastruktury a třetím je správa a monitoring virtuálních strojů.

Na základě teoretických poznatků a výsledků praktické části práce jsou formulovány závěry diplomové práce.

3 Přehled řešené problematiky

3.1 Úvod do virtualizace

Na začátku této kapitoly je nutné vysvětlit několik pojmů, které s virtualizací souvisí, a se kterými bude pracováno i v dalších částech práce.

Hostitelský sytém (Host) je počítač na kterém je nainstalován a spuštěn virtualizační nástroj (VMM)

Virtual Machine Monitor (VMM) označován také jako hypervisor je mezivrstva, která provádí virtualizaci hardwaru hostitelského systému a tyto prostředky poskytuje virtuálním strojům.

Hostující systém (Guest) označován také jako Virtual Machine (VM). Jedná se konkrétní operační systém (např. Windows, Linux) spuštěný v prostředí VMM. Počet souběžně pracujících VM na jednom hostitelském systému se dnes pohybuje od desítek až stovek v závislosti na výkonu hostitelského systému a požadavkům na výkon VM.

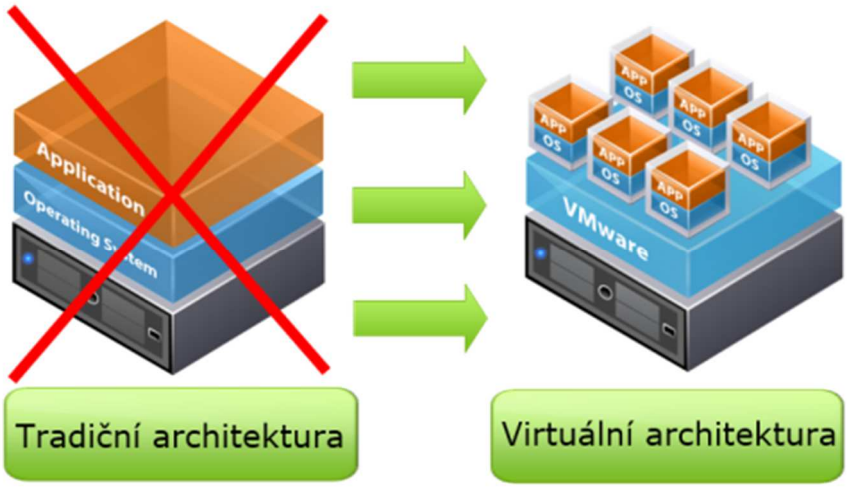
Virtuální infrastruktura je termín, kterým označujeme prostředí jako celek. Zahrnuje servery, síťové prvky, disková pole, virtualizační software apod.

Konsolidace znamená zmenšení počtu fyzických serverů

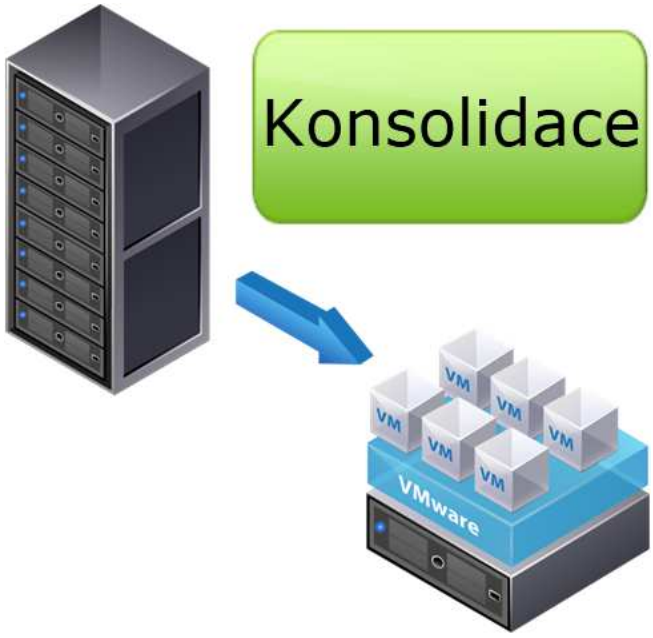
Zapouzdření (containment) je struktura VM (adresář, konfigurační soubory, datové soubory obsahující data VM)

Hovoříme-li o virtualizaci, máme na mysli množinu technologií a postupů, které umožňují využít jeden zdroj (představme si například server a jeho komponenty) pro více, než jeden operační systém[1]. Virtuální stroj je počítač uložený v podobě několika souborů na datovém úložišti. Běh virtuálních strojů řídí VMM mezivrstva, která se stará o přiřazování zdrojů (procesor, paměť, periferie apod.) mezi jednotlivé virtuální stroje a zajišťuje jejich vzájemné oddělení. I z tohoto důvodu je virtualizace vhodnou metodou k dosažení konsolidace fyzických serverů.

[1] (Prodělal, 2014)



Obrázek 1 - virtualizace serverů



Obrázek 2 - konsolidace serverů

3.1.1 Typy virtualizačních systémů

Parciální (částečná) virtualizace je zastoupena v moderních operačních systémech již nějakou dobu v podobě virtuální paměti.

OS-level virtualizace funguje tak, že více systémů sdílí jedno jádro. Jedná se o virtualizaci v rámci jednoho operačního systému. Představiteli tohoto typu virtualizace je chroot (Linux), jail (BSD), Linux-VServer, Virtuozzo, OpenVZ.

Paravirtualizace znamená pouze částečnou abstrakci na úrovni hostovaného stroje (VM). Hostovaný operační systém ví o existenci virtualizační vrstvy. Do této skupiny patří např. XEN (patří také do plné virtualizace), Oracle VM, SUN xVM, VMware Workstation, Microsoft Hyper-V.

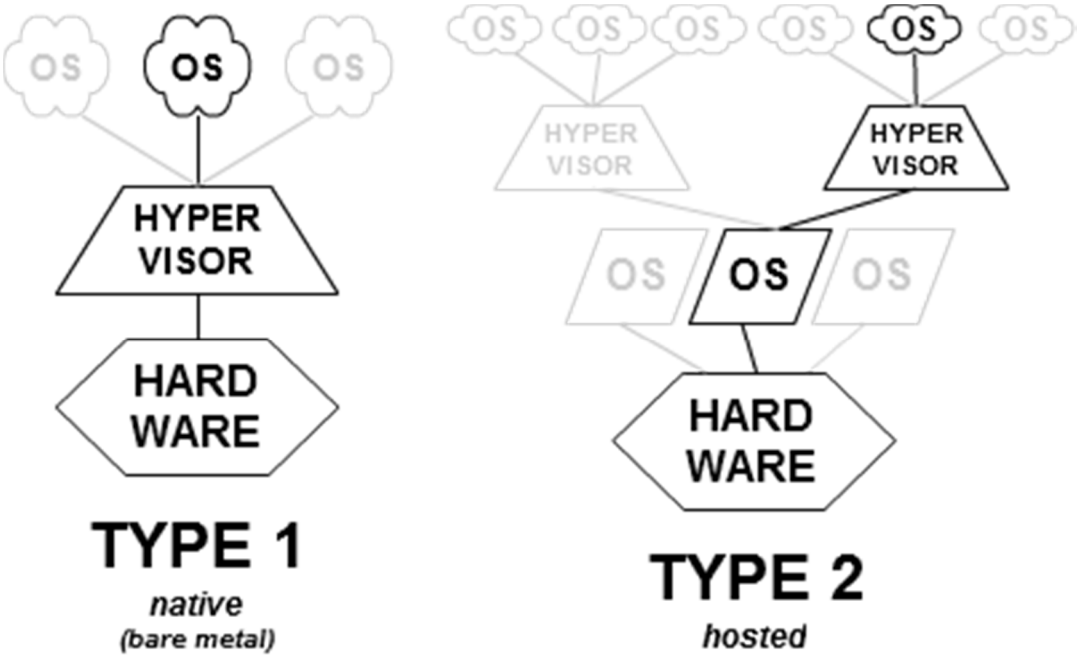
Plná virtualizace simuluje hardware a virtualizovaný (hostovaný) systém nemusí vědět o tom, že je virtualizován. Zástupci plné virtualizace jsou VMware ESXi, XEN, KVM.

HW-assisted virtualizace využívá podpory ze strany procesorů (pomocné instrukce) a využívá ji většina plných virtualizací.

Paravirtualizaci, plnou virtualizaci a HW-assisted virtualizaci dále dělíme na další dva typy.

- host-based (type-2) – v tomto případě běží hypervisor nad existujícím operačním systémem (Windows, Linux apod.). Do této skupiny patří produkty VMware Workstation (Server), Sun VirtualBox, Parallels Workstation, Microsoft Virtual PC[2]
- bare-metal (native, type-1) – hypervisor běží přímo na hardware. Do této skupiny patří produkty VMware ESXi, Citrix Xen Server, Microsoft Hyper-V, Oracle VM[3]

[2] (Peterka, 2011)
[3] (Matyska, 2011)



Obrázek 3 - native vs. hosted virtualizace

3.1.2 Historie virtualizace

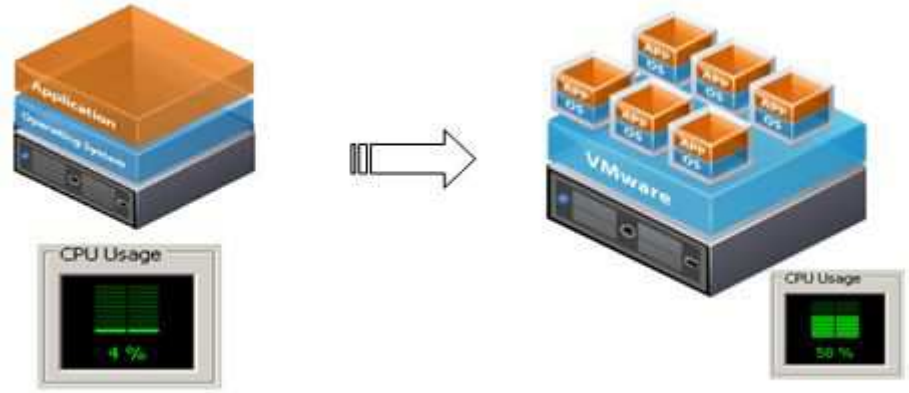
Počátky virtualizace sahají až do 60. let 20. století, kdy s hardwarovou virtualizací na úrovni procesoru přišla firma IBM. Důvodem byla snaha o lepší využití systémových prostředků sálových počítačů IBM CP – 40. Další masivní vzestup virtualizace nastal koncem 20. století v době, kdy je díky nárůstu výpočetního výkonu potřeba lépe konsolidovat a využívat fyzické servery.

V roce 1998 je založena firma VMware, která si nechává patentovat virtualizační technologie. V roce 1999 uvádí produkt VMware Virtual Platform (nyní VMware Workstation). O dva roky později uvádí na trh první verzi ESX serveru, VMware ESX 1.0. Jedná se o bare-metal virtualizaci. V roce 2003 uvádí VMware technologii vMotion (bezvýpadková migrace VM mezi fyzickými stroji). Ve stejném roce přichází další virtualizační nástroj XEN od firmy Citrix, který je však technologicky daleko za technologiemi VMware. V roce 2005 a 2006 je implementována podpora virtualizační technologie v procesorech Intel (Intel-VT) a AMD (AMD-V). V roce 2007 vzniká KVM (Kernel Virtual Machine) na platformě Linux. Jedná se o open source řešení. V roce 2008 přichází firma Microsoft se svým řešením nazvaným Hyper-V[4].

[4] (Prodělal, 2010)

3.1.3 Základní vlastnosti virtualizace

Základní rozdíl mezi tradiční a virtuální infrastrukturou ilustruje obrázek č. 4. Zatímco u tradiční infrastruktury je na jednom fyzickém serveru pouze jeden operační systém, virtuální infrastruktura dovoluje na stejném fyzickém serveru provozovat několik systémů současně. To vede k efektivnějšímu využití zdrojů fyzického serveru.



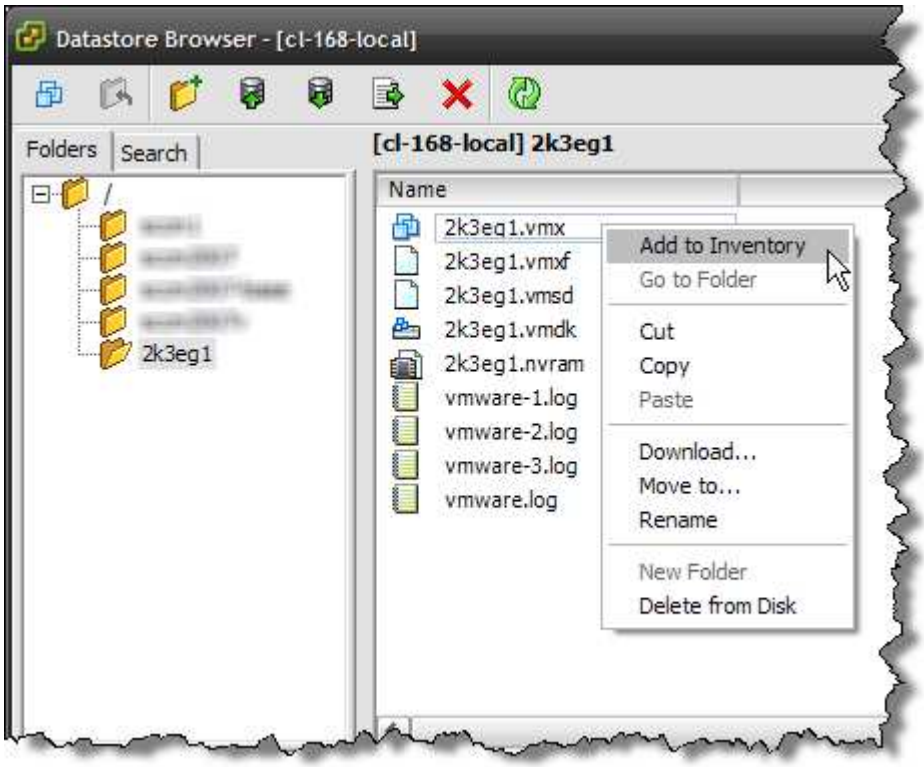
Obrázek 4 - fyzická vs. virtuální infrastruktura

Virtuální infrastruktura má svá specifika, která se podstatně liší od tradiční fyzické infrastruktury. Ty nejdůležitější jsou vysvětleny níže.

Oddělení operačního systému od hardware. Hardware tvoří virtuální vrstva. Z této skutečnosti plyne jedna z mnoha výhod virtualizace, a to je nezávislost na konkrétním hardware (kompatibilita napříč x86 servery). To umožňuje snadné přenášení virtuálních strojů mezi fyzickými servery.

Zapouzdření (containment) virtuálních strojů. Virtuální stroje jsou reprezentovány v podobě softwarových kontejnerů, které si lze představit jako adresář obsahující veškeré informace o virtuálním stroji. Nachází se zde konfigurační soubory definující virtuální hardware, konkrétní operační systém s aplikacemi apod. Obrázek č. 5 znázorňuje strukturu virtuálního stroje na platformě VMware[5].

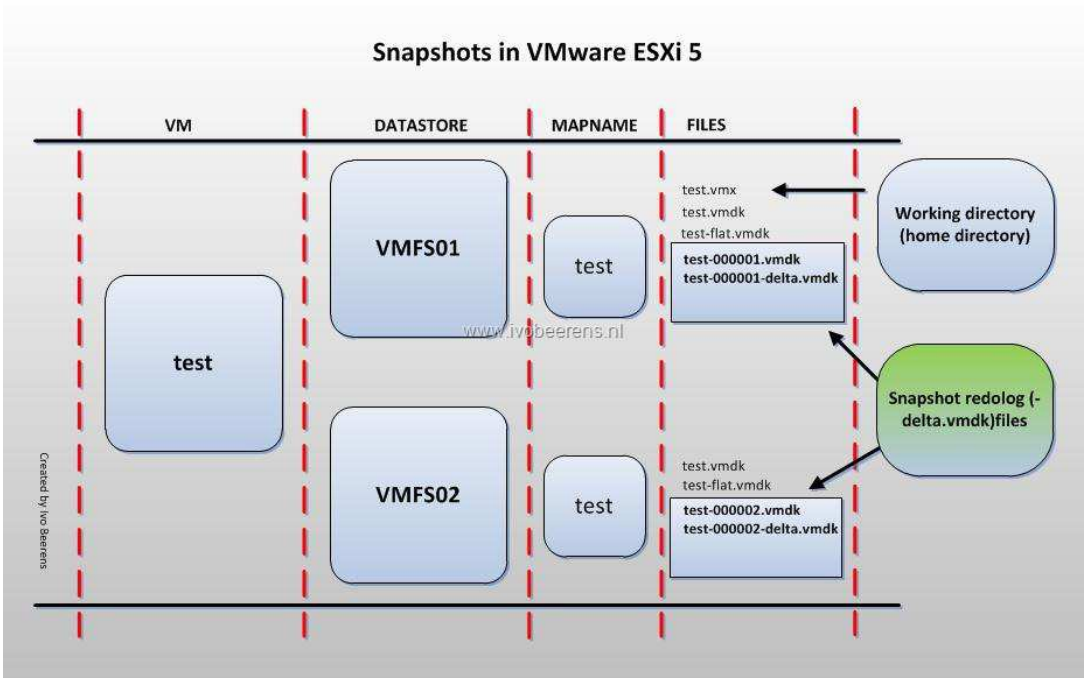
[5] (VCRITICAL, 2009)



Obrázek 5 - struktura virtuálního stroje na platformě VMware

Izolace virtuálních strojů zabezpečuje to, že se jednotlivé běžící virtuální stroje nemohou vzájemně ovlivňovat (např. nemají přístup do operační paměti, diskového úložiště ostatních virtuálních strojů). Z tohoto pohledu se chovají jako fyzicky oddělené stroje. Případné havarování jednoho virtuálního stroje nesmí ovlivnit běh ostatních virtuálních strojů.

Snapshoty umožňují uložit aktuální stav virtuálního stroje a v budoucnu se do tohoto stavu vrátit. Veškerá data od vytvoření snapshotu jsou ukládána do samostatného delta souboru. Snapshotů může být na jednom virtuálním stroji více, podporováno je také větvení, odstraňování jednotlivých snapshotů a jejich spojování. Jedná se o velice užitečnou vlastnost, která je často využívána ve chvíli, kdy je potřeba na virtuálním stroji testovat, instalovat aktualizace a obecně provádět rizikové zásahy, které mohou virtuální stroj poškodit z hlediska běhu a stability operačního systému a aplikací. Na principu snapshotů rovněž fungují některé produkty na zálohování virtuálních strojů. Strukturu snapshotu VMware ESXi 5 znázorňuje obrázek č. 6.

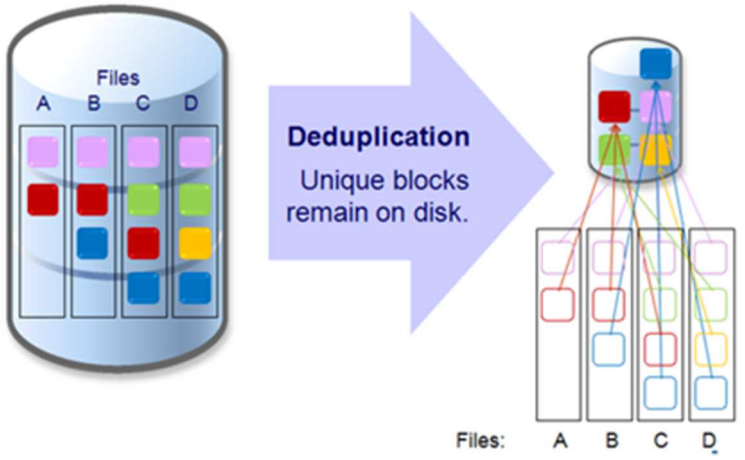


Obrázek 6 - snapshoty ve VMware ESXi 5

Klonování virtuálních strojů umožňuje vytvoření identické kopie existujícího virtuálního stroje. Je to vhodná metoda v případě, že potřebujeme několik virtuálních strojů se stejným operačním systémem. V takovém případě klonování usnadní spoustu práce. Tato metoda může mít i svá úskalí, například pokud je potřeba vytvořit několik virtuálních strojů s operačním systémem Windows. V takovém případě je jako první krok potřeba naklonované virtuální stroje dokonfigurovat nástrojem Sysprep[6]. Ten zajistí odstranění jednoznačných identifikátorů systému a vytvoří záznamy nové a jedinečné pro každý virtuální stroj. Toto je nezbytně nutné nejen v korporátním prostředí, kde může existence více počítačů se stejnými identifikátory způsobit nemalé problémy.

Datová deduplikace slouží k úspoře volného místa na diskových úložištích a v operační paměti hostujícího serveru. Funguje na principu detekce stejných souborů či bloků dat. Tyto duplicity následně odstraňuje (na základě kontrolních součtů) a ukládá pouze odkaz na původní zdroj. Zajímavostí je, že do roku 2020 se předpokládá nárůst informací na 35 zettabytů oproti 0,8 zettabytů v roce 2009[7].

[6] (Microsoft Corporation, 2012)
[7] (Skohoutilová, 2011)



Obrázek 7 - datová deduplikace na úrovni diskových bloků

Škálovatelnost nebo také rozšiřitelnost je vlastnost, která dovoluje měnit hardwarovou konfiguraci virtuálních strojů. V případě potřeby lze virtuálnímu stroji navýšit operační paměť, zvýšit počet jader procesoru, či přidat další disk nebo síťovou kartu. Oproti fyzickému serveru, kde tato potřeba nemusí být vůbec řešitelná, to je ve virtualizovaném prostředí velice jednoduché a efektivní. Některé modifikace v konfiguraci hardwaru lze provádět i za běhu virtuálního stroje.

3.1.4 Datová úložiště ve světě virtualizace

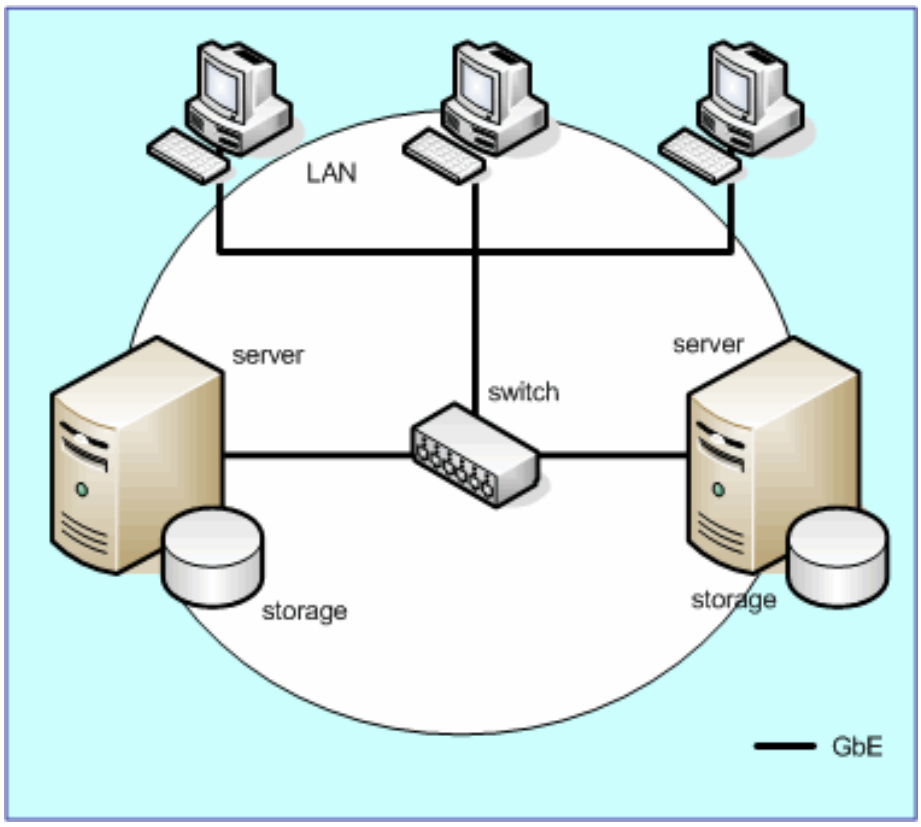
Datová úložiště jsou důležitou součástí virtuální infrastruktury. Jsou sdílena jednak mezi více hostitelskými systémy, tak mezi hostujícími systémy (virtuálními stroji). Správný návrh a výběr technologie a kapacity datového úložiště je stěžejní bod při návrhu virtuální infrastruktury.

3.1.4.1 Typy datových úložišť dle připojení

Připojení datových úložišť můžeme rozdělit do třech základních kategorií. Jsou to úložiště typu DAS, SAN a NAS. Ve virtuálním prostředí se většinou setkáváme s kombinací více druhů připojení v rámci jednoho prostředí.

DAS (Directly Attached Storage) neboli přímo připojená úložiště. Jedná se o disky, disková pole, optické mechaniky připojené k jednomu konkrétnímu fyzickému stroji. Neposkytují žádnou možnost sdílení mezi vícero fyzickými stroji, myšleno na úrovni hardware. Jejich nevýhodou je nedostupnost dat v případě poruchy fyzického stroje a

obtížnější rozšiřitelnost kapacity. Limitující může být také omezená délka připojovacího kabelu, pakliže se jedná o SCSI diskové pole[8].



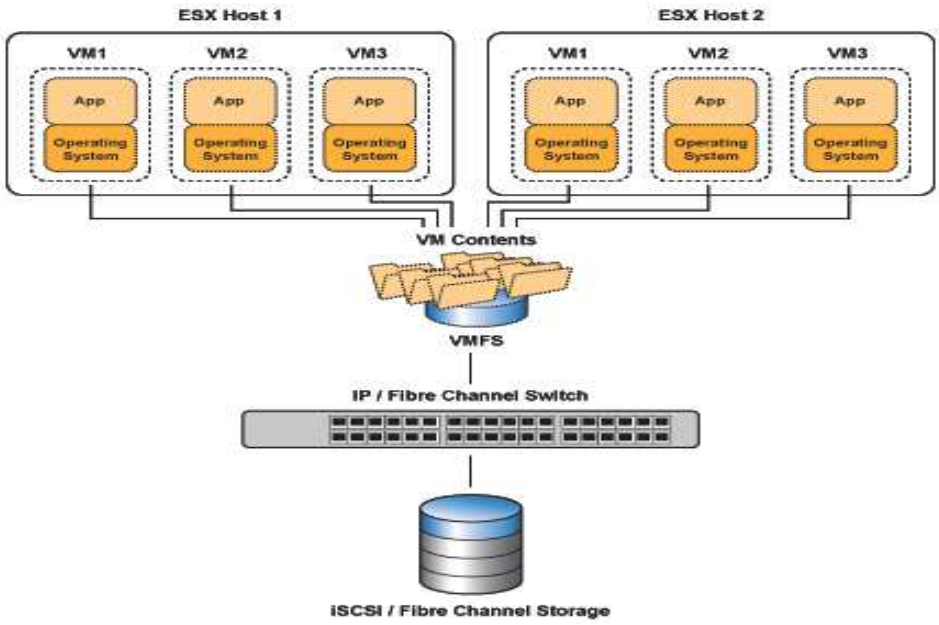
Obrázek 8 - schéma DAS úložiště

SAN (Storage Area Network) je samostatná síť, která slouží k propojení externích zařízení (diskové pole, páskové knihovny) se servery a přenosu dat mezi nimi. Vznikla díky vzrůstajícím požadavkům na zabezpečení a konsolidaci. Pracuje s bloky dat, nikoliv s celými soubory (oproti NAS přístupu, viz níže). Dříve havárie fyzického serveru s datovým úložištěm připojeným metodou DAS často znamenala ztrátu dat. Toto sítě SAN do značné míry eliminují. U běžných SAN se využívá protokolu Fibre Channel a jako nosné médium je použito optické vlákno. Hojně využívaný je také protokol iSCSI, který využívá pro přenos SCSI paketů zapouzdření do protokolu TCP/IP. Hlavní výhody SAN oproti DAS jsou[9]:

- fyzické oddělení dat od serverů
- sdílení zdrojů mezi více serverů

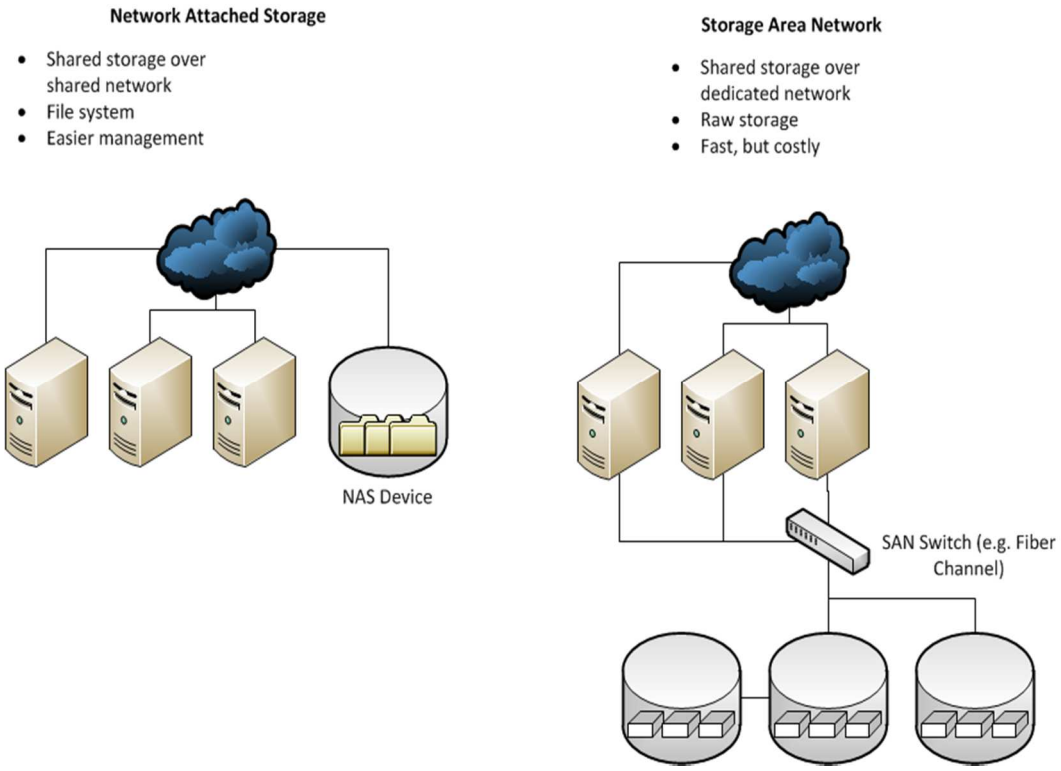
[8] (VAHAL s.r.o., 2009)
[9] (Bartolšic, 2013)

- vyšší datová propustnost
- podpora clusterových řešení
- vysoká dostupnost
- centralizovaná správa, škálovatelnost
- umožňují snížit růst provozních nákladů a zvýšit celkovou využitelnost diskových polí



Obrázek 9 - příklad použití úložiště typu SAN ve virtuální infrastruktuře

NAS (Network Attached Storage) v překladu úložiště na síti. Jedná se o sdílené úložiště připojené k lokální síti LAN, kde se využívá TCP/IP protokolu. Pracuje se přímo se soubory. Oproti technologii SAN, která je spíše určena pro připojení serverů k síťovému úložišti, je NAS určen pro připojení koncových uživatelů. Realizace NAS úložiště může být buď v podobě služby, která je spuštěna nad operačním systémem, specializované jednoúčelové distribuci (FreeNAS), nebo v podobě samostatného boxu. Přístup k datům je nejčastěji realizován pomocí protokolů NFS, SMB/CIFS či AFP. Bezpečnost dat je řešena použitím více disků v jednom RAID poli. Jedná se o relativně levné řešení vhodné například pro zálohování, sdílená uživatelská data apod.



Obrázek 10 - rozdíl mezi NAS a SAN

3.1.4.2 Typy souborových systémů

Virtualizace s sebou přináší také odlišné požadavky na vlastnosti souborových systémů. Důležitým požadavkem je možnost přístupu více systémů na jedno místo na disku bez poškození dat a bez toho, aniž by došlo k vzájemnému ovlivnění. Ve virtuální infrastruktuře se proto používají tak zvané clusterové filesystémy.

Clusterový souborový systém je typ souborového systému, který umožňuje pracovat s daty na diskovém oddílu, který má připojen jeden a více operačních systému[10]. Při použití clusterového filesystému je nutné zajistit, aby v jednom okamžiku mohl s jedním souborem pracovat pouze jeden operační systém. Používá se metody distribuovaného zamykání souborů.

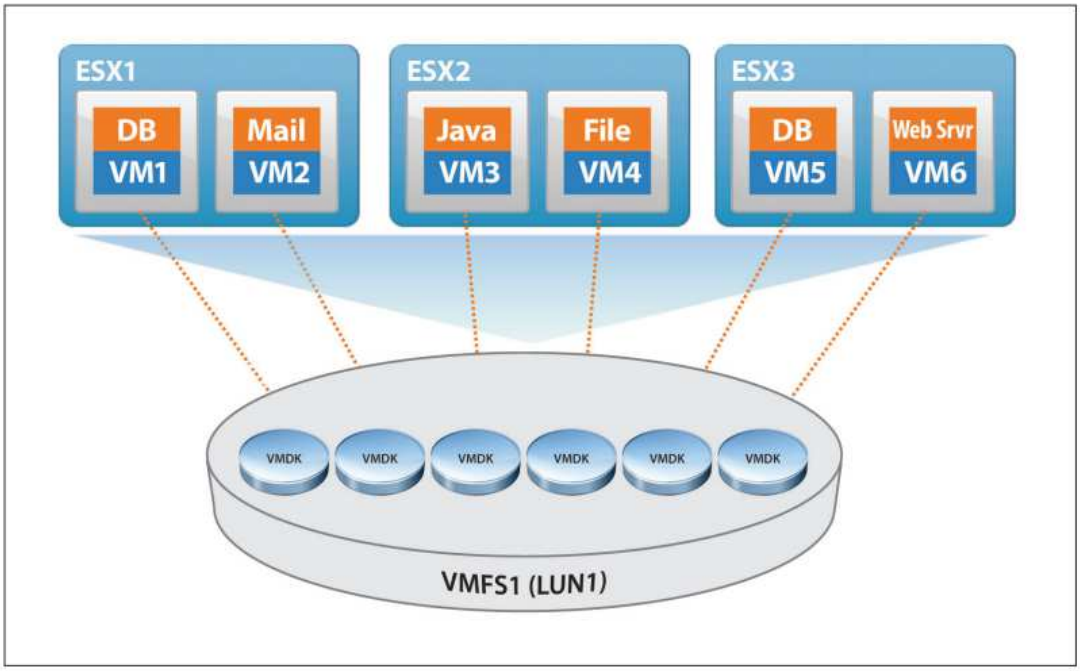
Konkrétní použití clusterového souborového systému VMFS (Virtual Machine File System) můžeme vidět na obrázku č. 11. Jsou zde tři ESX servery, každý z nich hostuje dva virtuální stroje. Každý virtuální stroj má připojen jeden disk, který se z pohledu virtuálního stroje jeví jako lokální SCSI disk. Ve skutečnosti se jedná o soubor (VMDK), uložený na clusterovém souborovém systému VMFS. VMFS oddíl je vytvořen přes celé diskové pole, resp. přes celou část LUN1. Každý virtuální stroj je uložen ve specifickém

[10] (Prodělal, 2014)

podadresáři (tvoří ho několik souborů) na VMFS. Pokud je virtuální stroj v zapnutém stavu, VMFS zamkne přístup k těmto souborům pro ostatní ESX servery a zaručí, že virtuální stroj nebude otevřen více, než jedním ESX serverem[11].

Clusterových souborových systémů existuje celá řada. Kromě výše zmíněného VMFS, který je proprietární souborový systém společnosti VMware, jsou to například:

- Cluster Shared Filesystem (CSV) – Microsoft
- Global File System (GFS) – Red Hat
- General Parallel File System (GPFS) – IBM
- Oracle Cluster File System (OCFS) – Oracle
- Sun QFS



Obrázek 11 - Clusterový souborový systém VMFS

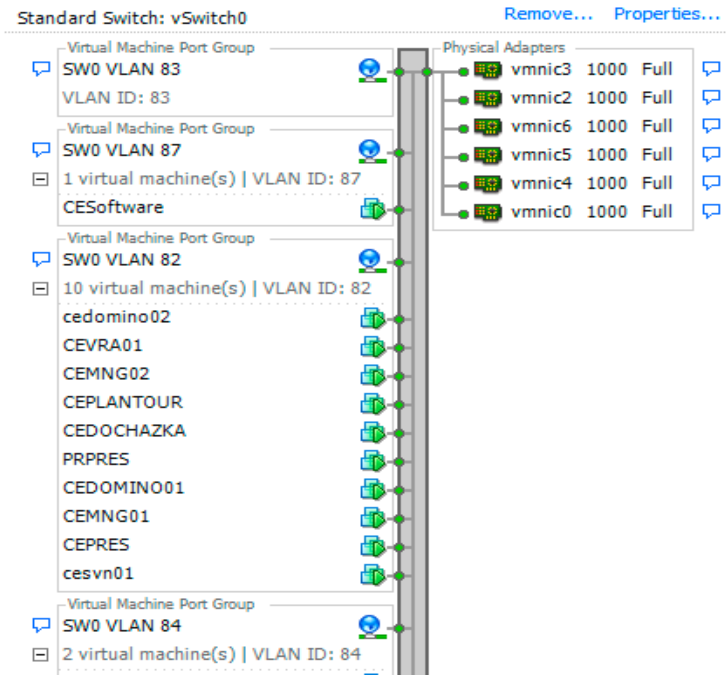
Souborové systémy uvnitř virtuálních strojů jsou závislé na použitém operačním systému a není zde rozdíl oproti běžným počítačům. Operační systémy firmy Microsoft využívají převážně NTFS či FAT32, Unix systémy například ext2 nebo ext3.

RDM (Raw Device Mapping) umožňuje připojení části diskového prostoru (LUN), přímo k virtuálnímu stroji a použít požadovaný souborový systém. Toto řešení se používá v případě potřeby vyššího výkonu diskového subsystému.

[11] (VMware Inc., 2012)

3.1.5 Sítě ve světě virtualizace

Při návrhu síťového prostředí pro virtuální infrastrukturu je důležité zajistit zejména propustnost a redundanci prvků (síťové karty, switche apod.). Je potřeba si uvědomit, že jednu síťovou kartu může využívat několik virtuálních strojů. Z tohoto důvodu se spojuje několik síťových karet do jednoho virtuálního celku. Tím lze dosáhnout větší propustnosti a zároveň redundance na úrovni síťového hardware. Tuto skutečnost znázorňuje obrázek č. 12. Vidíme zde 6. fyzických portů (fyzicky připojených do dvou samostatných switchů), které tvoří jeden celek. Tyto porty jsou přiřazeny do virtuálního switche, který zajišťuje síťovou konektivitu virtuálním strojům. Výpadek konektivity některé síťové karty, či switche tak neovlivní síťovou konektivitu virtuálních strojů (failover). Virtuální switch také řeší otázku rozdělování síťové zátěže (balancing). Více informací na toto téma je uvedeno v praktické části této diplomové práce. Dále je zpravidla potřeba řešit připojení virtuálních strojů do vícero lokálních sítí. To umožňuje použití technologie VLAN, kterou musí podporovat fyzické switche.

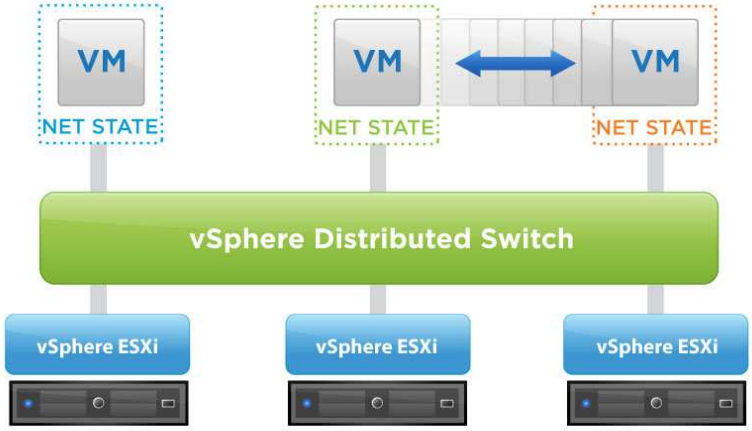


Obrázek 12 - ukázka síťového prostředí (VMware)

Distribuovaný switch[12] dává možnost správy síťového prostředí napříč několika fyzickými servery, na rozdíl od běžného virtuálního switche, který se konfiguruje pro každý server samostatně. Využití má tato technologie hlavně v rozsáhlých prostředích, kde

[12] (VMware Inc., 2014A)

značně zjednodušuje správu. Příkladem je switch Cisco Nexus 1000V, který je plně kompatibilní z hlediska nastavení, politik apod. s fyzickými Cisco switchi.



Obrázek 13 - distribuovaný switch

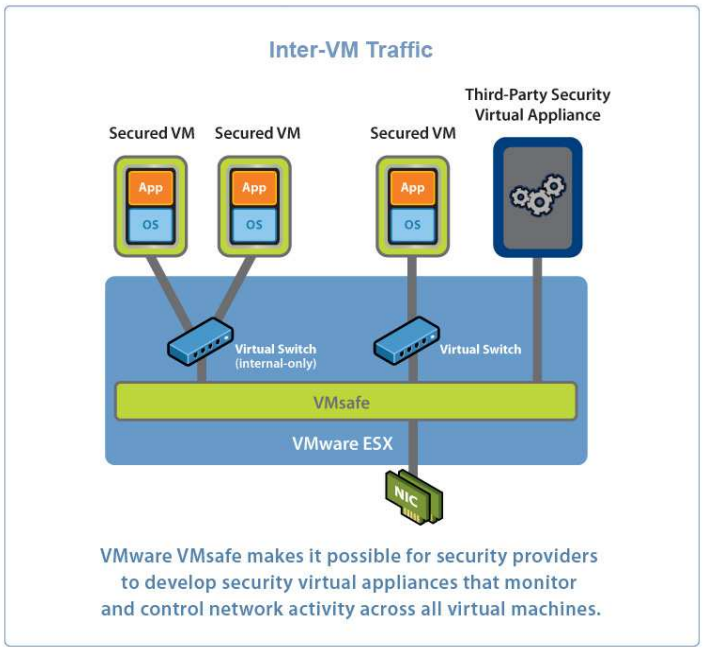
3.1.6 Bezpečnost prostředí

Fyzické zabezpečení můžeme chápat například jako umožnění přístupu k samotnému hardware pouze oprávněným osobám, zabezpečení kamerovým systémem, auditem přístupů apod. Do fyzického zabezpečení můžeme zahrnout také samotné prostory, kde je hardware umístěn. Zde jsou důležité zejména dva faktory. Prvním je dostatečně dimenzované napájení a záložní zdroje UPS pro všechny články infrastruktury. Druhým je zajištění dostatečně výkonného chlazení, správné umístění serverů (teplá, studená ulička), racky dostatečně daleko od klimatizačních jednotek, aby do nich v případě závady nenatekla zkondenzovaná voda. Výše napsané skutečnosti však musíme řešit také v případě nevirtualizovaného prostředí.

Softwarové zabezpečení, kde je potřeba brát v úvahu také možné chyby ve vlastním virtualizačním nástroji. Z tohoto pohledu je u virtualizovaného prostředí riziko o něco větší, právě díky použití virtualizační vrstvy. Stejně jako na jiných systémech musíme sledovat bezpečnostní rizika a reagovat na ně, například aplikováním bezpečnostních záplat. Ve virtualizovaném prostředí je potřeba si uvědomit, že odcizení několika serverů včetně dat je podstatně jednodušší, než u fyzických serverů. Útočníkovi stačí získat přístup na některý centrální prvek, který má přístup k datovému úložišti s virtuálními stroji a nic

mu nebrání jejich zkopírování. Z toho vyplývá skutečnost, že je potřeba dobře zabezpečit všechny prvky virtuální infrastruktury nastavením vhodných bezpečnostních politik (například samostatná oddělená VLAN na správu infrastruktury, nastavení administrátorských rolí, logování přístupů apod.).

Virtualizace přináší nový způsob ochrany virtuálních strojů z pohledu virových hrozeb. Díky virtualizační vrstvě, která je umístěna mezi hardware a software, můžeme virové hrozby detekovat dříve, než se dostanou dovnitř virtuálního stroje. Antivirová ochrana se v tomto případě přesouvá z koncových stanic na virtuální vrstvu. Klesá tím mimo jiné zatížení virtuálních strojů. S touto myšlenkou přichází společnost VMware, která oslovuje všechny hlavní hráče na poli bezpečnosti s požadavkem vytvořit produkt, který bude tuto problematiku řešit. Vzniká tak standard VMsafe, který je optimalizovaný pro virtualizaci s cílem vyplnit všechny mezery v zabezpečení virtuálního prostředí. Standard se týká tří základních částí. VMsafe-NET (ochrana sítě), VMsafe-CPU (kontrola prováděných operací) a VMsafe-STORAGE (disky a soubory)[13].



Obrázek 14 - rozhraní VMsafe

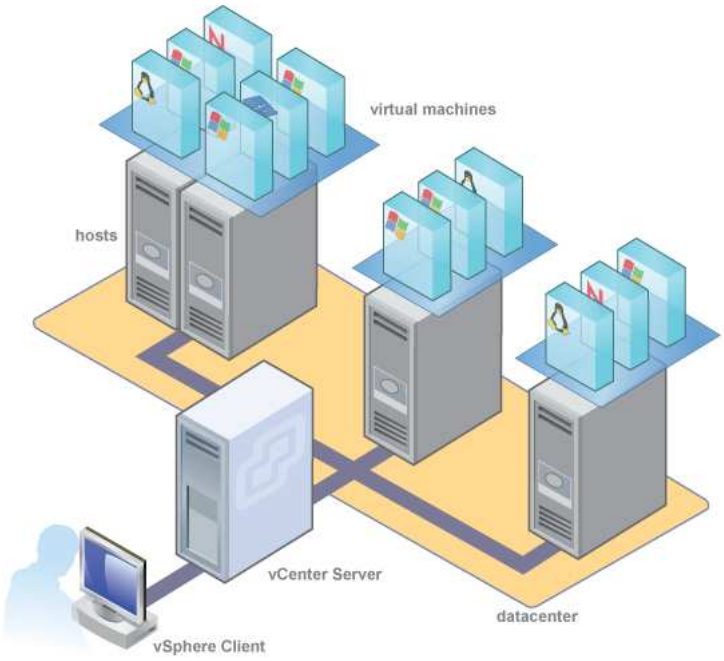
3.1.7 Správa virtuálního prostředí

Pro správu virtuální infrastruktury se využívají specializované nástroje, které umožňují konfiguraci, automatizaci, reportování a monitoring prostředí. Přístup k virtuální

[13] (Horák, 2014)

infrastruktuře umožňují buď pomocí grafického rozhraní nebo příkazů, které administrátor zadává přes příkazovou řádku. Výrobci virtualizačních nástrojů dávají k dispozici rovněž API rozhraní, pomocí kterého jsou jejich produkty ovladatelné. Toto rozhraní mohou využít administrátoři a výrobci třetích stran ve svých produktech.

Společnost VMware umožňuje správu svého prostředí produktem vCenter Server, ke kterému se administrátor připojuje pomocí konzole (vSphere Client). vCenter server umožňuje spravovat pouze VMware infrastrukturu, na rozdíl od řešení například společnosti Microsoft. Citrix dodává ke správě svého prostředí nástroj XenCenter, řešení společnosti Microsoft se jmenuje System Center Virtual Machine Manager.



Obrázek 15 - vCenter Server

3.2 Produkty a nástroje společnosti VMware

Společnost VMware poskytuje celou řadu produktů a nástrojů pro virtualizaci datových center, cloudové infrastruktury, desktopů a produkty pro stolní počítače. Vzhledem k velkému počtu těchto produktů se ve své diplomové práci omezím pouze na produkty pro virtualizaci datových center, se kterými bude pracováno v praktické části. Jednotlivé technologie použité v rámci implementace budou podrobněji představeny v praktické části.

3.2.1 vSphere ESXi

vSphere ESXi je virtualizační vrstva (hypervisor), která odděluje hardware fyzického serveru, řídí zdroje a poskytuje je mezi virtuální stroje. Instaluje se na fyzický server stejně jako jiný operační systém, nebo ji lze spustit bez potřeby instalace například z USB flash disku. Společnost VMware poskytuje zdarma základní verzi s určitým omezením funkcionalit a limitů fyzického stroje[14].

3.2.2 vCenter Server

Centralizovaný nástroj pro správu virtuální infrastruktury vCenter Server[15] zajišťuje konfiguraci virtuálního prostředí, zejména pak těchto oblastí:

- systémové nastavení ESXi serverů
- tvorba a konfigurace virtuální infrastruktury (datacentra, clustery)
- tvorba a konfigurace síťového prostředí (síťové adaptéry, virtuální switche, VLAN, teaming, balancing apod.)
- tvorba, konfigurace a manipulace virtuálních strojů (šablony, snapshoty, zdroje apod.)
- správa licencí
- správa účtů a rolí
- logy, události a monitoring (ESXi serverů a virtuálních strojů)
- plánované úlohy a mapy

vCenter Server podporuje práci se zásuvnými moduly (pluginy), které rozšiřují jeho schopnosti. Moduly mohou být také od výrobců třetích stran. Nasazení vCenter serveru je možné několika způsoby. Lze jej nainstalovat na jakýkoliv fyzický stroj, podporována je

[14] (VMware Inc., 2014B)
[15] (VMware Inc., 2014C)

instalace do virtuálního stroje a poslední způsob je použití předpřipravené instalace v podobě virtuální appliance. Pomocí vCenter serveru lze nasazovat již předkonfigurované virtuální stroje, tzv. virtuální appliance. Tímto způsobem je distribuována celá řada zejména jednoúčelových virtuálních strojů. Výhodou je rychlost jejich nasazení. Virtuálnímu stroji většinou stačí po jeho prvním spuštění nastavit konfiguraci sítě, hostname a lze jej začít plnohodnotně využívat.

K vCenter Serveru lze přistupovat rovněž několika způsoby. Tím starším je přístup pomocí aplikace nazvané vSphere Client, která je dostupná pouze na Windows. Dalším způsobem, do budoucna preferovaným, je přístup přes internetový prohlížeč. V prohlížeči je následně spuštěn VMware vSphere Web Client. Nutno podotknout, že administrátorům zvyklých na nástroj Windows vSphere Client dá trochu práci se v novém klientovi orientovat. Snaha společnosti VMware donutit administrátory k používání webového klienta je však poměrně veliká. Důkazem toho je postupné omezovaní funkcionalit staršího klienta a nepřidávání nových funkcionalit.

3.2.3 vCenter Operations Manager

Tento nástroj umožňuje pohled na virtuální infrastrukturu z hlediska využívání a vytížení jednotlivých zdrojů. Dokáže vyhodnotit a doporučit optimální nastavení virtuálního stroje z hlediska jeho umístění na konkrétním ESXi serveru, diskovém LUNu, vyhodnotit případné nedostatky v nastavení zdrojů (procesor, paměť) apod. Monitoruje stav a reportuje problémy s vytížením ESXi serverů, diskového prostoru apod. Nasazuje se jako virtuální appliance. Jeho cílem je poskytnout komplexní pohled na stav virtuální infrastruktury, podle kterého může administrátor provést optimalizaci[16].

3.2.4 Update Manager

Update Manager[17] slouží k instalaci záplat a nových verzí komponent. Jeho hlavní úkol je pravidelně stahovat aktualizace, které poté může administrátor aplikovat. Instaluje se jako samostatná komponenta zpravidla na vCenter Server, kam se po instalaci integruje a odkud se s ním pracuje.

[16] (VMware Inc., 2014D)
[17] (VMware Inc., 2014E)

3.2.5 vSphere Storage Appliance

vSphere Storage Appliance[18] je softwarové řešení sdíleného datového úložiště, které využívá interních disků ESXi serverů. Z těchto disků vytvoří úložiště, které je k dispozici všem ESXi serverům. Vývoj a prodej tohoto produktu byl ukončen k 1.4.2014. Nástupcem je produkt Virtual SAN.

3.2.6 vSphere Data Protection

Tento nástroj je určen k zálohování virtuálních strojů. Nasazuje se v podobě virtual appliance, konfigurovat lze pouze pomocí nástroje vSphere Web Client. Vytváří tzv. restore points, což jsou snapshoty virtuálních strojů ukládané na záložní server, či diskové pole. Existuje ve dvou verzích. V té základní jsou omezené možnosti nastavení jednotlivých záloh, časových oken apod. Advanced verze má více možnosti nastavení. Dále dokáže zálohovat jak virtualizované, tak nevirtualizované aplikační servery společnosti Microsoft (Exchange, SQL a SharePoint). K tomu využívá specializovaných agentů, kteří musí být nainstalovaní na zálohovaných systémech[19].

3.2.7 vCenter Converter Standalone Client

vCenter Converter Standalone Client[20] umožňuje převést fyzický počítač na virtuální. Podporované operační systémy jsou Windows a Linux. Na počítač, který požadujeme virtualizovat se nainstaluje agent, který zajistí přenos celého systému na ESXi server za běhu fyzického počítače. Podporována je odložená finalizace konverze, kdy je možné v první fázi přenést většinu počítače a dokončení odložit. To je velice výhodné v případech, kdy je potřeba zajistit co nejmenší prodlevu mezi přepnutím fyzického počítače na jeho virtuální klon. V době spuštění finální synchronizace již vSphere Convertor přenáší pouze rozdíly od poslední synchronizace a zpravidla dochází k odstavení fyzického počítače a zapnutí jeho klonu ve virtuálním prostředí. V jednu chvíli je možné provádět několik konverzí najednou.

[18] (VMware Inc., 2014F)
[19] (VMware Inc., 2014G)
[20] (VMware Inc., 2014H)

4 Praktická část

Praktická část této práce je realizována ve firmě První novinová společnost a.s., dále PNS. Hlavním předmětem činnosti PNS je distribuce tisku na prodejní místa po celé republice. Zajišťuje dodávky periodického i neperiodického tisku, elektronických médií a dalšího obdobného sortimentu od více než 480 vydavatelů. Tiskem zásobuje 17 000 prodejních míst. V září 2014 PNS spouští službu Baliczech. Jedná se o službu pro tuzemské e-shopy, která umožňuje vybraná místa (nejčastěji trafiky) po celé republice využít jako výdejní místa pro odběr zboží.

4.1 Analýza stávajícího firemního prostředí

PNS má hlavní distribuční a administrativní centrum v Praze Horních Počernicích, kde se nachází dvě oddělené serverovny propojené mezi sebou několika optickými propoji. V Praze je také část serverové infrastruktury umístěna v hostingovém centru GTS Nagano. S centrálou je hostingové centrum propojeno dvěma nezávislými síťovými propoji o rychlostech 480Mbps a 32Mbps. Dále má PNS dalších 7 poboček. Ty se nachází v Brně, Ostravě, Olomouci, Českých Budějovicích, Ústí nad Labem, Pardubicích a Plzni. Vzájemnou konektivitu zajišťují dvě oddělené WAN sítě, každá o rychlosti 4Mbps. Přehled a role serverů v celé sopečnosti jsou uvedeny v tabulce č 1.

Lokalita	Model serveru	Název	Operační systém	Využití	Virtualizovat
Praha DC	Dell PowerEdge 2950 2x 4Core CPU, 4GB RAM + diskové pole MD1000, 1,2TB	CEDC01	Windows 2003 R2 Server	doménový řadič, DNS, DHCP a souborový server	NE
Praha DC	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	CEDC02	Windows 2003 R2 Server	doménový řadič, DNS, docházkový a přístupový systém	NE
Praha DC	Dell PowerEdge 1950 1x 4Core CPU, 6GB RAM	CEALEA	Windows 2003 R2 Server 64bit	MIS SW (SQL)	ANO
Praha DC	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	CECLUSTER01	Windows 2003 R2 Server	poštovní server	ANO
Praha DC	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	CECLUSTER02	Windows 2003 R2 Server	poštovní server, tiskový server	ANO

Lokalita	Model serveru	Název	Operační systém	Využití	Virtualizovat
Praha DC	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	CEJ2B	Windows 2003 R2 Server	interface server do systému SAP - vlastní vývoj (SQL)	ANO
Praha DC	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	CEESO9M01	Windows 2000 Server	server se starým účetním systémem (archiv)	ANO
Praha DC	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	CEMNGNTF01	Windows 2003 R2 Server	aplikační server pro CMS Altiris a SEP	ANO
Praha DC	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	CEMNGSQL01	Windows 2003 R2 Server	databázový server pro CMS Altiris a SEP (SQL)	ANO
Praha DC	Dell PowerEdge 1950 1x 4Core CPU, 8GB RAM	CEPLANTOUR	Windows 2003 R2 Server	aplikační server pro výpočet silničních tras + SQL	ANO
Praha DC	Dell PowerEdge 1950 1x 4Core CPU, 24GB RAM	CEBACKUP	Windows 2003 R2 Server	server pro zálohování - Symantec Backup Exec	NE
Praha DC	Dell PowerEdge R410 1x 4Core CPU, 4GB RAM + diskové pole MD1000, 13TB	CECAM	Windows 2003 R2 Server	server pro záznam z kamerového systému	NE
Praha DC	Dell PowerEdge SC440 1x CPU, 2GB RAM	PRPRES	Windows XP	stanice pro generování a tisk dodacích a remitendních listů a generování PDF verze	ANO
Praha DC	Dell PowerEdge SC440 1x CPU, 2GB RAM	PRPDF	Windows XP	záložní stanice pro systém PRES + PDF archiv výstupu ze stanice PRPRES	ANO
Praha DC	Dell PowerEdge 2950 2x 4Core CPU, 64GB RAM	-	-	server vyčleněný pro virtualizaci hostingového centra Nagano	-
Praha DC	Dell PowerEdge 2950 2x 4Core CPU, 64GB RAM	-	-	server vyčleněný pro virtualizaci hostingového centra Nagano	-
Praha Nagano	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	ALDC01	Windows 2003 R2 Server EE	doménový řadič, DNS, DHCP, IAS, CA, PRTG monitoring	NE
Praha Nagano	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	ALWEB01	Windows 2003 R2 Server	webový server	ANO

Lokalita	Model serveru	Název	Operační systém	Využití	Virtualizovat
Praha Nagano	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	ALSMS01	Linux RedHat	antispam server (appliance)	ANO
Praha Nagano	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	ALSMS02	Linux RedHat	antispam server (appliance)	ANO
Praha Nagano	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	ALPROXY	Windows 2003 R2 Server	proxy server pro přístup k internetu	NE
Praha Nagano	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	ALCLUSTER01	Windows 2003 R2 Server	poštovní server	ANO
Praha Nagano	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	ALCLUSTER02	Windows 2003 R2 Server	poštovní server, sametime	ANO
Praha Nagano	Dell PowerEdge R200 1x 1Core CPU, 1GB RAM	ALBACKUP	Linux CentOS 5.9	server pro zálohování	NE
Praha Nagano	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	ALWC01	Symantec (Linux)	monitorovací a řídící server přístupu k internetu (appliance)	NE
Praha Nagano	HP ProLiant	PRCUCM	Cisco (Linux)	řídící server IP telefonie (appliance)	NE
Ústí nad Labem	Dell PowerEdge 2950 1x 4Core CPU, 4GB RAM + 1TB interní diskové pole	ULDC	Windows 2003 R2 Server	doménový řadič, DNS, DHCP a souborový server PDF archiv výstupu ze stanice PRPRES	NE
Ústí nad Labem	Dell PowerEdge SC440 1x CPU, 2GB RAM	ULPRES	Windows XP	stanice pro generování a tisk dodacích a remitendních listů a generování PDF verze	ANO
Ústí nad Labem	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	ULCISCONN	Windows 2003 R2 Server	interface server KC - SAP	ANO
Ústí nad Labem	Dell PowerEdge 2950 2x 4Core CPU, 4GB RAM	ULCALLREC	Linux	server pro záznam nahrávek KC	NE
Ústí nad Labem	Dell PowerEdge 1950 1x 4Core CPU, 4GB RAM	ULTAS	Windows 2003 R2 Server	tarifikační server IP telefonie	ANO
Ústí nad Labem	HP ProLiant	ULCUCM	Cisco (Linux)	řídící server IP telefonie (appliance)	NE

Lokalita	Model serveru	Název	Operační systém	Využití	Virtualizovat
Brno	Dell PowerEdge 2950 2x 4Core CPU, 4GB RAM	BRDC	Windows 2003 R2 Server	DNS, DHCP, souborový server	ANO
Brno	Dell PowerEdge SC440 1x CPU, 2GB RAM	BRPRES	Windows XP	stanice pro generování a tisk dodacích a remitendních listů a generování PDF verze	ANO
Brno	Dell PowerEdge SC440 1x CPU, 2GB RAM	BRPDF	Windows XP	záložní stanice pro systém PRES + PDF archiv výstupu ze stanice PRPRES	ANO
Brno	Dell PowerEdge R410 1x 4Core CPU, 4GB RAM + diskové pole MD1000, 13TB	BRCAM	Windows 2003 R2 Server	server pro záznam z kamerového systému	NE
Ostrava	Dell PowerEdge 2950 2x 4Core CPU, 4GB RAM	OSDC	Windows 2003 R2 Server	DNS, DHCP, souborový server	ANO
Ostrava	Dell PowerEdge SC440 1x CPU, 2GB RAM	OSPRES	Windows XP	stanice pro generování a tisk dodacích a remitendních listů a generování PDF verze	ANO
Ostrava	Dell PowerEdge SC440 1x CPU, 2GB RAM	OSPDF	Windows XP	záložní stanice pro systém PRES + PDF archiv výstupu ze stanice PRPRES	ANO
Ostrava	Dell PowerEdge R410 1x 4Core CPU, 4GB RAM + diskové pole MD1000, 13TB	OSCAM	Windows 2003 R2 Server	server pro záznam z kamerového systému	NE
Olomouc	Dell PowerEdge 2950 2x 4Core CPU, 4GB RAM	OLDC	Windows 2003 R2 Server	DNS, DHCP, souborový server	ANO
Olomouc	Dell PowerEdge SC440 1x CPU, 2GB RAM	OLPRES	Windows XP	stanice pro generování a tisk dodacích a remitendních listů a generování PDF verze	ANO
Olomouc	Dell PowerEdge SC440 1x CPU, 2GB RAM	OLPDF	Windows XP	záložní stanice pro systém PRES + PDF archiv výstupu ze stanice PRPRES	ANO

Lokalita	Model serveru	Název	Operační systém	Využití	Virtualizovat
Plzeň	Dell PowerEdge 2950 2x 4Core CPU, 4GB RAM	PLDC	Windows 2003 R2 Server	DNS, DHCP, souborový server	ANO
Plzeň	Dell PowerEdge SC440 1x CPU, 2GB RAM	PLPRES	Windows XP	stanice pro generování a tisk dodacích a remitendních listů a generování PDF verze	ANO
Plzeň	Dell PowerEdge SC440 1x CPU, 2GB RAM	PLPDF	Windows XP	záložní stanice pro systém PRES + PDF archiv výstupu ze stanice PRPRES	ANO
Pardubice	Dell PowerEdge 2950 2x 4Core CPU, 4GB RAM	PADC	Windows 2003 R2 Server	DNS, DHCP, souborový server	ANO
Pardubice	Dell PowerEdge SC440 1x CPU, 2GB RAM	PAPRES	Windows XP	stanice pro generování a tisk dodacích a remitendních listů a generování PDF verze	ANO
Pardubice	Dell PowerEdge SC440 1x CPU, 2GB RAM	PAPDF	Windows XP	záložní stanice pro systém PRES + PDF archiv výstupu ze stanice PRPRES	ANO
České Budějovice	Dell PowerEdge 2950 2x 4Core CPU, 4GB RAM	CBDC	Windows 2003 R2 Server	DNS, DHCP, souborový server	ANO
České Budějovice	Dell PowerEdge SC440 1x CPU, 2GB RAM	CBPRES	Windows XP	stanice pro generování a tisk dodacích a remitendních listů a generování PDF verze	ANO
České Budějovice	Dell PowerEdge SC440 1x CPU, 2GB RAM	CBPDF	Windows XP	záložní stanice pro systém PRES + PDF archiv výstupu ze stanice PRPRES	ANO

Tabulka 1 – přehled a role serverů

4.2 Posouzení vhodnosti virtualizace jednotlivých serverů

Většina serverů byla posouzena jako vhodná pro virtualizaci. U některých však bylo rozhodnuto, že v první fázi virtualizovány nebudou. Tyto servery se dají rozdělit do několika skupin.

- servery kamerového systému, které kladou velké požadavky na diskové úložiště (rychlost zápisu a kapacita).

- řadiče domény, jejichž virtualizace (proces P2V) není doporučena s ohledem na problémy, které přináší. Jedná se zejména o problémy replikací Active Directory databáze.
- servery určené pro zálohování nebudou virtualizovány z hlediska ochrany zálohovaných dat, která budou udržována na odděleném hardware.
- jednoúčelové servery (appliance) nebudou v první fázi virtualizovány. Jejich virtualizace je zvažována jako součást upgradu v budoucnu. V některých případech budou nové verze produktů poskytovány pouze jako virtuální stroje, např. Cisco Unified Communication Manager.

4.3 Výběr a zapojení serverů a diskových polí

Tato kapitola je věnována výběru, fyzické instalaci a zapojení serverů, diskových polí a síťových prvků. Rozdělena je do tří částí, které pokrývají centrálu PNS, hostingové centrum GTS Nagano a pobočky.

4.3.1 Centrála PNS

Na základě analýzy potřebných prostředků (výpočetní výkon, operační paměť, IOPS) bylo rozhodnuto o pořízení celkem tří serverů a dvou diskových polí. Dva servery a jedno diskové pole jsou umístěny v hlavní serverovně (DR1). Oba tyto servery mají připojeno diskové pole jako shared storage. Na těchto serverech budou provozovány pro chod společnosti kritické virtuální stroje. Třetí server s diskovým polem je umístěn ve druhé serverovně (DR2). Na tomto serveru budou umístěny méně důležité virtuální stroje.

Při návrhu řešení byla zohledněna celá řada kritérií. V první řadě byl kladen důraz na vytvoření prostředí s co největší odolností proti výpadku (hardware) a prostředí, které bude výkonnostně i kapacitně dostačovat po dobu minimálně pěti let. Každý server i diskové pole má dva nezávislé zdroje napájení připojené do různých UPS. Připojení serverů k diskovým polím je realizováno několika cestami. Servery jsou připojeny do LAN sítě několika síťovými kartami. Každý server je připojen ke dvěma switchům. Servery jsou vybaveny DRAC kontrolérem, který umožňuje vzdálenou správu serveru (zapnutí/restart/vypnutí serveru, vzdálenou konzoli, připojení ISO souboru s instalačními soubory operačního systému, pokročilé nastavení hardware, podpora protokolu IPMI apod.). Na všechny servery a disková pole je zakoupen support na 5 let s garancí vyřešení

závady během druhého pracovního dne. Na diskové pole Dell PowerVault MD3220 je zakoupen support s garancí doby vyřešení problému do 4 hodin od nahlášení závady.

Neméně důležitou roli hrály pořizovací náklady. Bylo zvažováno několik variant zejména při výběru diskových polí. Zde se nabízely dvě hlavní řešení. První předpokládalo vybudování separátní SAN sítě pro připojení diskových polí. Vzhledem k tomu, že by bylo potřeba vybudovat celou infrastrukturu od základu (SAN switche, kabeláž apod.), což by celé prostředí značně prodražilo, bylo zvoleno řešení, kde jsou disková pole přímo připojena k serverům. Náklady rovněž ovlivnilo pořízení licencí na jednotlivé produkty VMware, kterými se budu zabývat v dalších kapitolách.

Parametry nových serverů jsou uvedeny v tabulce č. 2. Parametry diskového pole umístěného v serverovně DR1 jsou uvedeny v tabulce č.3 a parametry diskového pole umístěného v serverovně DR2 jsou uvedeny v tabulce č. 4. Umístění jednotlivých serverů a diskových polí v rámci centrály PNS je uvedeno v tabulce č. 5.

Parametry nových serverů	
Model	Dell PowerEdge R720, 2U
CPU	2x Intel Xeon E5-2650 2.00Ghz, 8Core, 20M Cache
RAM	128GB (8x16GB) RDIMM 1600Mhz
Konektivita	Broadcom 5720 QP 1Gbps 4port Broadcom 5719 QP 1Gbps 4port
Úložiště	2GB SD CARD
Adaptér (HBA)	SAS 6Gbps HBA External Controller
Zdroj	Dual, Hot-Plug, Redundant Power Supply 750W
Management	IDRAC 7 (Integrated Dell Remote Access Controller) Enterprise
Support	5 Year ProSupport, Next Business Day

Tabulka 2 - parametry serverů

Parametry diskového pole v DR1	
Model	Dell PowerVault MD3220
Rozhraní	Serial Atached SCSI (SAS) 6Gbps
Počet a typ disků	24 x 900GB SAS 6Gbps 10K 2,5” HD Hot Plug (z toho 1 disk Hot Spare)
Virtuální disky	LUN0 RAID10 (12 disků), kapacita ~ 5TB LUN1 RAID5 (11 disků), kapacita ~ 8,3TB
Konektivita	2x 100Mbps Ethernet Card
Zdroj	Redundant Power Supply (2 PSU) 600W
Management	PowerVault Modular Disk Storage Manager (Windows aplikace)
Support	5 Year ProSupport, 4Hr Mission Critical

Tabulka 3 - parametry diskového pole v DR1

Parametry diskového pole v DR2	
Model	Dell PowerVault MD1220
Rozhraní	Serial Atached SCSI (SAS) 6Gbps
Počet a typ disků	24 x 900GB SAS 6Gbps 10K 2,5” HD Hot Plug (z toho 1 disk Hot Spare)
Virtuální disky	LUN0 RAID10 (12 disků), kapacita ~ 5TB LUN1 RAID5 (11 disků), kapacita ~ 8,3TB
Zdroj	Redundant Power Supply (2 PSU) 600W
Management	Pomocí management rozhraní serveru
Support	5 Year ProSupport, Next Business Day

Tabulka 4 - parametry diskového pole v DR2

Model	Název	Umístění
R720	CEVMW01	DR1
R720	CEVMW02	DR1
MD3220	CEMD3220	DR1
R720	CEVMW03	DR2
MD1220	CEMD1220	DR2

Tabulka 5 - umístění serverů a diskových polí

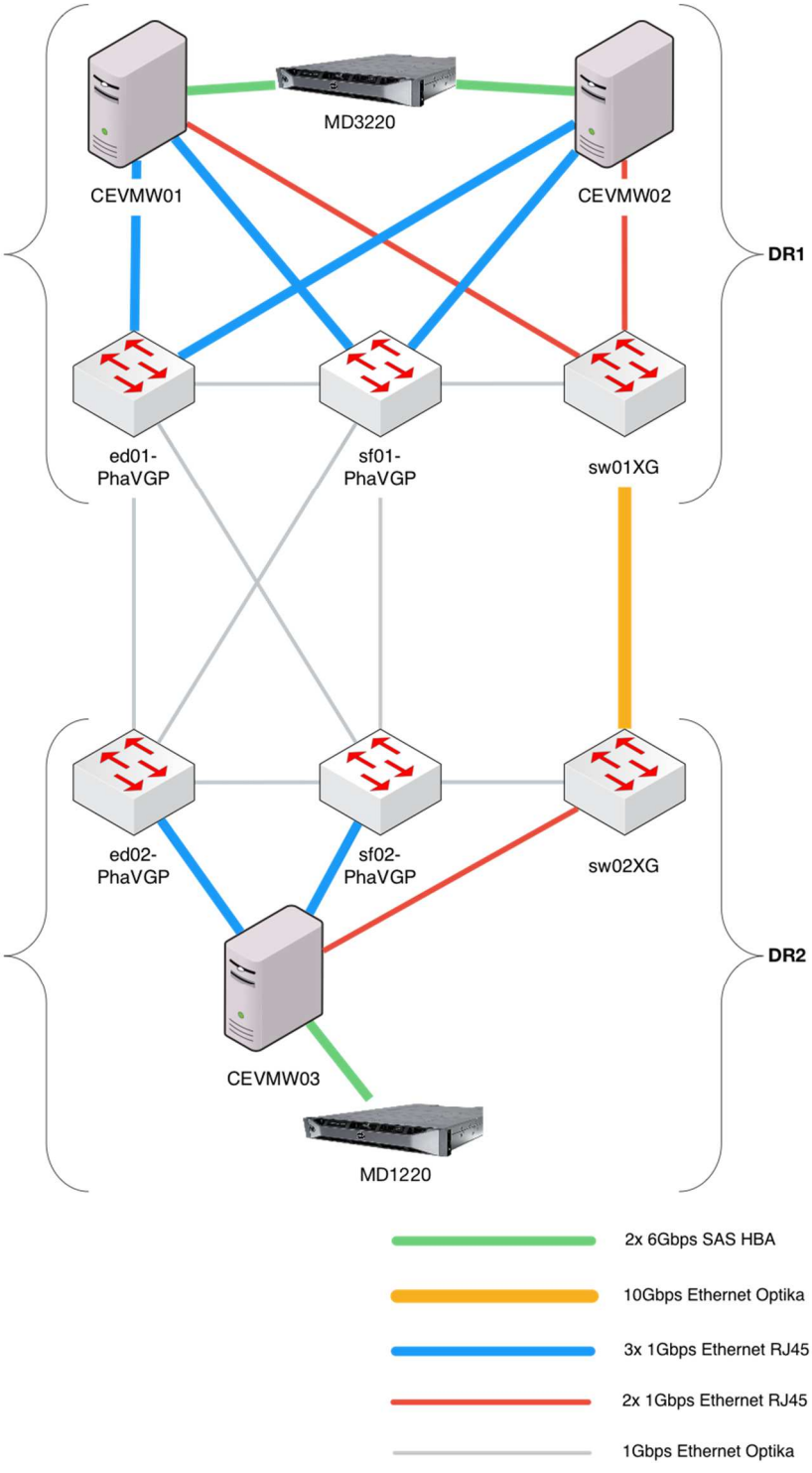
Před připojením serverů do LAN sítě musí být správně nakonfigurovány porty switchů. Vzhledem k tomu, že se na centrále PNS používá několik různých sítí realizovaných pomocí VLAN, je potřeba tyto sítě zpřístupnit také pro VMware prostředí. Konfigurace jednoho portu Cisco switche vypadá takto.

```
interface GigabitEthernet0/25
 description CEVMW01 vmnic4
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 80, 82-84, 87, 90
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 auto qos voip trust
 macro description cisco-switch
 spanning-tree link-type point-to-point
end
```

Port je nastaven do módu trunk. To znamená, že skrze něj může procházet komunikace z více než jedné sítě (VLAN). Pokud paket není správně tagován, je přiřazen do native VLAN. Doporučení je na trunk portu povolit pouze takové VLANy, které jsou na serveru používané. V našem případě povolujeme VLAN 80, 82-84, 87, 90. Pro lepší a rychlejší orientaci je dobré u každého portu napsat do poznámky (description) název, či

jinou identifikaci zařízení, které je do portu připojeno. Konfigurace síťového prostředí na straně serverů bude vysvětlena v dalších kapitolách.

Celkové schéma fyzického zapojení jednotlivých komponent na centrále PNS ukazuje obrázek č. 16.



Obrázek 16 - schéma zapojení Centrála PNS

4.3.2 Hostingové centrum GTS Nagano

Servery použité pro virtualizaci v hostingovém centru jsou modely dosud využívané na centrále PNS. Jedná se o dva modely Dell PowerEdge 2950 III, které jsou hardwarově posíleny tak, aby výkonnostně odpovídaly požadavkům na virtualizaci v hostingovém centru. Hlavní rozdíl oproti řešení na centrále PNS spočívá v tom, že jako úložiště je použito interní diskové pole na každém serveru. Výsledné řešení je s ohledem na dostupné možnosti navrženo tak, že co nejvíce komponent je redundantních, což minimalizuje riziko SPOF – nicméně ne vše. Vzhledem k počtu dostupných síťových adaptérů, resp. jednotlivých portů a skutečnosti, že v hostingovém centru je potřeba konektivita k několika odděleným switchům, resp. odděleným VLAN, není připojení redundantní. Problém je částečně řešen tak, že jsou severy připojeny k různým switchům. Celkový počet virtuálních strojů je rozdělen mezi oba servery. V případě výpadku jednoho serveru je možné virtuální stroje z nedostupného serveru zapnout na druhém funkčním serveru. To je možné díky nastavení replikací virtuálních strojů mezi oběma servery, které probíhají v určitých intervalech. Podrobněji se této problematice budu věnovat v dalších kapitolách. Parametry obou serverů jsou uvedeny v tabulce č. 6.

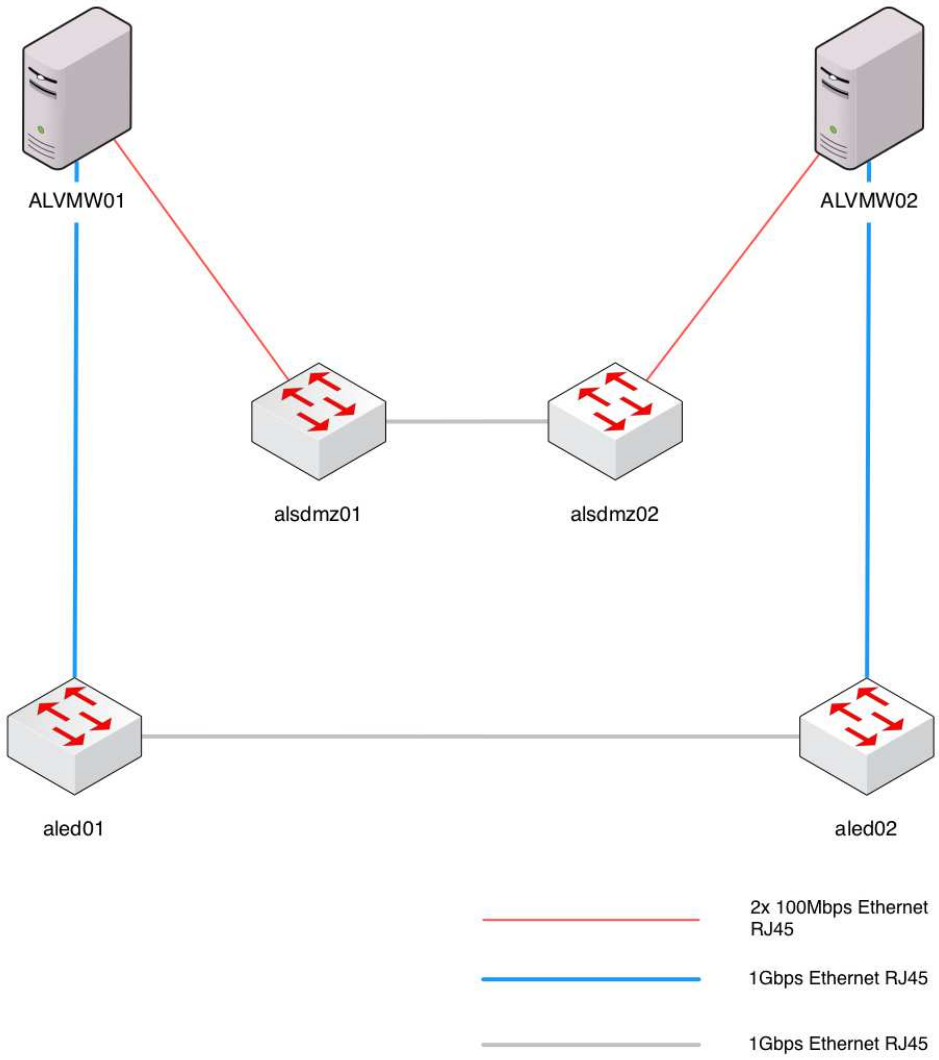
Parametry serverů v hostingovém centru GTS Nagano	
Model	Dell PowerEdge 2950 III, 2U
CPU	2x Intel Xeon E5450 3.00Ghz, 4Core
RAM	64GB (8x8GB) RDIMM 667Mhz
Konektivita	Broadcom NetXtreme II BCM5708 1Gbps 2port Intel 82571EB 1Gbps 2 port
Úložiště	6x SAS 400GB
RAID adaptér	PERC 6/I, Integrated Controller
Virtuální disky	LUN0 RAID1 (2 disky), kapacita ~ 400GB LUN1 RAID5 (4 disky), kapacita ~ 1,1TB
Zdroj	Dual, Hot-Plug, Redundant Power Supply 750W
Management	IDRAC 5 (Integrated Dell Remote Access Controller) Enterprise
Support	5 Year ProSupport, Next Business Day (zbývá 1 rok)

Tabulka 6 - parametry serverů v hostingovém centru

Konfigurace portů na straně switchů aled01 a aled02 je obdobná jako na centrále PNS. V případě switchů a alsdmz01 a alsdmz02 je na každém portu nastavena jedna konkrétní VLAN. Port proto nemusí být v režimu trunk, ale je nastaven jako access. Konfigurace portu vypadá takto.

```
interface FastEthernet0/14
 description ALVMW01-vmnic1
 switchport access vlan 502
 switchport mode access
 switchport nonegotiate
end
```

Schéma fyzického zapojení serverů v hostingovém centru je vidět na obrázku č. 17.



Obrázek 17 - schéma zapojení v hostingovém centru

4.3.3 Pobočky

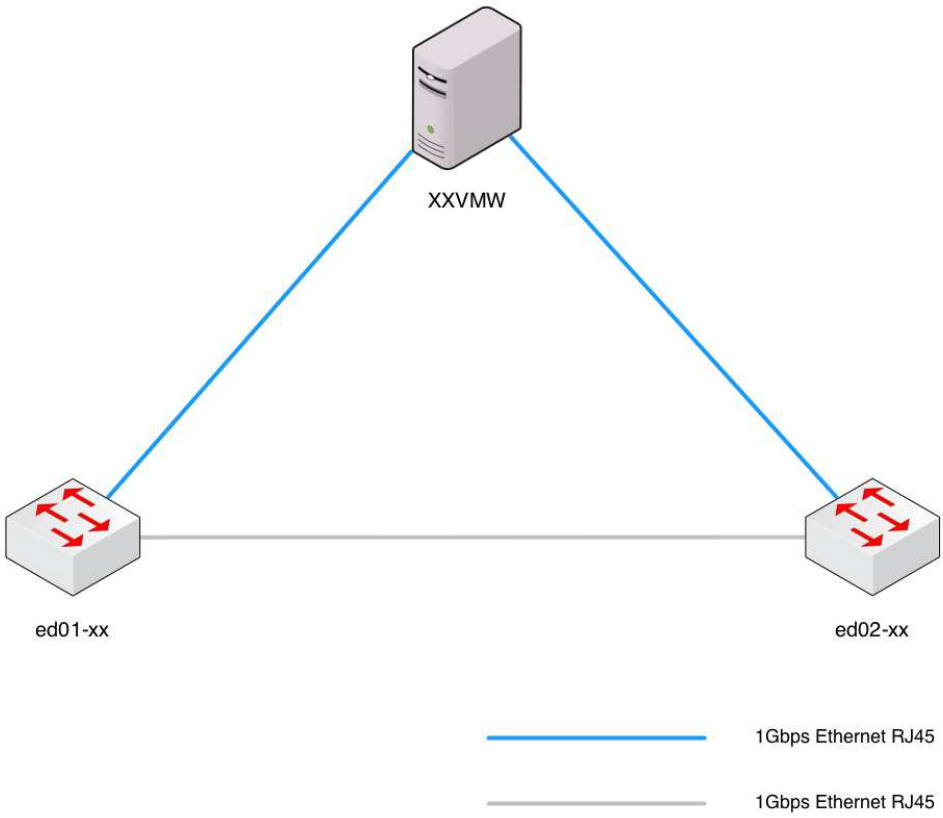
Server použitý na každé pobočce je rovněž Dell PowerEdge 2950 III posílený tak, aby výkonnostně odpovídal požadavkům na virtualizaci poboček. Redundance je zde řešena pouze částečně (připojení do různých switchů, dva zdroje napájení apod.). V případě fatální havárie serveru jsou pobočky po nezbytně nutnou dobu schopny fungovat bez funkčního serveru. Parametry pobočkového serveru jsou uvedeny v tabulce č. 7. Výjimkou je server v Ústí nad Labem, který má 16GB RAM, protože jsou na něm provozovány virtuální stroje kontaktního centra a IP telefonie.

Parametry serveru na pobočkách	
Model	Dell PowerEdge 2950 III, 2U
CPU	Intel Xeon E5450 3.00Ghz, 4Core
RAM	12GB RDIMM 667Mhz
Konektivita	Broadcom NetXtreme II BCM5708 1Gbps 2port
Úložiště	6x SAS 400GB
RAID adaptér	PERC 6/I, Integrated Controller
Virtuální disky	LUN0 RAID1 (2 disky), kapacita ~ 400GB LUN1 RAID5 (4 disky), kapacita ~ 1,1TB
Zdroj	Dual, Hot-Plug, Redundant Power Supply 750W
Management	IDRAC 5 (Integrated Dell Remote Access Controller) Enterprise
Support	5 Year ProSupport, Next Business Day (zbývá 1 rok)

Tabulka 7 - parametry serverů na pobočkách

Porty na switchích jsou nakonfigurovány v režimu access, stejně jako porty switchů alsdmz01 a alsdmz02 v hostingovém centru. Výjimku opět tvoří server v Ústí nad Labem, kde jsou porty nastaveny v módu trunk.

Schéma fyzického zapojení serverů v na pobočkách je vidět na obrázku č. 18. XX a xx ve skutečnosti odpovídá označení jednotlivých poboček, např. UL, BR apod.



Obrázek 18 - schéma zapojení na pobočkách

4.4 Příprava serverů

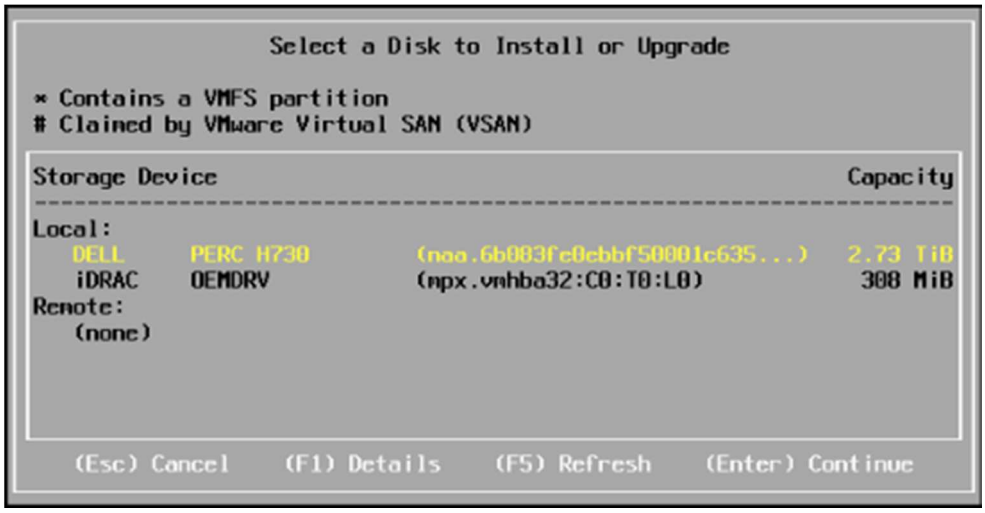
Tato kapitola je rozdělena do dvou částí. První část se zabývá instalací produktu VMware ESXi na fyzické servery. Druhá kapitola je zaměřena na konfiguraci a další potřebné kroky pro správné fungování serveru.

4.4.1 Instalace VMware ESXi 5.5

Instalace na všechny servery probíhá stejným způsobem, proto je proces instalace demonstrován na jednom konkrétním serveru. Obecně existuje několik způsobů, jak instalaci provést. U všech je potřeba z webových stránek VMware stáhnout instalační ISO soubor. Tento ISO soubor lze následně buď vypálit na CD, vytvořit spouštěcí USB flash disk, nebo jako v našem případě zpřístupnit na síti a pomocí DRAC kontroléru připojit k serveru. Podmínkou je tedy připojený a nakonfigurovaný DRAC kontrolér do sítě a dostupná sdílená složka s nahraným ISO souborem. Na obrázku č. 19 je vidět připojený instalační soubor.

Obrázek 19 - připojení instalačního ISO souboru pomocí DRAC kontroléru

Samotná instalace se skládá z několika kroků. V prvním kroku vybíráme úložiště, na které bude instalace provedena. V našem případě to bude interní SD karta u serverů Dell PowerEdge R720 a LUN0_RAID1 u serverů Dell PowerEdge 2950 (obrázek č. 20). Po výběru úložiště následuje nastavení hesla uživatele root (obrázek č. 21).

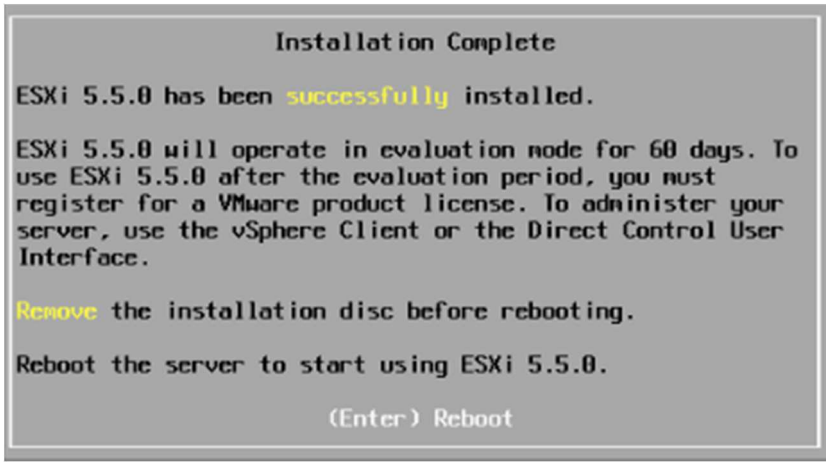


Obrázek 20 - výběr úložiště pro instalaci

Obrázek 21 - nastavení hesla uživatele root

Po nastavení hesla již probíhá samotná instalace (obrázek č. 22). Její závěr vidíme na obrázku č. 23.

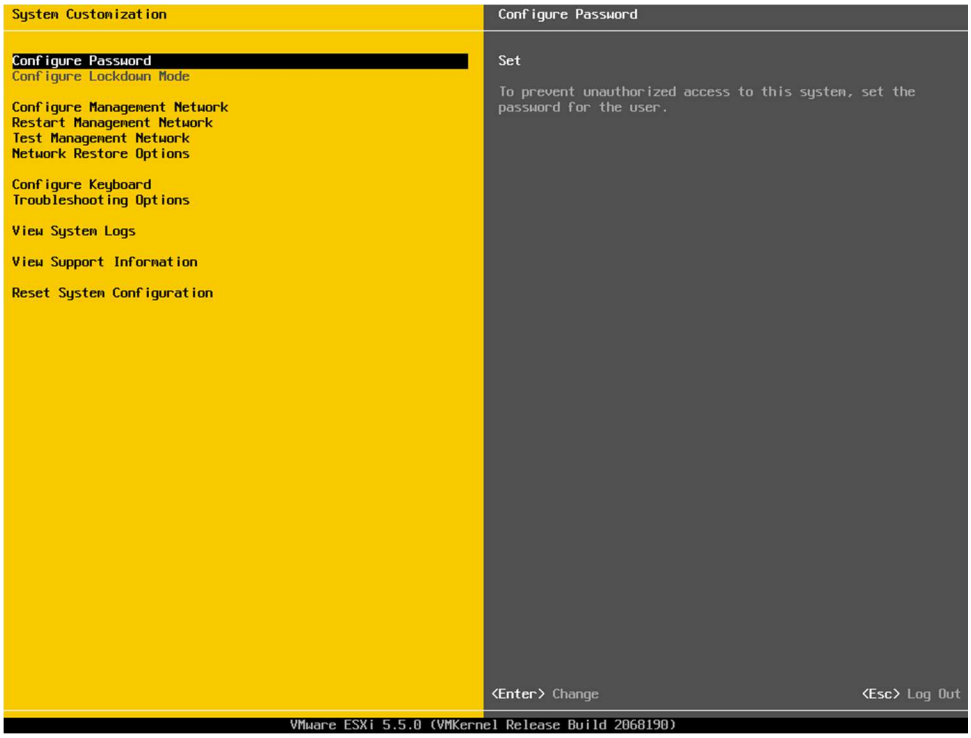
Obrázek 22 - průběh instalačního procesu



Obrázek 23 - závěr instalace

4.4.2 Základní konfigurace

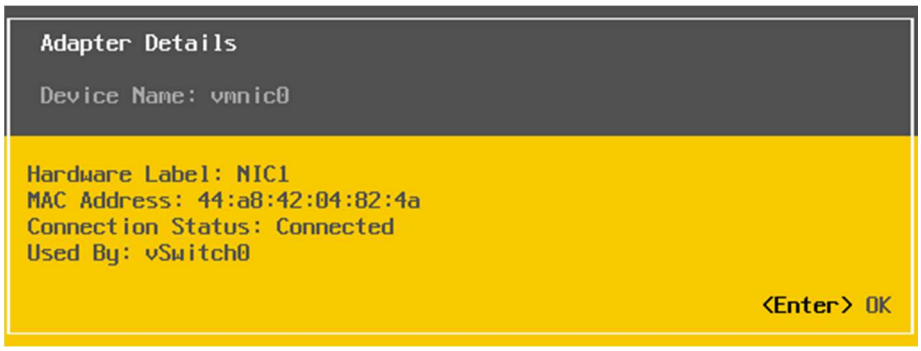
Po dokončení instalačního procesu je nezbytné nastavit několik parametrů. K tomu slouží obrazovka na obrázku č. 24.



Obrázek 24 - obrazovka nastavení základních parametrů

Nejdůležitější parametry se nachází v sekci Management Network.

- Síťové adaptéry, které budou použity pro správu. V základním nastavení stačí zvolit pouze jeden adaptér. V pozdější konfiguraci budou adaptéry přidány, resp. bude záležet na tom, kolik fyzických adaptérů má přiřazen virtuální switch, který obsahuje Management Network port. Doporučené je použít několik adaptérů, které od sebe budou co nejvíce fyzicky odděleny (různé fyzické porty připojené do různých switchů apod.). Podrobné informace o adaptéru zvoleného pro Management Network vidíme na obrázku č. 25.



Obrázek 25 - podrobné informace o adaptéru pro Management Network

- VLAN, ve které se nachází použité adaptéry. Tento parametr je potřeba nastavit v případě, že používáme adaptéry v režimu trunk. Toto je náš případ, proto bude hodnota VLAN vyplněna. Pokud by číslo VLAN nebylo nastaveno, připojení k serveru by nebylo funkční.
- Konfigurace IP protokolu obsahuje IP adresu, masku sítě a výchozí bránu. Můžeme zvolit automatickou konfiguraci pomocí DHCP protokolu nebo zadat statickou IP adresu. V našem případě použijeme statickou IP adresu.
- IPv6 zapíná podporu tohoto protokolu. V síti PNS není IPv6 nasazen, proto tuto volbu vypínáme.
- Konfigurace DNS dovoluje nastavit dva servery pro překlad IP adres na jména a opačně. Dále se v této sekci nastavuje název (hostname) našeho serveru.
- Volitelný DNS suffix je v tomto případě chápán jako doména. V prostředí PNS jej nastavujeme na hodnotu pns.cz.

Za zmínku dále stojí sekce Troubleshooting Options, ve které povolíme přístup k ESXi serveru pomocí protokolu SSH. Ostatní volby z obrázku č. 24 slouží pro řešení problémů či diagnostiku.

4.4.3 Pokročilá konfigurace

Jakmile je provedena základní konfigurace a server je dostupný na síti, můžeme se k němu připojit nástrojem vSphere Client, který slouží pro konfiguraci pokročilých funkcí. Dříve, než přistoupíme ke konfiguraci serveru pomocí vSphere klienta, je potřeba na server nainstalovat podporu pro správu serveru dodanou výrobcem serveru, tedy společností Dell. Software, který budeme instalovat se jmenuje Dell OpenManage Server Administrator vSphere Installation Bundle. Jedná se o soubor typu VIB (vSphere Installation Bundle)[21]. Pro instalaci použijeme nástroj VMware vSphere CLI.

VMware vSphere CLI je sada příkazů, které lze spouštět z operačního systému Windows nebo Linux a cílit je buď na konkrétní ESXi server, nebo na vCenter Server. Tímto nástrojem provedeme také konfiguraci protokolu SNMP.

Instalace VIB souboru:

```
esxcli --server=192.168.82.14 --username=root software vib install –d
/vmfs/volumes/alvmw01_lun0_raid5/OM-SrvAdmin-Dell-Web-8.0.2-1331.VIB-
ESX55i_A00.zip
Enter password:
Installation Result
Message: The update completed successfully, but the system needs to be rebooted
for the changes to be effective.
Reboot Required: true
VIBs Installed: Dell_bootbank_OpenManage_8.0.2-0000
VIBs Removed:
VIBs Skipped:
```

Konfigurace SNMP protokolu[22]:

```
vicfg-snmp.pl --server 192.168.82.14 --username root -c public –t
192.168.82.76@162/public
Enter password:
Changing community list to: public...
Complete.
Changing notification(trap) targets list to: 192.168.82.76@162/public...
Complete.
vicfg-snmp.pl --server 192.168.82.14 --username root –E
Enter password:
Enabling agent...
Complete.

vicfg-snmp.pl --server 192.168.82.14 –username root -s
Enter password:
```

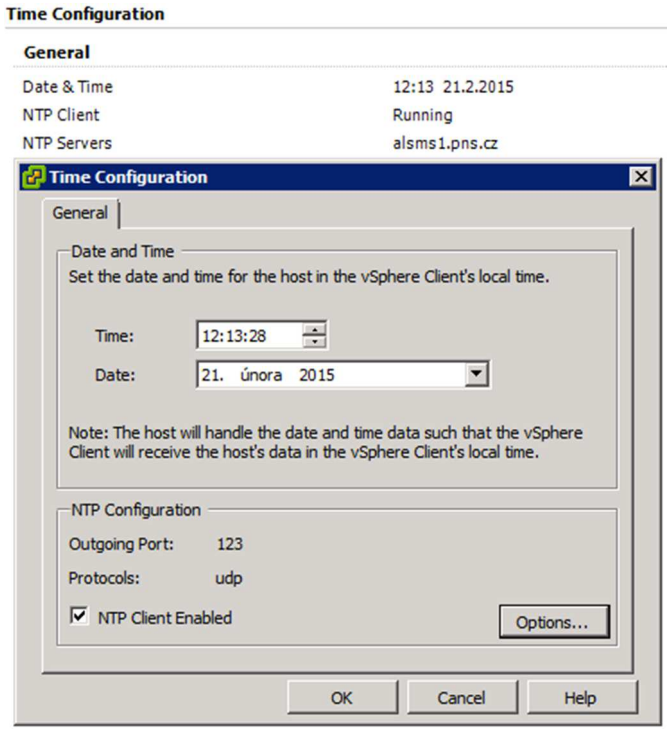
[21] (Gleed, 2011)
[22] (VMware Inc., 2014I)

```
Current SNMP agent settings:
Enabled: 1
UDP port: 161
Communities: public
Notification targets: 192.168.82.76@162/public
Options:
EnvEventSource=indications
engineid=00000063000000a100000000
loglevel=info
```

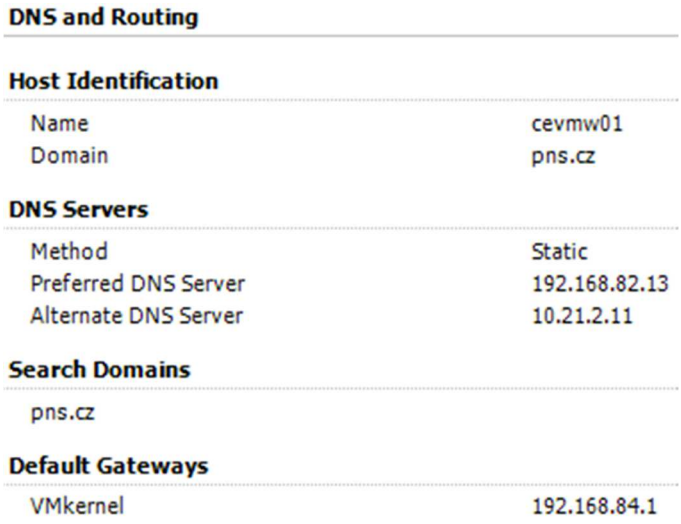
Prvním příkazem nastavujeme SNMP komunitu na hodnotu `public`. Dále zadáváme IP adresu, port a komunitu serveru, na který budou odesílány SNMP zprávy (trapy). Komunita určuje skupinu zařízení, která mezi sebou mohou komunikovat v rámci SNMP protokolu.

Druhým příkazem aktivujeme SNMP agenta a třetím příkazem ověřujeme správnost uloženého nastavení.

Nyní přistoupíme k nástroji vSphere Client, který lze instalovat na libovolný počítač či server s operačním systémem Windows. Odkaz na stažení je dostupný na adrese našeho serveru. Po spuštění vSphere klienta dokončíme nezbytné konfigurační kroky serveru, kterými jsou nastavení synchronizace času s NTP serverem, konfigurace DNS a směrování. Udržovat aktuální správný čas na všech ESXi serverech je nutné zejména z hlediska logování, iSCSI autentifikace, zabezpečení apod. Na ESXi je synchronizace času řešena pomocí NTP služby, jejíž konfiguraci znázorňuje obrázek č. 26. Služba má nastaven automatický start s ESXi serverem. Parametry DNS vidíme na obrázku č. 27. Kromě názvu serveru (hostname) nastavujeme také doménu pns.cz. Výchozí bránu a DNS servery již máme přednastaveny, použity jsou hodnoty zadané během konfigurace Management Network.



Obrázek 26 - konfigurace času – NTP



Obrázek 27 - konfigurace DNS a výchozí brána

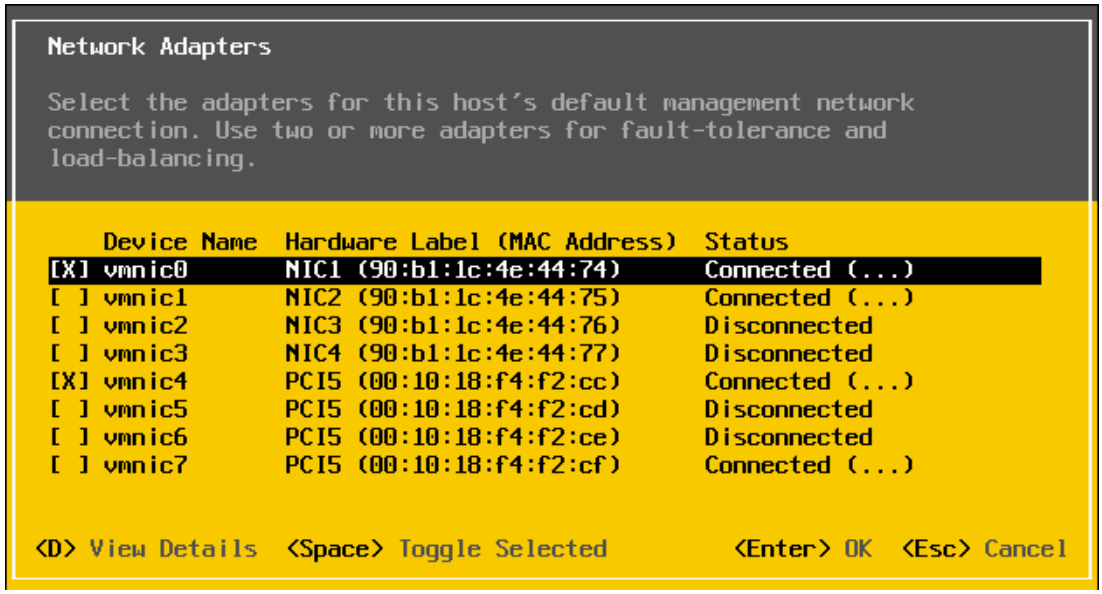
4.4.4 Konfigurace sítě

Správná síťová konfigurace je zásadní pro nasazení celého řešení virtualizace. Na úvod je potřeba definovat základní pojmy, se kterými bude dále pracováno.

4.4.4.1 vmnic

Vmnic je označení síťových adaptérů. Každý adaptér je jeden fyzický port (např. RJ45, SFP apod.), který má server k dispozici. První adaptér má označení vmnic0. Na

obrázku č. 28. je vidět, že server má celkem osm síťových adaptérů. Vmnic0 – vmnic3 je jedna síťová karta (označení HW je NIC1-NIC4). Vmnic4 – vmnic7 je druhá síťová karta (označení HW je PCI5). Vmnic adaptéry lze rozdělovat a sdružovat pomocí tzv. virtuálních switchů – vSwitch.

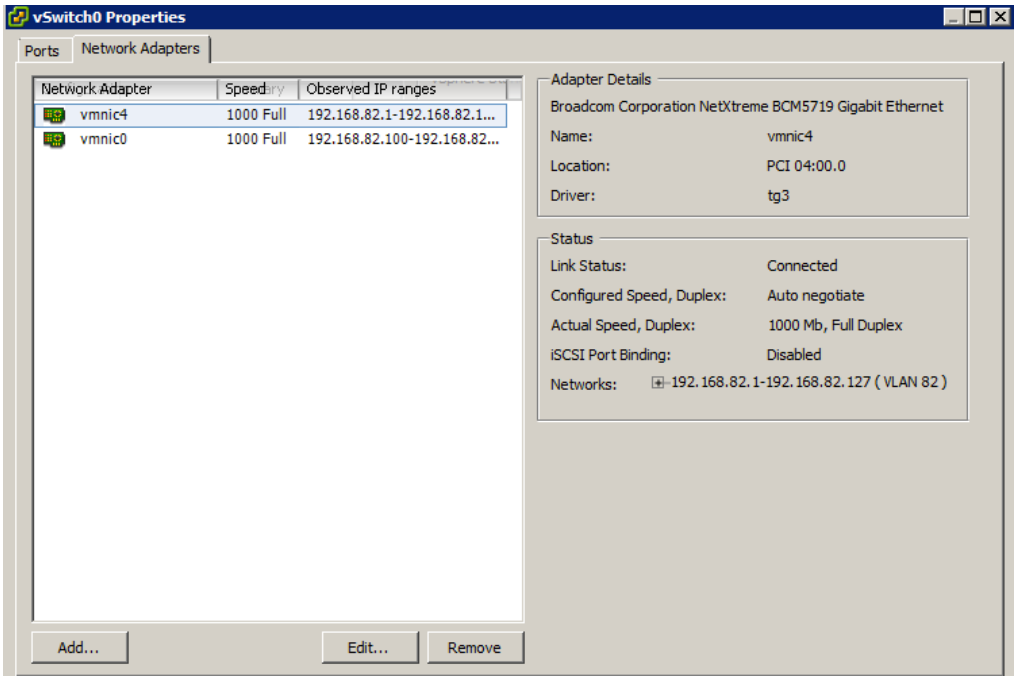


Obrázek 28 - vmnic adaptéry

4.4.4.2 vSwitch

vSwitch tedy sdružuje vmnic adaptéry a jeho hlavní funkcí je, že umožňuje připojení virtuálních strojů do sítě na základě určitých pravidel. V podstatě zajišťuje L2 konektivitu. K tomu, aby vše fungovalo je potřeba vSwitch správně nakonfigurovat. Nastavení, která můžeme nad virtuálním switchem provádět se dají rozdělit do dvou částí.

V první řadě je potřeba vSwitchi přiřadit jeden nebo více vmnic adaptérů. Doporučení je použít minimálně dva vmnic adaptéry na jeden vSwitch . Je to zejména z důvodu zajištění odolnosti vůči výpadku, či rozložení síťového provozu mezi více adaptérů, resp. fyzických switchů. V prostředí PNS jsou tato doporučení dodržena u všech fyzických serverů, které mají dostatečný počet adaptérů a tam, kde to má význam z hlediska dalších prvků. Např. vSwitch, který realizuje připojení samostatného segmentu sítě pro zálohování (10Gbps propoj DR1 – DR2, viz obrázek č. 16) je realizován pouze jedním adaptérem. Je to z toho důvodu, že na centrále PNS se nachází pouze dva 10Gbps switche. Přiřazení vmnic adaptérů je vidět na obrázku č. 29.

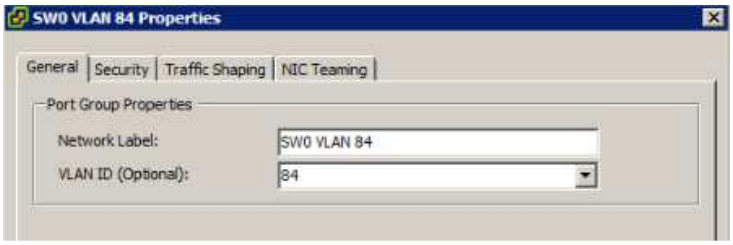


Obrázek 29 - přiřazení vmnic adaptérů k virtuálnímu switchi

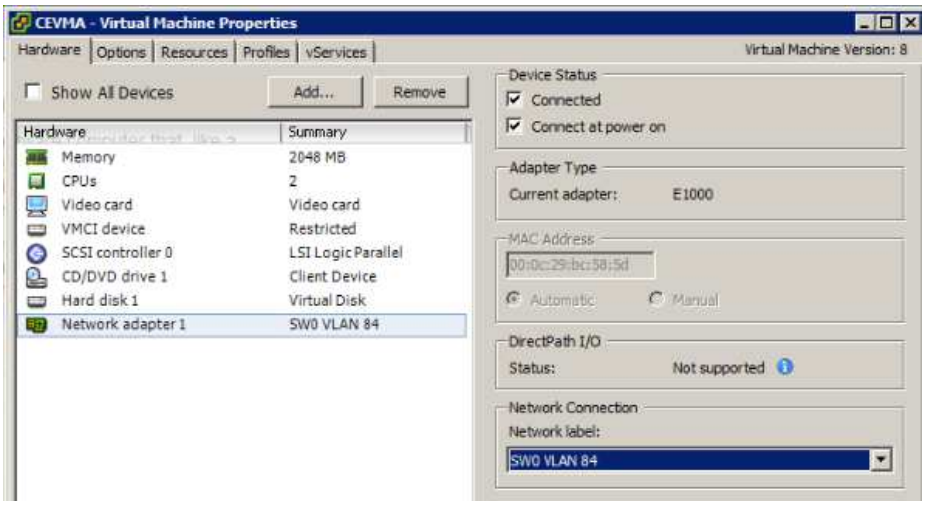
Dalším parametrem, který budeme konfigurovat je počet portů, které bude vSwitch obsahovat. Počet portů určuje kolik VM bude možné k vSwitchi připojit. Defaultní hodnota je 120, maximum je 4088 na jeden vSwitch (platné pro verzi ESXi 5.5). V případě použití více vmnic adaptérů, máme možnost nastavit NIC Teaming, o kterém se zmíním dále.. V případě potřeby můžeme nastavit řízení šířky přenosového pásma (Traffic Shaping). Toto nastavení se promítne na každý virtuální adaptér připojený k vSwitchi. V prostředí PNS není požadavek na řízení šířky pásma, volba proto nastavena nebude.

Síťové prostředí PNS je relativně složité. Je použita segmentace sítě pomocí VLAN, z nichž některé potřebujeme zpřístupnit ESXi serverům. K tomuto účelu slouží tzv. Port Group. Každá Port Group odpovídá jednomu segmentu sítě, tedy právě jedné VLAN. Nastavujeme název sítě a VLAN ID (obrázek č. 30). Port Group následně přiřazujeme jednotlivým VM. Tím určíme, do jaké sítě VM patří (např. 192.168.87.0/24, 172.22.1.0/28 apod.). Přiřazení Port Group k VM je vidět na obrázku č. 31. Vhodné je od sebe pomocí VLAN oddělit např. serverový síťový provoz od klientského a obecně VLAN konfigurovat tak, aby v rámci jedné VLAN komunikovaly napřímo pouze prvky stejného typu, tedy např. servery, koncové stanice, IPT zařízení apod. Toto se netýká pouze virtulizovaného prostředí, ale obecně. Jedním z důvodů je omezení velikosti broadcastové domény, možnosti vytvářet ACL mezi jednotlivými segmenty sítě apod. Podmínkou použití VLAN je podpora a správná konfigurace této technologie na síťových prvcích. Nad jednotlivými

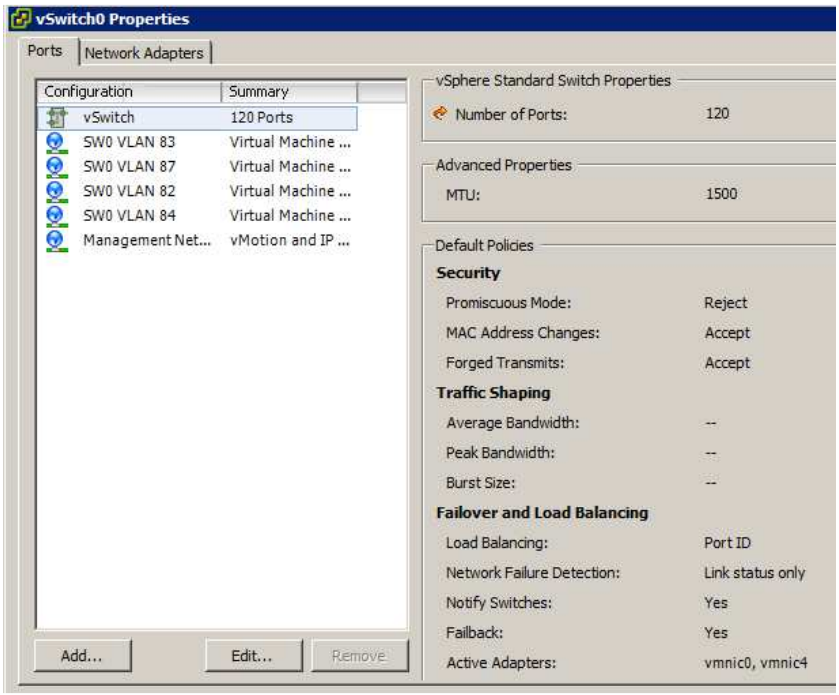
Port Group je možné měnit nastavení Security, Traffic Shaping a NIC Teaming. V našem případě konfiguraci na úrovni jednotlivých Port Group neměníme, přebírá se proto z nadřazeného vSwitche.



Obrázek 30 - vytvoření Port Group



Obrázek 31 - přiřazení Port Group konkrétní VM



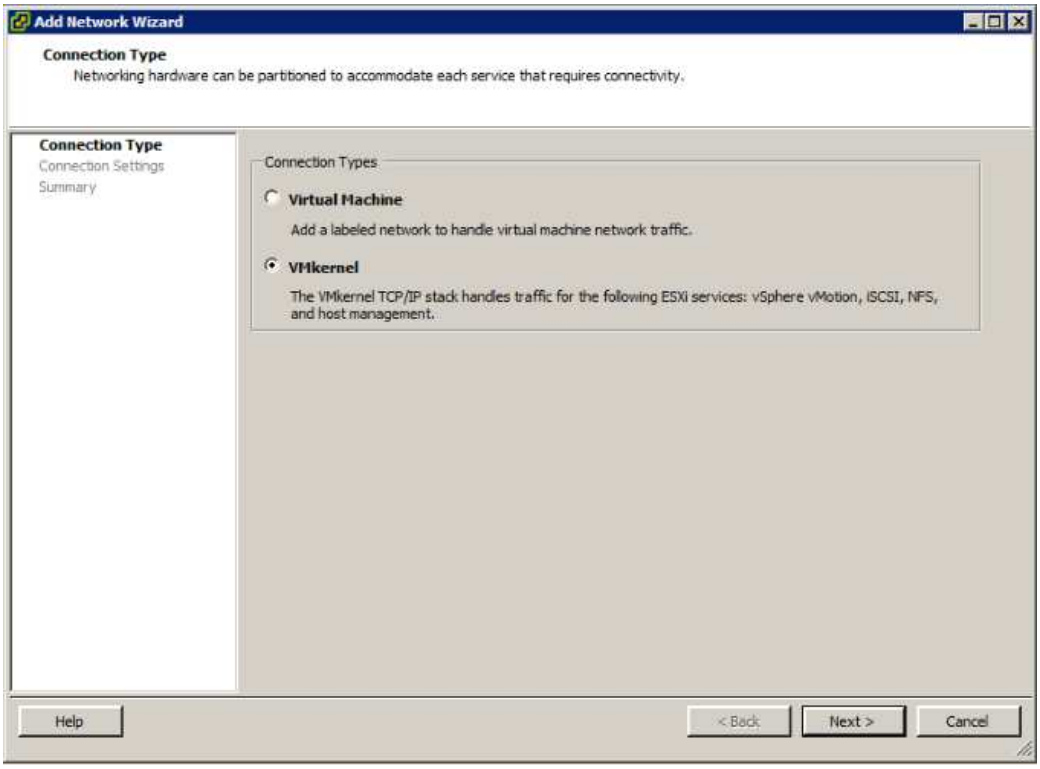
Obrázek 32 - nakonfigurovaný vSwitch

4.4.4.3 VMkernel port

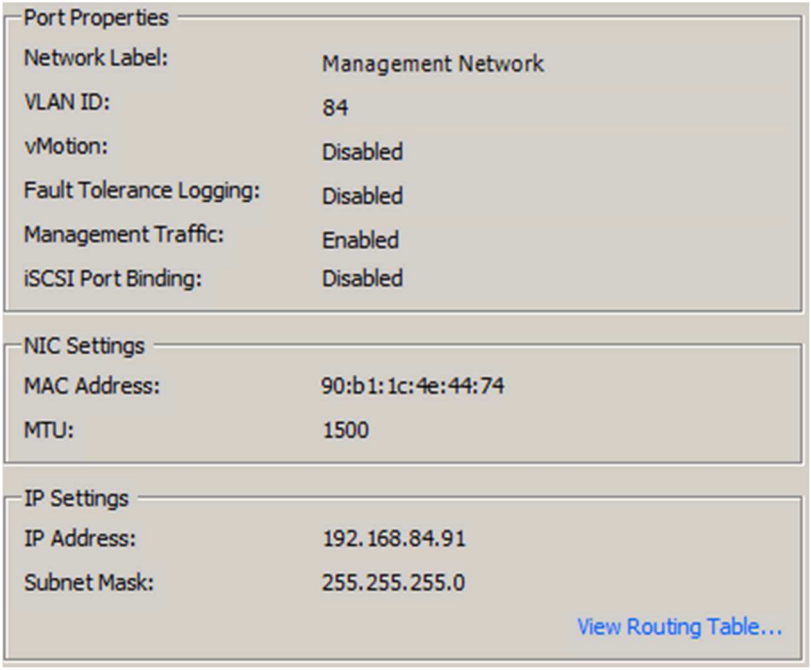
VMkernel port je specifický port, jehož úkolem je zachytávat síťový provoz jednotlivých služeb ESXi serveru. VMkernel port může být definován pro:

- Management Traffic
- Fault Tolerance Logging
- vMotion
- iSCSI a NFS provoz

Vyznačuje se tím, že má přiřazenu IP adresu. Pojmy vMotion a Fault Tolerance budou vysvětleny v dalších kapitolách. VMkernel port se vytváří na úrovni vSwitche (obrázek č.33).Vytvoření Konfiguraci VMkernel portu znázorňuje obrázek č. 33. Vytvořený VMkernel port pro Managemnt Traffic vidíme na obrázku č. 34.



Obrázek 33 - vytvoření VMkernel portu



Obrázek 34 - vytvořený VMkernel port pro Managemnt Network

4.4.4.4 NIC Teaming

NIC Teaming v sobě zahrnuje mechanismy pro zjištění a následné řešení problémů na úrovni připojení ESXi serveru k síti (Network Failover Detection) a řízení rozložení zátěže (Load Balancing).

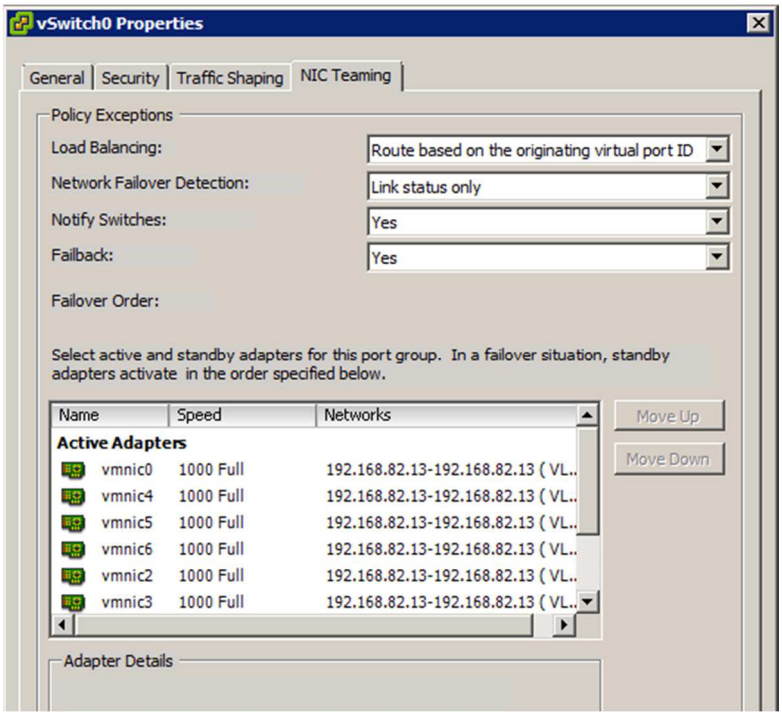
Network Failover Detection - může fungovat dvěma způsoby. Prvním je pouhá detekce stavu portu síťového adaptéru (connected nebo disconnected). V případě změny stavu jednoho z adaptérů se veškerý provoz směruje přes další funkční (Active) adaptér, či je použit do té doby záložní (Standby) adaptér.

Druhým způsobem je použití metody Beacon Probing, která funguje tak, že ze všech adaptérů posílá v určitých periodách broadcastové zprávy. Tyto broadcasty switch přeposílá automaticky na všechny porty, které jsou v jedné broadcastové doméně, tedy i na všechny ostatní adaptéry v teamu. Pokud je detekována ztráta tří po sobě jdoucích broadcastových paketů, adaptér je vyhodnocen jako disconnected. Tento způsob detekce je doporučeno použít v případě tří a více adaptérů. Pokud by byl použit pouze se dvěma adaptéry, a došlo by k výpadku na jednom z nich, nelze s určitostí poznat, o který z adaptérů se jedná. Servery v PNS jsou nakonfigurovány prvním způsobem, tedy Link status only. Všechny adaptéry jsou ve stavu Active. V případě výpadku některého z nich je provoz směrován zbývajícími funkčními adaptéry.

Load Balancing – existuje několik možností, ze kterých si můžeme vybrat. Nejpoužívanější možnosti jsou Route based on the originating virtual switch port ID a Route based on IP hash.

Route based on the originating virtual switch port ID – pro odesílání i příjem dat se používá vždy stejný fyzický adaptér. Jedna VM, resp. každý virtuální adaptér VM může komunikovat pouze přes jeden fyzický adaptér. Výběr konkrétního síťového adaptéru je v režii ESXi serveru. Tato možnost je vybrána jako defaultní nastavení.

Route based on IP hash – výběr fyzického adaptéru se provádí pro každý paket na základě výpočtu hash hodnoty. Hash se počítá ze zdrojové a cílové IP adresy. Všechny síťové adaptéry ze stejné skupiny (teamu), musí být přiřazeny do jednoho fyzického switche (popřípadě být součástí jednoho stacku mezi vícero switchi). Z těchto portů musí být vytvořen agregovaný port (switch musí podporovat standard IEEE 802.3ad). Na Cisco switchích se tato funkce nazývá EtherChannel. Při konfiguraci v prostředí na centrále PNS bylo cílem použít tuto metodu, bohužel to díky typům použitých Cisco switchů nebylo možné. Každý ESXi server je připojen současně do dvou různých switchů. Jedná se o modely Cisco Catalyst WS-C2960G-48-TC-L a Cisco Catalyst WS-C3560G-48TS. Tyto switche nepodporují vytvoření jednoho agregovaného portu mezi vícero prvky, což je nutný předpoklad pro konfiguraci. Použita proto byla volba Route based on the originating virtual switch port ID.



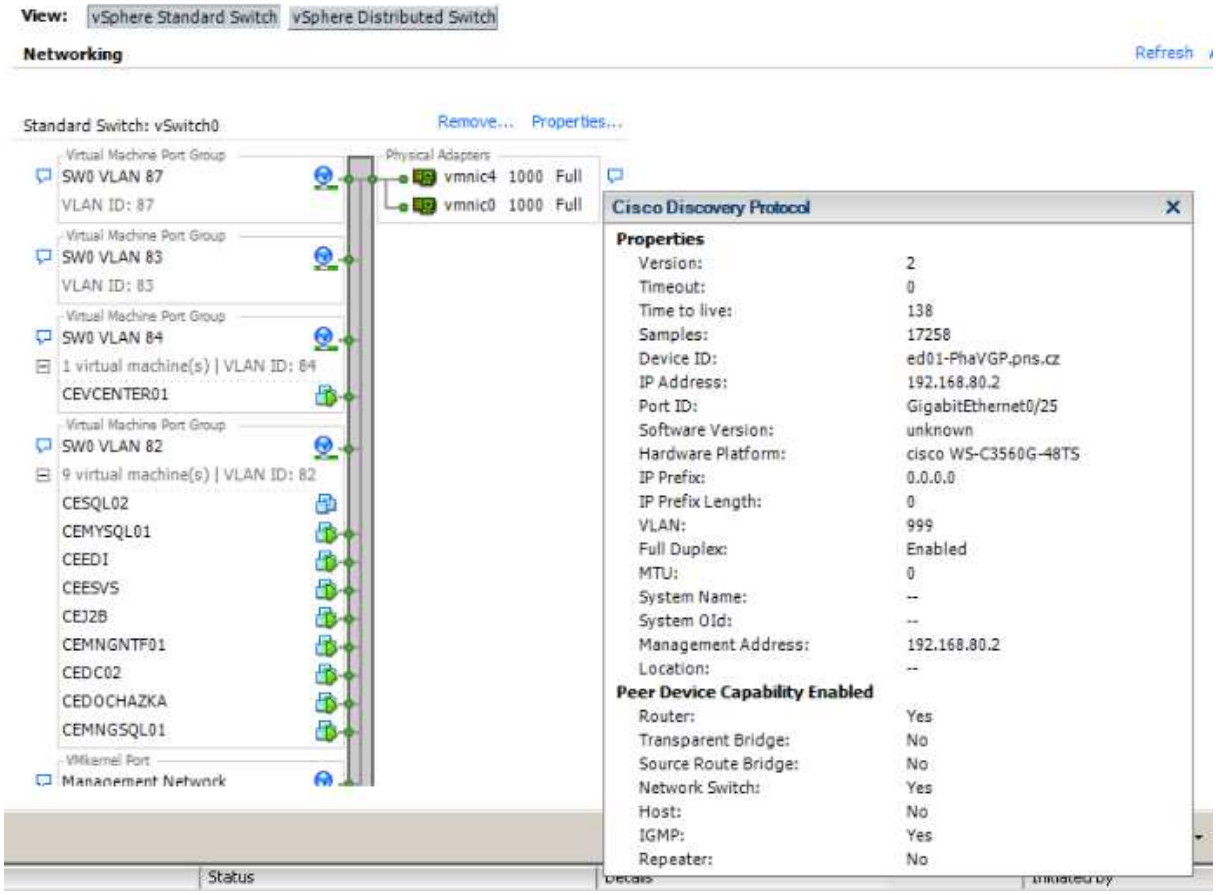
Obrázek 35 - konfigurace Nic Teaming

4.4.4.5 Konfigurace sítě pro jednotlivé ESXi servery v PNS

Na centrále PNS vytvoříme tři virtuální switche. První bude obsahovat celkem 6 vmnic adaptérů a několik Port Group pro připojení serverů, koncových stanic (stanice pro vývoj a testování), správu zařízení a VMkernel port pro Management Network. Přes tento vSwitch bude směrován hlavní síťový provoz jak mezi VM v rámci ESXi serverů, tak s jejich okolím. Ve druhém switchi bude jeden vmnic adaptér s vytvořeným iSCSI VMkernel portem (segment pro zálohování). Třetí vSwitch bude obsahovat jeden vmnic adaptér s vMotion VMkernel portem. Tímto adaptérem bude směrován vMotion provoz, který slouží k přenosu VM mezi jednotlivými ESXi servery.

V hostingovém centru GTS Nagano budou vytvořeny tři virtuální switche. V prvním bude jeden vmnic adaptér a několik Port Group pro připojení serverů v lokálním segmentu sítě, prvků IP Telefonie, správu zařízení a VMkernel port pro Managemnt Network. Druhý vSwitch bude obsahovat jeden vmnic adaptér a Port Group pro připojení firewallem odděleného segmentu sítě (DMZ2). V tomto segmentu se nachází poštovní a antispam servery, proxy server pro přístup k internetu apod. Třetí vSwitch bude rovněž obsahovat jeden vmnic adaptér s Port Group pro připojení k dalšímu firewallem odděleného segmentu sítě (DIRTYDMZ), ve kterém se nachází webový server a server pro e-shop.

Použité switche podporují Cisco Discovery Protocol (CDP), můžeme tak pomocí vSphere klienta zjistit některé užitečné informace o připojení vmnic adaptéru k Cisco switchi. Informace, které lze vyčíst znázorňuje obrázek č. 36.



Obrázek 36 - zobrazení informací o portu, do nějž je připojen vmnic adaptér

4.5 vCenter Server

Existují dva způsoby, jak vCenter Server nasadit. První způsob je použít již připravenou tzv. virtual appliance v OVF formátu a tuto následně pomocí vSphere klienta naimportovat na některý ESXi server. Výhodou tohoto způsobu je rychlost jeho nasazení a snadná konfigurace.

Druhá možnost je nainstalovat vCenter Server na operační systém Microsoft Windows Server. Tento způsob je složitější, ale má určité výhody. Touto tématikou se zabývá Justin King na VMware Blogu[23].

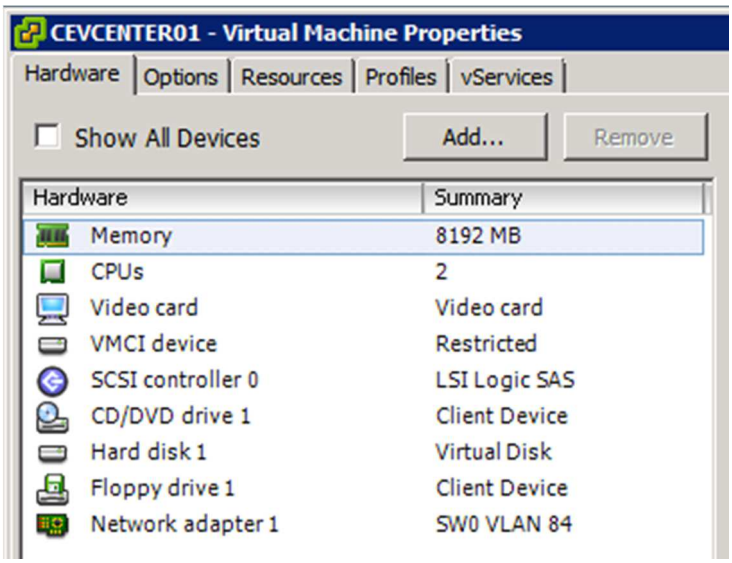
Z hlediska prostředí PNS je výhodnější použít druhou možnost, a vCenter nainstalovat na operační systém Microsoft Windows Server 2008 R2 (64bit). Důvodů pro tuto variantu je hned několik. Jednak je to použitý operační systém, v případě virtual appliance se jedná o SUSE Linux, který je upraven tak, že jej např. není možné aktualizovat a aplikovat bezpečnostní záplaty. Toto je v režii společnosti VMware a z pohledu toho, že by měla být zaručena především funkčnost samotného vCenter

[23] (King, 2014)

Serveru je to i pochopitelné. Další potenciální nevýhodou prvního způsobu je použití interní databáze a chybějící možnost využít databáze dalších výrobců. Dále pak skutečnost, že virtual appliance nepodporuje komponentu Update Manager, která tak musí být nainstalována na odděleném serveru s operačním systémem Windows.

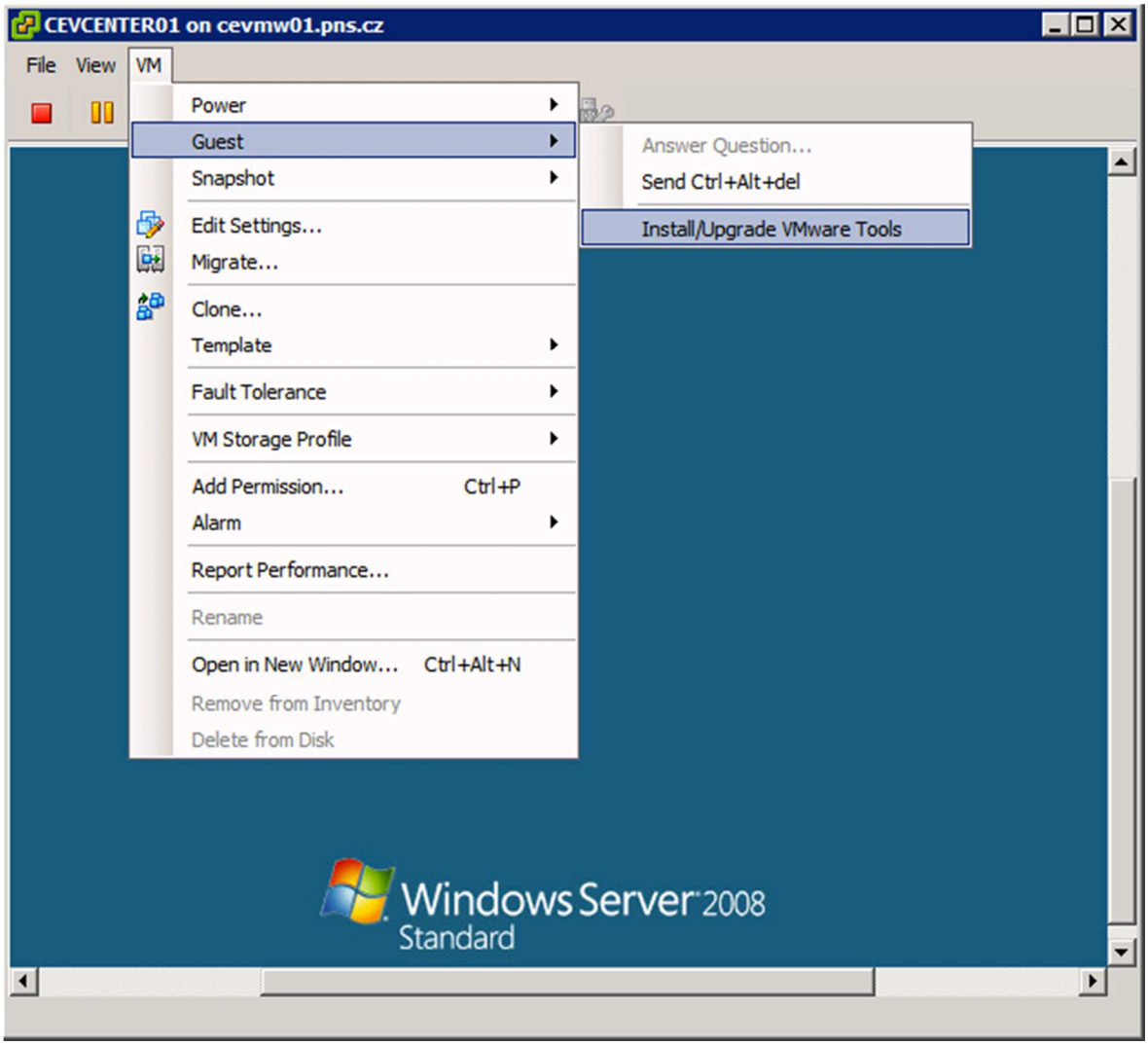
4.5.1 Instalace operačního systému a aplikace vCenter Server

K přípravě operačního systému použijeme nástroj vSphere klient. Na serveru CEVMW01 vytvoříme nový virtuální stroj pomocí průvodce, ve kterém zadáváme název VM, úložiště na kterém se bude VM nacházet, typ operačního systému volíme Microsoft Windows 2008 R2 (64bit), počet a typ síťových karet, síť (VLAN, resp. Port Group), velikost a typ disku. Parametry VM, na které bude nainstalován vCenter Server znázorňuje obrázek č. 37.



Obrázek 37 - HW parametry pro vCenter Server

Nyní se na vytvořený virtuální stroj připojíme pomocí Virtual Machine Console, která je součástí vSphere klienta. Ještě předtím nahrajeme instalační ISO soubor s operačním systémem na diskové uložiště, odkud jej připojíme k VM. Instalace operačního systému probíhá standardním způsobem a na jejím závěru je potřeba do systému nainstalovat podporu a ovladače virtuálního hardware v podobě instalačního balíku s názvem VMware Tools. Jedná se o instalační soubor typu MSI, který lze nainstalovat buď manuálně s pomocí průvodce, nebo automaticky z vSphere konzole. Na obrázku č. 30 je vidět VM Console již nainstalovaný operační systém a způsob, jakým jsme do systému nainstalovali VMware Tools.



Obrázek 38 - VM Console a instalace VMware Tools

Po úspěšné instalaci operačního systému můžeme začít s instalací aplikace vCenter Server. Ještě předtím ale vytvoříme snapshot aktuálního stavu VM. V příúadě, že by během instalace došlo k potížím, bude možné vrátit VM do stabilního stavu. Na výběr máme mezi dvěma způsoby instalace. Jsou to metody Simple Install, nebo Custom Component Install[24]. Metoda Simple Install nainstaluje všechny potřebné komponenty, kterými jsou vCenter Single Sign-On, vSphere Web Client, Inventory Service a vCenter Server. Metoda Custom Component Install umožňuje instalovat jednotlivé komponenty samostatně na více serverů a je vhodná pro střední a velká prostředí. V prostředí PNS budou všechny komponenty provozovány pouze na jednom serveru, volíme tedy metodu Simple Install. Instalace proběhla bez problému a dalším krokem bude instalace doplňku

[24] (VMware Inc., 2014J)

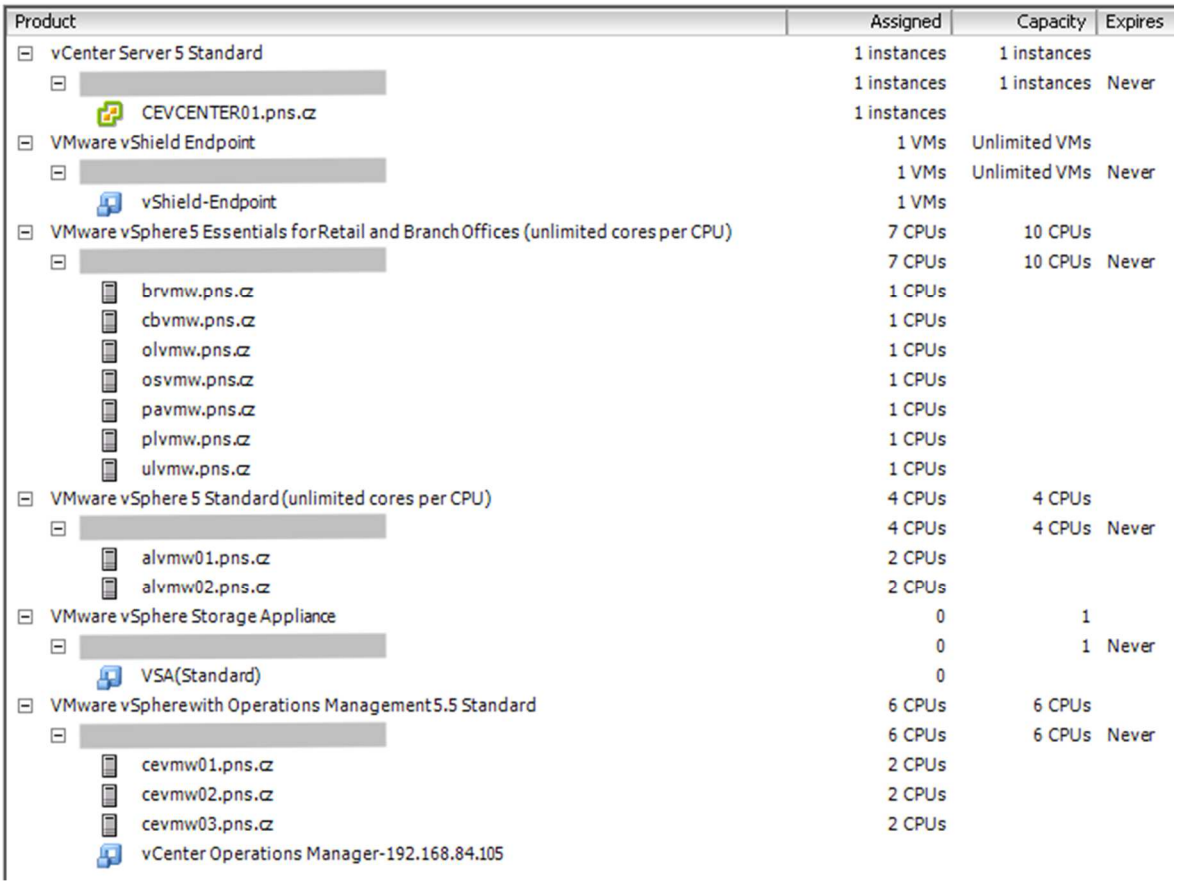
Update Manager, který slouží pro řízení stahování a instalaci aktualizací a dále vSphere klienta.

4.5.2 Licence

Licenční model společnosti VMware je nastaven tak, že počítá s osazenými CPU sockety. Jeden CPU socket může obsahovat maximálně 6 jader (core) a spotřebuje jednu CPU licenci. Pokud máme server se dvěma osazenými CPU, každý CPU po čtyřech jádrech, potřebujeme dvě CPU licence. Pokud máme server se dvěma sockety, kde osazený je pouze jeden, server spotřebuje jednu CPU licenci.

V prostředí PNS bylo nutné pokrýt 12 serverů takovým způsobem, aby je bylo možné přiřadit a spravovat jedním vCenter Serverem. Z toho 5 serverů je součástí celkem dvou clusterů, zbytek jsou servery na divizích bez požadavku na pokročilé funkce, které umožňuje cluster. Limitující je zde požadavek administrace jedním vCenter Serverem, který dopředu vyřazuje použití licenčních balíků Essentials Kit a Essentials Kit Plus. Další možnou verzí je licence Standard v počtu celkově 10 CPU, z toho 4 CPU bez omezení na počet jader a 6 CPU s dodatečnou licencí na VMware Operations Management. ESXi servery na divizích jsou pokryté licencí Essentials for Retail and Branch Offices v počtu deseti kusů. Tato licence dovoluje připojení serverů k vCenter Serveru a umožňuje tak jejich administraci. Přehled licencí a funkcionalit má společnost VMware uveden na svých internetových stránkách[25]. Přehled použitých licencí je vidět na obrázku č. 39.

[25] (VMware Inc., 2014K)



Product	Assigned	Capacity	Expires
vCenter Server 5 Standard	1 instances	1 instances	
[redacted]	1 instances	1 instances	Never
CEVCENTER01.pns.cz	1 instances		
VMware vShield Endpoint	1 VMs	Unlimited VMs	
[redacted]	1 VMs	Unlimited VMs	Never
vShield-Endpoint	1 VMs		
VMware vSphere 5 Essentials for Retail and Branch Offices (unlimited cores per CPU)	7 CPUs	10 CPUs	
[redacted]	7 CPUs	10 CPUs	Never
brvmw.pns.cz	1 CPUs		
cbvmw.pns.cz	1 CPUs		
olvmw.pns.cz	1 CPUs		
osvmw.pns.cz	1 CPUs		
pavmw.pns.cz	1 CPUs		
plvmw.pns.cz	1 CPUs		
ulvmw.pns.cz	1 CPUs		
VMware vSphere 5 Standard (unlimited cores per CPU)	4 CPUs	4 CPUs	
[redacted]	4 CPUs	4 CPUs	Never
alvmw01.pns.cz	2 CPUs		
alvmw02.pns.cz	2 CPUs		
VMware vSphere Storage Appliance	0	1	
[redacted]	0	1	Never
VSA(Standard)	0		
VMware vSphere with Operations Management 5.5 Standard	6 CPUs	6 CPUs	
[redacted]	6 CPUs	6 CPUs	Never
cevmw01.pns.cz	2 CPUs		
cevmw02.pns.cz	2 CPUs		
cevmw03.pns.cz	2 CPUs		
vCenter Operations Manager-192.168.84.105			

Obrázek 39 - licence VMware

4.5.3 Logická struktura objektů na úrovni vCenter Serveru a jejich konfigurace

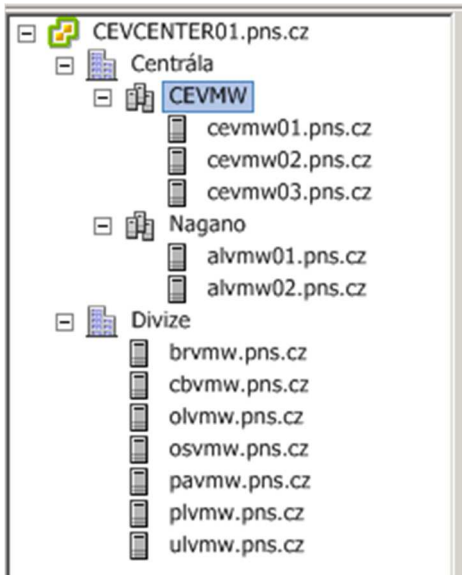
Na úrovni vCenter Serveru budeme definovat logickou strukturu prostředí PNS. K dispozici máme několik stavebních bloků, kterými toho docílíme. Návrh logické struktury je důležitý krok a má vliv např. na vzájemnou spolupráci jednotlivých ESXi serverů, oprávnění apod.

- Datacenter je primární kontejner, který obsahuje ESXi servery (hosty), virtuální stroje, složky a clustery
- Cluster je skupina hostů, která sdružuje jejich prostředky, které se stávají součástí clusteru, který je obhospodařuje. Na úrovní clusteru se definuje vSphere High Availability (HA) a vSphere Distributed Resource Scheduler (DRS).

V prostředí PNS se logická struktura skládá ze dvou datacenter a dvou clusterů. V prvním datacentru (centrála) jsou umístěny všechny servery z obou lokalit v Praze. Tyto servery jsou dále rozmístěny ve dvou clusterech, které odpovídají centrále PNS (název clusteru je CEVMW) a hostingovému centru (název clusteru je Nagano). Druhé datacentrum (Divize) obsahuje ESXi servery na pobočkách. Logickou strukturu znázorňuje obrázek č. 40. Na

clusteru CEVMW je zapnuta funkce vSphere HA, která zajišťuje vysokou dostupnost tím, že periodicky monitoruje jednotlivé ESXi servery v clusteru a v případě nedostupnosti některého z nich startuje jeho VM na zbylých serverech. Monitoring probíhá formou tzv. heartbeatingu. To znamená, že je kontrolována dostupnost ESXi serverů přes Managemnt Network a současně se používá také heartbeting na úrovni úložiště, kam všechny servery v clusteru zapisují data do adresáře .vSphere-HA, čímž prokazují, že fungují správně. Oba tyto způsoby detekce jsou v prostředí PNS aktivní. Aby byl server vyhodnocen jako nedostupný, musí dojít k odmlčení jak na straně Management Network, tak úložiště.

Detekovat problém je možné také na jednotlivých VM stejnou technologií jako v předchozích případech. Heartbeating generují VMware Tools nainstalované v operačním systému jednotlivých VM. Tato možnost není v prostředí PNS povolena. Ze zkušeností vyplývá, že občas dojde k problému na úrovni VMware Tools, nicméně ve většině případů není potřeba VM restartovat.

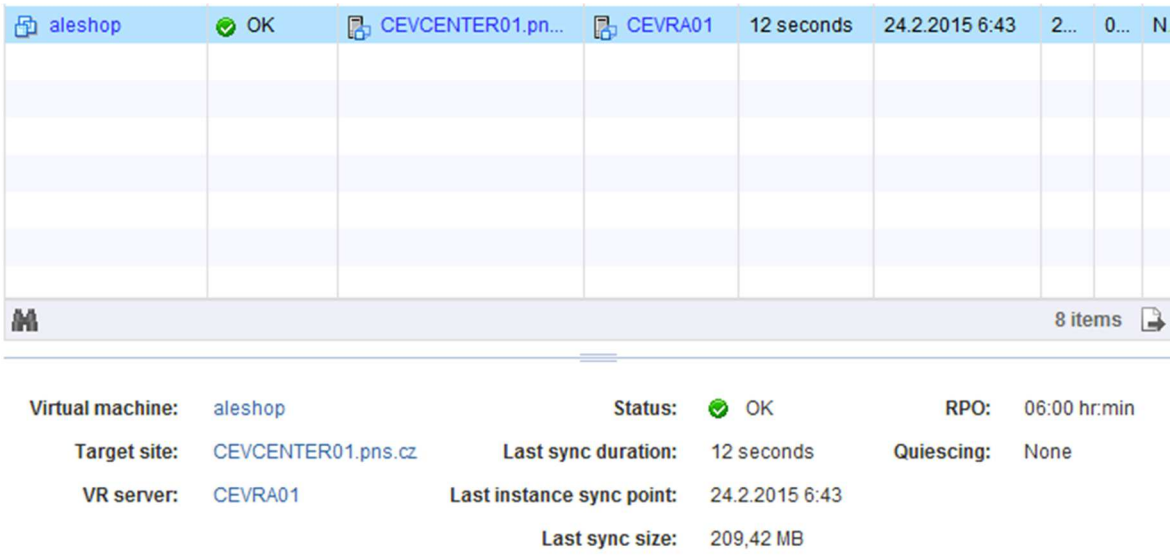


Obrázek 40 - logická struktura objektů – vCenter Server PNS

Vzhledem k tomu, že servery v hostingovém centru Nagano nemají sdílené úložiště, není na clusteru povolena funkce vSphere HA. Jako optimální řešení této situace se ukázalo být využití replikací na úrovni VM. Tuto funkci zajišťuje nástroj vSphere Replication (nasazený v podobě VMware appliance). Nástroj je integrovaný do vCenter Serveru, jeho ovládání je možné pomocí nástroje VMware Web Client, což je náhrada původního vSphere klienta. VM jsou rozděleny mezi oba ESXi servery v clusteru a každá VM má nastavenu replikaci na druhý server. Replikace probíhají každých 6 hodin.

V případě nedostupnosti jednoho serveru je potřeba manuální zásah administrátora, který na funkčním serveru zaregistruje replikované VM, které následně nastartuje. Kontrola stavu replikace pomocí nástroje VMware Web Client je na obrázku č. 41.

Zvažováno bylo také řešení VMware VSA[26] (vSphere Storage Appliance), které vytváří softwarově definované sdílené úložiště z interních disků umístěných v serverech. Během nasazení se však objevily výkonostní problémy, problémy se síťovým zapojením, resp. jeho nároky a v neposlední řadě fakt, že společnost VMware toto řešení přestala podporovat k 1.4.2014. Nástupcem VSA je produkt VMware Virtual SAN, který je však určen pro větší prostředí a nutný předpoklad jeho nasazení jsou minimálně 3 ESXi servery.



Obrázek 41 - kontrola stavu replikace VM v hostingovém centru

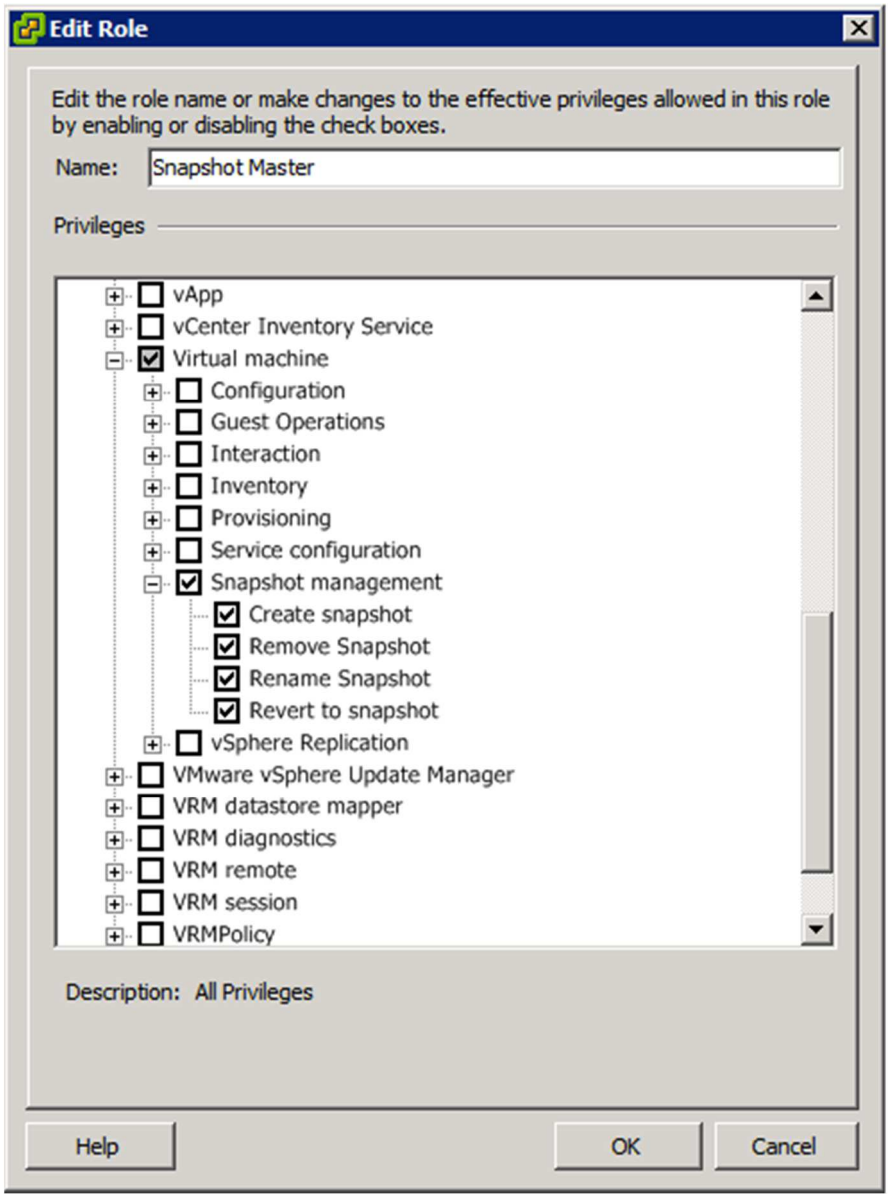
ESXi servery na pobočkách nejsou proti výpadku chráněné. Na servery je poskytována podpora společností Dell s reakční dobou vyřešení problému do dalšího pracovního dne. Případný výpadek a nedostupnost VM v řádu několika hodin je akceptovatelný a na chod společnosti nemá vážnější vliv.

4.5.4 Řízení přístupu a oprávnění

Na úrovni vCenter Serveru lze definovat role, které lze následně přiřadit uživatelům nebo skupinám. Společnost PNS využívá adresářových služeb společnosti Microsoft, na které lze vCenter Server napojit a pracovat tak s uživatelskými účty a skupinami uloženými v Active Directory. Za tímto účelem byla vytvořena skupina CE_ESXi_Admins, jejíž členové mají plná oprávnění spravovat virtuální prostředí. Dále

[26] (VMware Inc., 2014F)

bylo vytvořeno několik specifických rolí, které byly přiděleny administrátorům na pobočkách a dalším uživatelům. Vytvořenou roli, která uživateli povoluje pouze práci se snapshoty na úrovni VM ukazuje obrázek č. 42. Jak je patrné z obrázku, možnosti definování jednotlivých oprávnění jsou velice podrobné a v praxi se problém s definováním složitějších rolí nevyskytl.



Obrázek 42 - vytvoření role

4.5.5 Správa aktualizací

K řízení aktualizací slouží nástroj Update Manager. Pomocí tohoto nástroje lze definovat tzv. baseline. Baseline jsou skupiny aktualizací, které lze aplikovat na ESXi servery nebo VM. Je možné volit verze produktů, které požadujeme sledovat. V prostředí

PNS je vytvořeno několik baseline, které slouží k aktualizaci ESXi serverů, upgradu ESXi na novější verze a aktualizací VMware Tools. Každý den ve 3h ráno probíhá kontrola dostupných aktualizací na serverech společnosti VMware. Pokud jsou aktualizace nalezeny, proběhne jejich stažení na vCenter Server a zároveň je poslán email administrátorům, kteří následně provedou instalaci. Po aplikování většiny aktualizací je potřeba restart ESXi serverů. Na centrále PNS je možné servery CEVMW01 a CEVMW02, které mají společné sdílené pole aktualizovat bez nutnosti výpadku dostupnosti VM. Mezi oběma servery je možné VM přesouvat za běhu pomocí technologie vMotion. U serveru CEVMW03 a obou serverů v hostingovém centru Nagano se aktualizace neobejde bez alespoň krátkého výpadku dostupnosti VM. Technologii vMotion lze v tomto případě rovněž využít, avšak přenášená VM musí být vypnutá. V takovém případě je možné provést přesun na jiný server i zároveň úložiště a ESXi server aktualizovat. Aktualizace serverů na divizích znamená odstávku VM po dobu aktualizace.

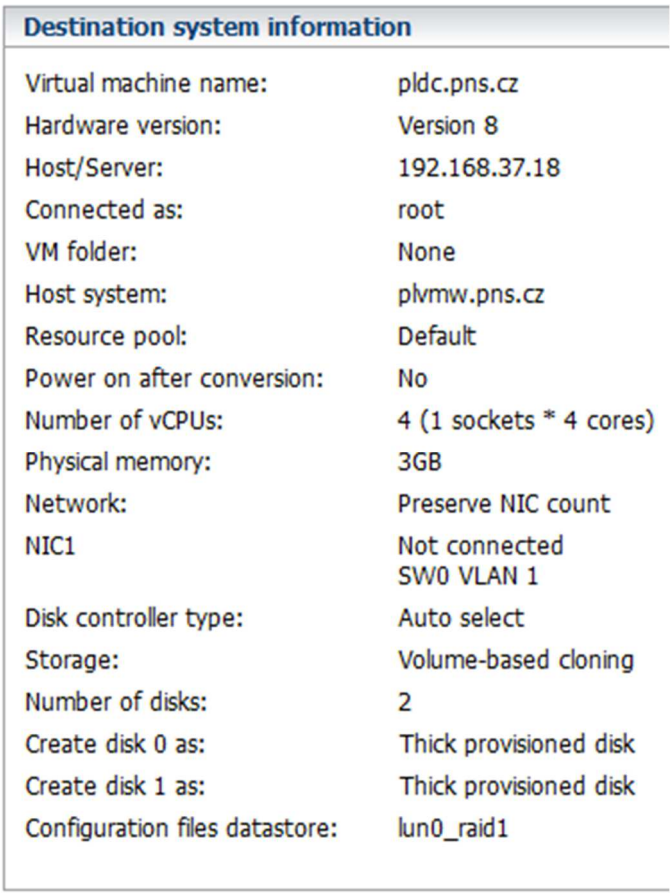
4.6 Migrace fyzických serverů do virtuálního prostředí

Společnost VMware poskytuje nástroj vCenter Converter Standalone Client[27], který umožňuje migraci fyzického serveru do virtuálního prostředí. Tento proces se nazývá P2V (Physical to Virtual). Podporovány jsou operační systémy společnosti Microsoft, Linux a diskové obrazy dalších výrobců (Microsoft Hyper-V, Virtual Server a Virtual PC, Parallels Desktop, Symantec System Recovery, Norton Ghost a další).

V prostředí PNS bylo potřeba tento proces použít několikrát na každé z lokalit. Následující scénář popisuje migraci pobočkového serveru do virtuálního prostředí. V prvním kroku byl nakonfigurovaný ESXi server poslán interní dopravou na danou lokalitu. Po připojení serveru do pobočkové sítě byla provedena jeho kontrola a registrace na vCenter Server. Díky tomu, že vCenter Converter Client umožňuje ve vytvořené migrační úloze zvolit, resp. deaktivovat volbu finální synchronizace, je možné celou migraci rozdělit do několika úloh. Toho bylo využito také v případě migrací serverů v prostředí PNS. První a zároveň nejdelší část P2V procesu, kdy byla migrována data o velikosti řádově 500 až 600GB, byla spuštěna v době, kdy byl server nejméně vytížen. Ve chvíli, kdy bylo naplánováno odstavení fyzického serveru, byla spuštěna finální synchronizace, která zajistila zapracování změn od poslední dílčí synchronizace a následné vypnutí fyzického serveru. Následně na to byl vytvořen snapshot migrovaného serveru

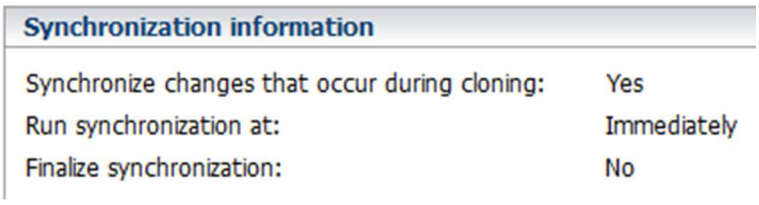
[27] (VMware Inc., 2014H)

a provedena optimalizace operačního systému. Byly odstraněny veškeré nepotřebné komponenty jako např. původní ovladače a programy. Na závěr byly nahrány ovladače virtuálního hardware v podobě VMware Tools, byla zkontrolována správná funkčnost a jako poslední krok byl odstraněn snapshot. Vytvořená migrační úloha je na obrázku č. 43. Obrázky č. 44 a č. 45 ukazují možné nastavení synchronizace.



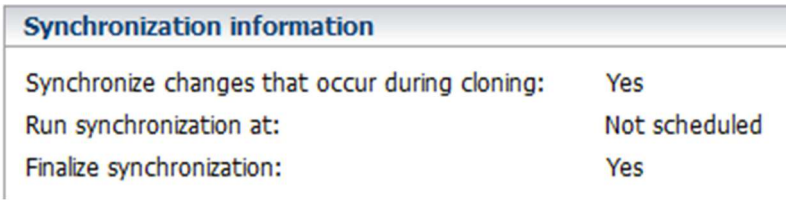
Destination system information	
Virtual machine name:	pldc.pns.cz
Hardware version:	Version 8
Host/Server:	192.168.37.18
Connected as:	root
VM folder:	None
Host system:	plvmw.pns.cz
Resource pool:	Default
Power on after conversion:	No
Number of vCPUs:	4 (1 sockets * 4 cores)
Physical memory:	3GB
Network:	Preserve NIC count
NIC1	Not connected SW0 VLAN 1
Disk controller type:	Auto select
Storage:	Volume-based cloning
Number of disks:	2
Create disk 0 as:	Thick provisioned disk
Create disk 1 as:	Thick provisioned disk
Configuration files datastore:	lun0_raid1

Obrázek 43 - vytvořená migrační úloha



Synchronization information	
Synchronize changes that occur during cloning:	Yes
Run synchronization at:	Immediately
Finalize synchronization:	No

Obrázek 44 - dílčí synchronizace



Synchronization information	
Synchronize changes that occur during cloning:	Yes
Run synchronization at:	Not scheduled
Finalize synchronization:	Yes

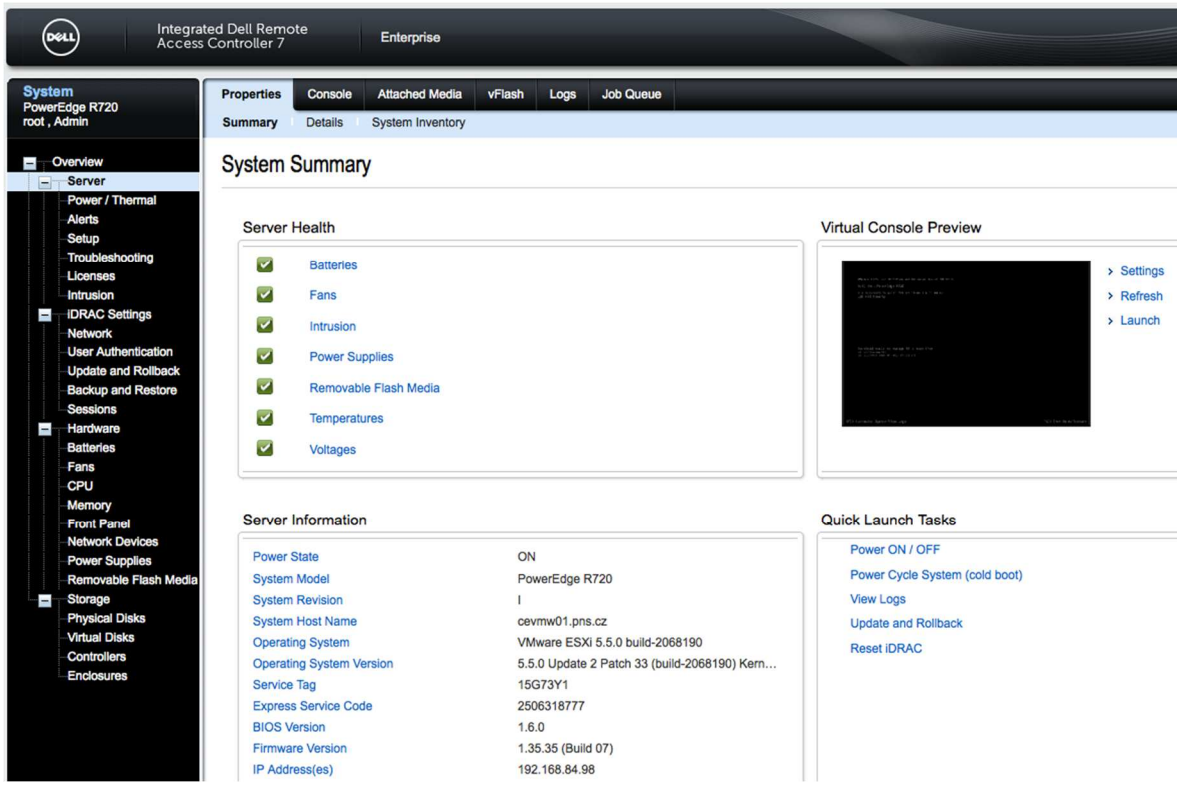
Obrázek 45 - finální synchronizace

4.7 Monitoring a správa prostředí

Na monitoring a správu prostředí můžeme nahlížet z několika hledisek. Monitoring a správa HW, virtuální infrastruktury a virtuálních strojů. K tomuto účelu existuje celá řada nástrojů a některé z nich pokrývají více oblastí.

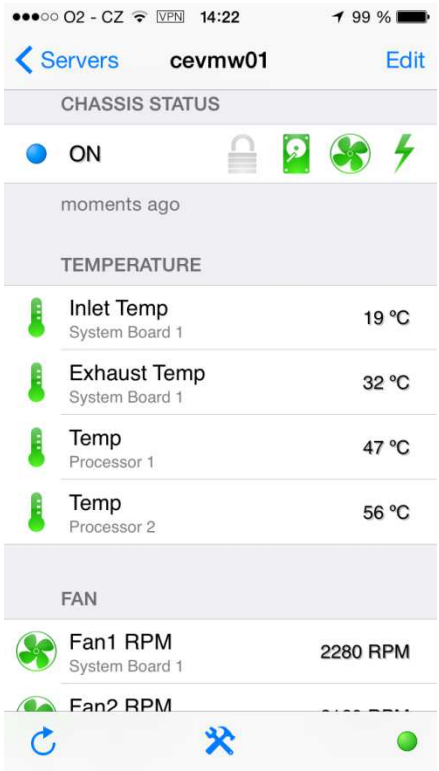
4.7.1 Monitoring a správa HW

Při nasazení virtualizace je velice důležitý přehled o stavu hardware jednotlivých částí infrastruktury a možnost vzdálené kontroly serveru. V prostředí PNS je tato oblast řešena několika způsoby. Všechny ESXi servery jsou osazeny kontrolérem Dell DRAC / iDRAC (u nových serverů doplněným o Lifecycle Kontroler), který umožňuje vzdálenou správu (výstup obrazovky serveru do konzole, připojení ISO obrazů apod.), monitoring, upgrade firmware a nasazení OS. Možné je rovněž zasílání zpráv v podobě SNMP trapů na centrální management server Dell OpenManage Essentials, který následně zprávy zpracuje, vyhodnotí, a dle nastavených pravidel zasílá na definované kontakty (email, SMS) jednotlivým administrátorům. Na tento server jsou nasměrována obě disková pole na centrále PNS. Webové rozhraní, které poskytuje DRAC resp. iDARC kontrolér je vidět na obrázku č. 46.



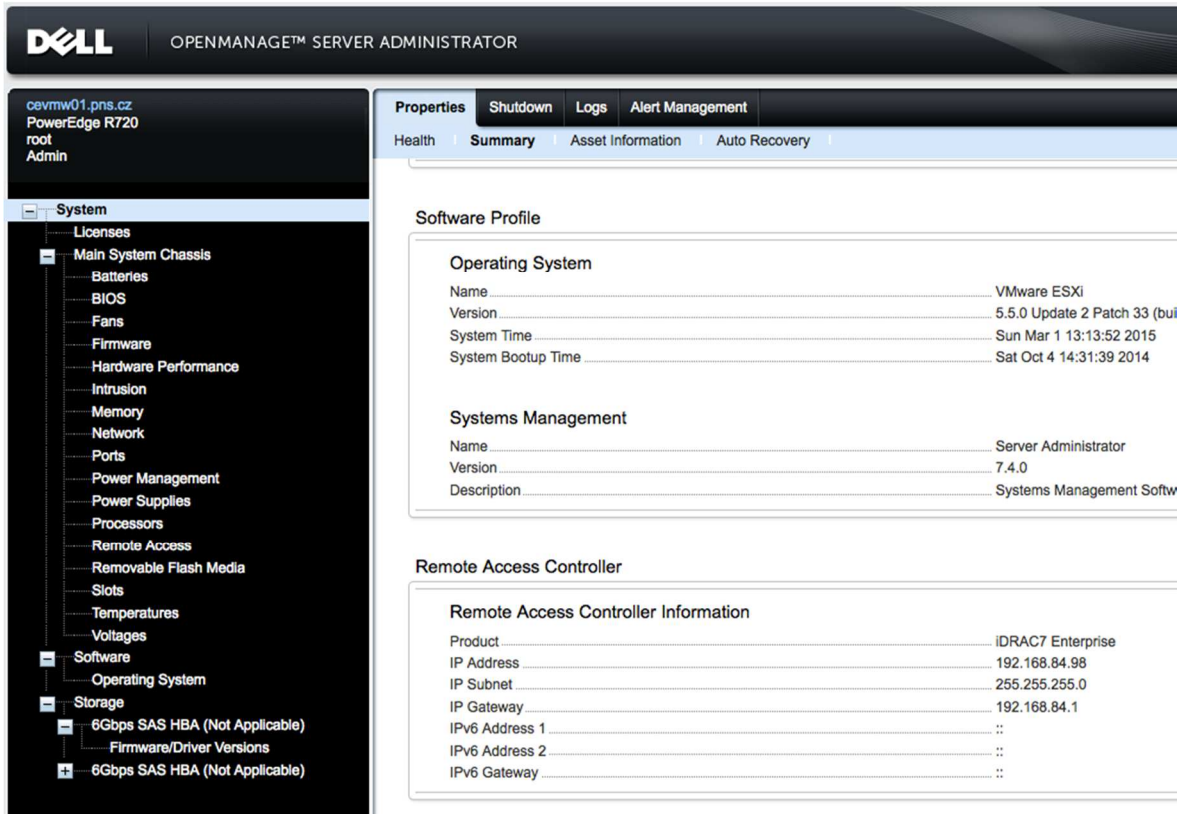
Obrázek 46 - webové rozhraní DRAC / iDRAC kontroléru

Všechny ESXi servery podporují a mají nastaven IPMI (Intelligent Platform Management Interface). Díky IPMI je možný vzdálený přístup na monitoring HW, diagnostiku a řízení na úrovni zapnutí / vypnutí / restartu serveru. To je velice výhodné, pokud se server dostane do nedefinovaného stavu, nebo jej např. korektně vypne UPS při výpadku napájení. Protože má IPMI poměrně hodně bezpečnostních nedostatků, je přístup povolen pouze z vnitřní sítě PNS a VPN. Na obrázku č. 47 je vidět aplikace IPMI touch dostupná pro systém iOS společnosti Apple.



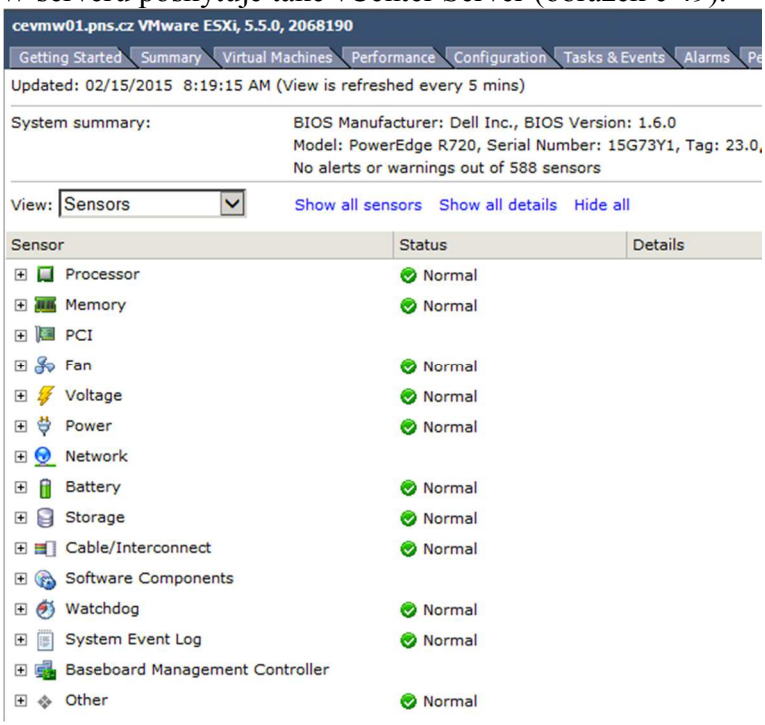
Obrázek 47 - iOS aplikace IPMI touch

Na všech ESXi serverech je nainstalována podpora správy hardware serverů Dell OpenManage Server Administrator vSphere Installation Bundle. Každý ESXi server je dostupný pomocí nástroje Dell OpenManage Server Administration přes webové rozhraní, které poskytuje celou řadu informací včetně možností konfigurace některých komponent a zasílání SNMP trapů na centrální server stejně jako v případě DRAC / iDRAC kontroléru.



Obrázek 48 - Dell OpenManage Server Administrator

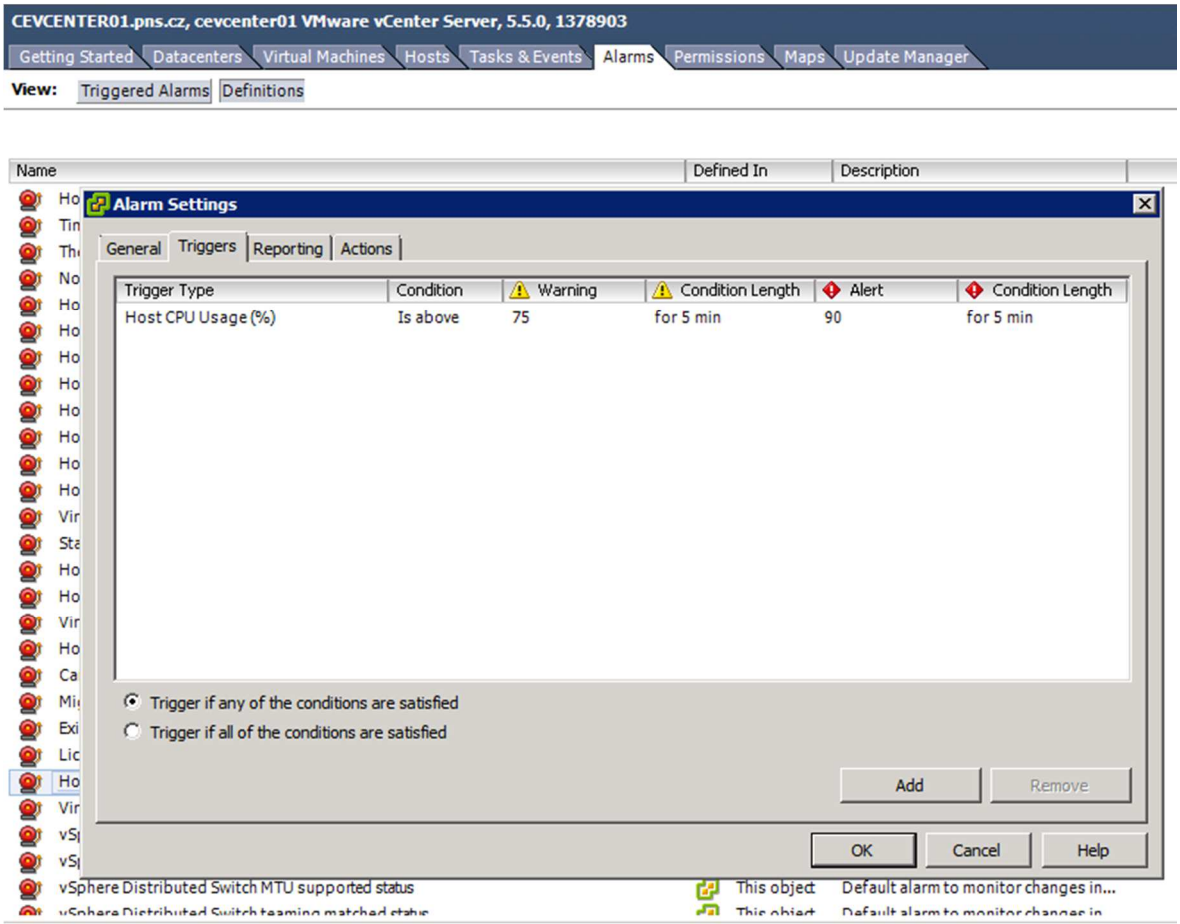
Pohled a stav HW serveru poskytuje také vCenter Server (obrázek č 49).



Obrázek 49 - pohled na stav HW pomocí vCenter Serveru

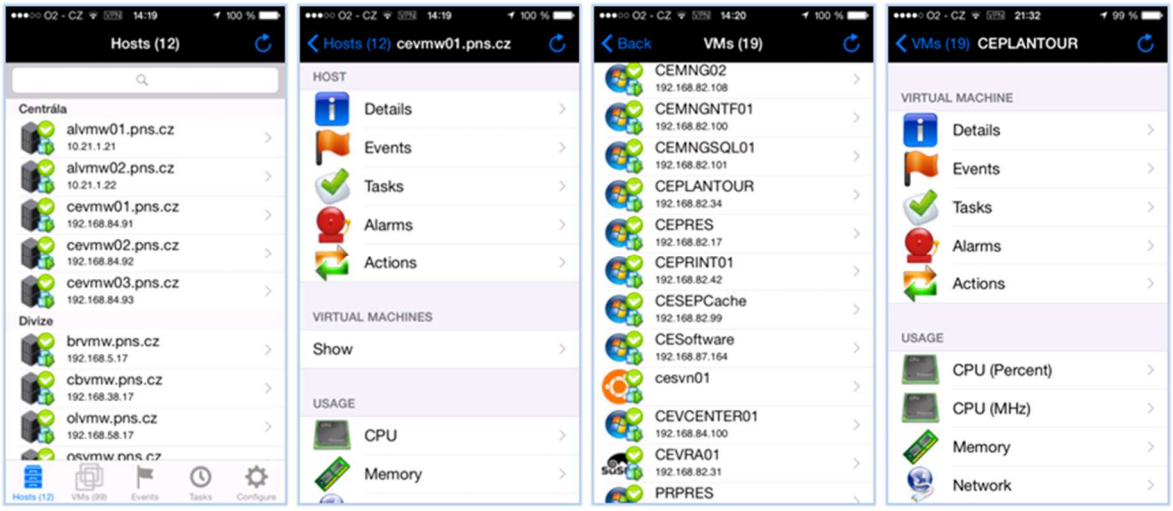
4.7.2 Monitoring a správa virtuální infrastruktury a VM

Ke správě a monitoringu virtuální infrastruktury a VM slouží v první řadě vCenter Sever, který obsahuje celou řadu událostí, na které je možné definovat alarmy. Alarmy lze použít již přednastavené, nebo nadefinovat vlastní. Každému alarmu lze přiřadit akci, která se provede v momentě, kdy k alarmu dojde. Lze nastavit např. zaslání emailu, vypnutí problémové VM, či restart celého serveru. Upozornění na jednotlivé alarmy se zobrazují přímo ve vSphere konzoli. Příklad nastavení alarmu, který reaguje na vysoké vytížení procesoru ESXi serveru je na obrázku č. 50.



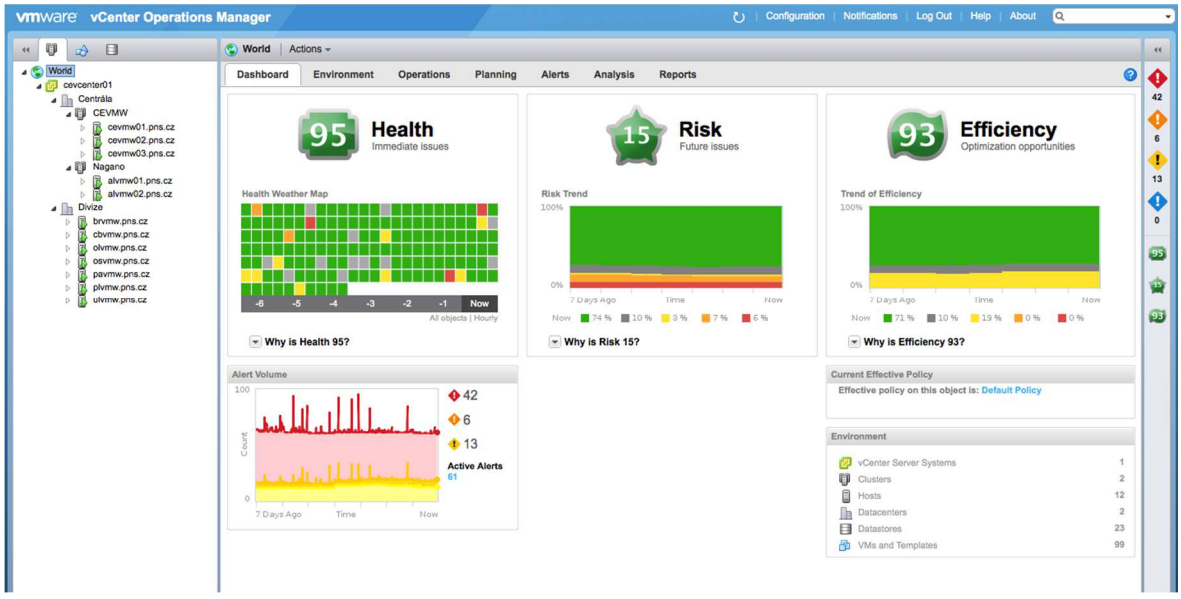
Obrázek 50 - příklad definice alarmu na vCenter Serveru

Z aplikací pro mobilní zařízení je to např. aplikace iVMControl pro systém iOS, která dokáže komunikovat s vCenter Serverem a umožňuje správu jak ESXi serverů, tak VM. S její pomocí lze např. restartovat či vypnout ESXi server, prohlížet vytížení zdrojů ESXi serverů a VM. Dále je možné přesunout VM na jiný ESXi či úložiště v clusteru, či prohlížet alarmy a úlohy.



Obrázek 51 - iOS aplikace iVMControl

Celkový pohled na stav ESXi serverů a VM poskytuje nástroj vCenter Operations Manager společnosti VMware, který byl představen v kapitole 3.2.3. S jeho pomocí lze optimalizovat a předcházet problémům spojeným s výkonem celého prostředí. Dokáže upozornit na problém, který již nastal nebo může nastat s určitou pravděpodobností, např. úbytek volného místa na úložištích. Dokáže také upozornit na nevhodně natavené parametry VM, např. nedostatek, nebo naopak přebytek operační paměti. Jeden z mnoha pohledů, které nástroj umožňuje je na obrázku č. 52.



Obrázek 52 - vCenter Operations Manager

Další systém, který je v prostředí PNS používán je ZABBIX. Jedná se o Open Source dohledový systém určený do podnikového prostředí, který je možné použít

k monitorování prvků jako jsou servery, prvky síťové infrastruktury, IPT, tiskárny apod. ZABBIX podporuje celou řadu protokolů pro dohled od jednoduchého ICMP (ping na síťové prvky a vyhodnocení jejich dostupnosti), SNMP (dotazování na konkrétní OID), IPMI až po pokročilou komunikaci pomocí agenta, kterého lze použít na systémech s OS Microsoft a Linux. Informace lze zobrazit pomocí internetového prohlížeče či využít některou z mobilních aplikací pro systém Android a iOS (MobileOP, Mozaby, Zabbkit apod.). Virtuální infrastruktura je ve společnosti PNS monitorována systémem ZABBIX na několika úrovních. ESXi servery a VM jsou monitorovány z hlediska dostupnosti na síti (ICMP ping), SNMP (využití CPU, RAM, síťové adaptéry, úložiště apod.). Na pokročilejší dohled je využit agent, který je nainstalován v OS dané VM a poskytuje informace ZABBIX serveru. Příklad využití agenta je např. SQL dotaz do databáze vCenter Serveru, odkud se získává hodnota aktuálního počtu snapshotů na všech VM, které jsou pod správou vCenter Serveru. Hodnoty se následně zanáší do grafu viz obrázek č. 53. Lze zobrazit historická data, což dává možnost zkoumat současné hodnoty a porovnávat je s hodnotami nasbíranými v průběhu času. To může být vhodné např. pro porovnání využití CPU ESXi serverů v průběhu času, či při řešení problémů na úrovni konkrétní VM.

Obrázek 53 - ZABBIX a zobrazení počtu všech snapshotů ve vCenter Serveru

5 Zhodnocení výsledků a doporučení

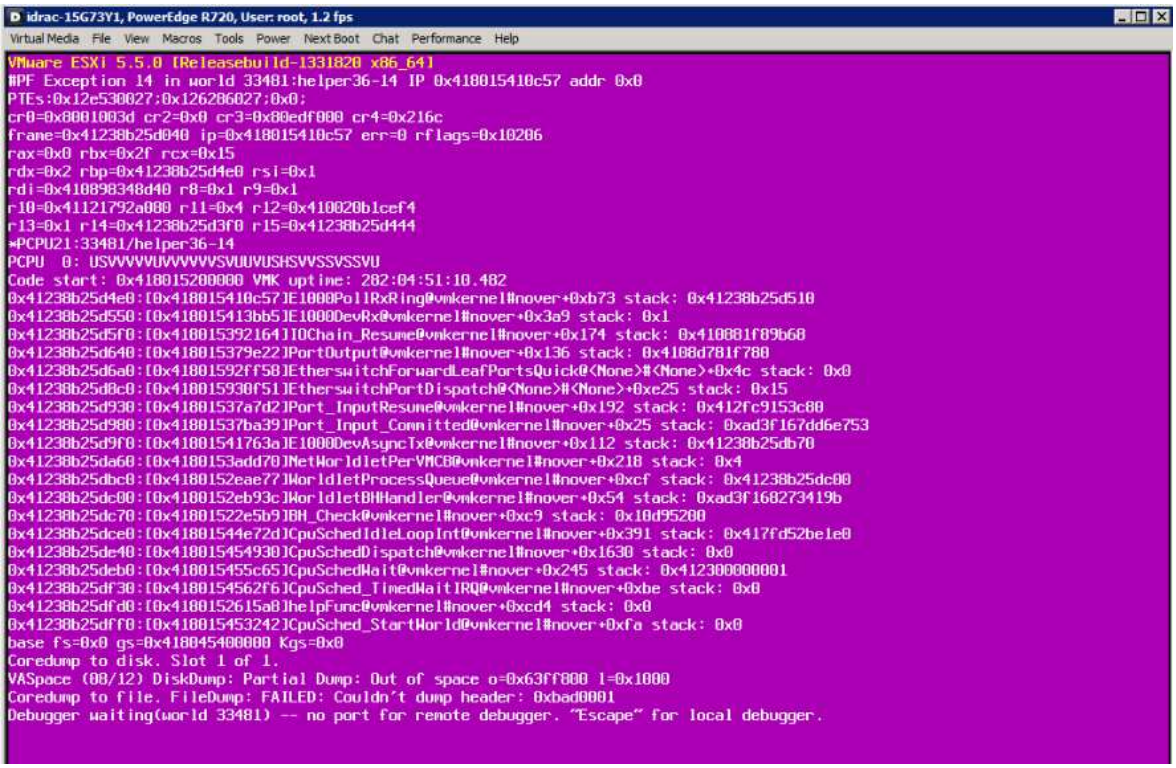
5.1 Zhodnocení a přínosy

Ke konci měsíce 02/2015 má společnost PNS většinu své serverové infrastruktury ve vnitropodnikovém virtualizovaném prostředí. Celkový počet serverů, které hostují virtuální stroje je 12. Dohromady je provozováno celkem 99 virtuálních strojů. Všechny fyzické servery označené v tabulce č. 1 jako vhodné pro virtualizaci se podařilo do nového prostředí převést. Během samotného projektu, který trval přibližně 4 měsíce se neodehrál žádný závažnější problém a podařilo se udržet vysokou dostupnost služeb, které poskytuje oddělení IT infrastruktury. Všechny navržené postupy a jednotlivé kroky se ukázaly být správné a prostředí splňuje nároky, na které bylo navrženo.

Během provozu se vyskytlo několik problémů, které nebylo možné dopředu předvídat. První problém nastal s jedním z virtualizovaných serverů, který je specifický tím, jaké výpočty na něm probíhají. Jedná se o server na kterém je provozován program Plantour, který počítá a optimalizuje trasy pro řidiče. Ukázalo se, že doba potřebná pro výpočty těchto tras je zhruba o třetinu delší, než doba potřebná pro výpočet na původním fyzickém serveru. Po konzultacích s výrobcem programu Plantour se ukázalo, že aplikace je pouze jednovláknová a nedokáže plně využít moderních vícejádrových procesorů použitých v nových serverech. Problém byl dále konzultován a v reálném čase předveden podpoře společnosti VMware. Vyjádření společnosti VMware bylo, že není možné změnou nastavení, či parametrů zvýšit výkon této aplikace a jako úzké hrdlo se zde ukázal nižší nominální takt procesorů v nových serverech oproti vyššímu taktu procesoru ve fyzickém serveru. Poměr byl 2GHz oproti 3GHz, což odpovídá třetině času navíc, kterou potřebuje k výpočtu virtuální server.

Další, tentokrát již fatální dopad na provoz měl problém, který se v prostředí PNS projevil a který měl následující průběh. Během noci na 11.9.2014 havaroval ESXi server CEVMW01 do PSOD (Purple Screen Of Death). Problém byl vyřešen ještě během noci. Problém se nádledně opakoval 11.9.2014 během dopoledne a způsobil výpadek dostupnosti VM, které na serveru běží po dobu, než byly automaticky spuštěny na serveru CEVMW02. Po pár minutách stejným způsobem havaroval také server CEVMW02. V té chvíli byly všechny VM nedostupné. Server CEVMW03 nemá přístup na sdílené úložiště a nebylo tedy možné VM spustit na něm. Po pár minutách se ukázalo, že problém

způsobila chyba na straně hypervisoru, kdy došlo při více souběžně spuštěných VM s operačním systémem Windows 2012 R2 Server s virtuální síťovou kartou E1000 k pádu do PSOD[28]. PSOD obrazovku ukazuje obrázek č. 54. V prostředí PNS opravdu vzrostl počet VM s operačním systémem Windows 2012 R2 Server, protože 10.9.2014 probíhal upgrade poštovních serverů právě na tento operační systém. Rychlá oprava problému spočívala v nahrazení virtuálního adaptéru E1000 za adaptér VMXNET3 u postižených VM. Problém byl ze strany společnosti VMware řešen aktualizací, která byla následně aplikována na všechny ESXi servery společnosti PNS.



Obrázek 54 - fatální selhání ESXi PSOD

Přínos virtuálního prostředí je pro společnost PNS bezesporu v možnostech flexibilního využití dostupných zdrojů a vysoké dostupnosti. Virtualizace se velice osvědčila např. při vytváření testovacích prostředí, kde se z výhodou používají snapshoty. Jako příklad může posloužit velice rychlá výroba testovacího serveru pro e-shop. Vytvoření serveru bylo otázkou několika minut. Jako vzor posloužila stávající VM, ze které byl vytvořen klon. Změnily se některé důležité parametry (hostname, IP adresa) a server byl připraven. Dalším přínosem virtualizace je možnost libovolně rozdělovat

[28] (VMware Inc., 2014N)

zdroje a poskytnout vysoký výkon vybraným VM v době, kdy jej opravdu potřebují. Zcela se změnil pohled na správu, který je centralizovaný a umožňuje všechny VM napříč celou společností spravovat z jednoho místa s jasně definovanými rolemi jednotlivých uživatelů. Společnost PNS se v prvním a druhém kvartále roku 2015 chystá nasadit nové servery v hostingovém centru Nagano a na pobočkách. Přechod na nové servery bude znamenat jen minimální dopady na dostupnost VM a nebude znamenat žádný zásah do jejich operačních systémů díky oddělení od fyzického hardware. Naproti tomu obměna fyzických serverů by byla značně komplikovanější a v mnoha případech by se neobešla bez nutnosti nové instalace operačního systému jednotlivých serverů.

5.2 Ekonomická zhodnocení

Ekonomické zhodnocení je možné a nejlépe vyčíslitelné na nákladech potřebných k pořízení hardware, podpory a licencí. Další možný pohled je na výdaje za elektrickou energii a chlazení.

5.2.1 Hardware a licence

Koncem roku 2007 společnost PNS obměnila všechny své servery za nové. Bylo pořízeno několik modelů, které jsou uvedeny v tabulce č. 1 v kapitole 4.1. Pořizovací cena všech těchto serverů byla přibližně 3 200 000 Kč bez DPH. V ceně je zahrnuta podpora společností Dell na 7 let NBD.

V roce 2013 byly nakoupeny severy a disková pole pro vybudování VMware prostředí na centrále PNS, seznam hardware je uveden v tabulkách 2, 3 a 4 v kapitole 4.3.1. Celková pořizovací cena včetně licencí na produkty VMware uvedených na obrázku č. 39 v kapitole 4.5.2 byla 1 277 300 Kč bez DPH včetně podpory 5 let NBD a 4Hr Mission Critical na diskové pole MD3220.

Vzhledem k ukončení podpory společnosti Dell na servery Dell PowerEdge 2950, které jsou nasazeny na virtualizaci v hostingovém centru Nagano a na všech pobočkách, bylo začátkem roku 2015 pořízeno devět nových serverů. Jejich pořizovací cena včetně podpory 5 let NBD je 635 000 Kč bez DPH.

Pokud sečteme celkové náklady na hardware a licence potřebné pro virtualizaci, dostaneme se na částku **1 912 300 Kč bez DPH** oproti částce **3 200 000 Kč bez DPH** za nevirtualizované prostředí, což je více než třetinová úspora. Faktem je, že po pěti letech bude potřeba nakoupit dodatečnou podporu na servery, protože se jejich životnost

předpokládá delší, než 5 let. To bude představovat další investici, jejíž výši v tuto chvíli nelze přesně odhadnout. Na druhou stranu ze zkušeností s provozem nevirtualizovaného prostředí víme, že je občas potřeba posílit parametry některých serverů, což také přináší další náklady. Naproti tomu jsou nové servery výkonostně naddimenzované, takže se nepředpokládá další investice do vylepšení jejich parametrů.

5.2.2 Porovnání spotřeby elektrické energie

Další nezanedbatelnou úsporu představuje snížení nákladů na elektrickou energii. Výpočet provedeme tak, že sečteme příkon fyzických serverů, které budeme virtualizovat a porovnáme s příkonem všech ESXi serverů, které hostují VM. Servery PowerEdge 1950 mají maximální příkon 670W, servery PowerEdge 2950 mají maximální příkon 750W, servery SC430 a SC440 mají maximální příkon 300W. Ve výpočtu budeme uvažovat maximální zatížení zdrojů v nonstop provozu. Celkový příkon všech serverů je 20 020W, cena za 1kWh je v průměru 4,75 Kč bez DPH, počet hodin odpovídající 365 dnům je 8 760. Po dosazení hodnot dostáváme výsledek.

Cena = 20.02 x 8 760 x 4.75 = 833 032 Kč bez DPH za rok, **69 419 Kč bez DPH za měsíc**.

Stejně vypočteme spotřebu elektrické energie u virtualizovaného prostředí. Uvažovat budeme všechny ESXi servery, tedy PowerEdge R720 s maximálním příkonem jednoho serveru 750W, disková pole MD3220 a MD1220 s maximálním příkonem 600W a servery PowerEdge 2950 v hostingovém centru Nagano a pobočkách s maximálním příkonem 750W. Cena za 1kWh a počet hodin zůstává stejný jako v předchozím výpočtu, celkový příkon je 9 450W.

Cena = 9.45 x 8 760 x 4.75 = 393 214 Kč bez DPH za rok, **32 768 Kč bez DPH za měsíc**.

Rozdíl v ročních nákladech na elektrickou energii činí **439 818 Kč bez DPH** ve prospěch virtualizace. Toto číslo je spíše ilustrativní, protože servery většinu času nepotřebují plný výkon. Pokud budeme uvažovat reálnější odhad průměrného vytížení zdrojů (50%), dostaneme částku 416 516 Kč bez DPH oproti 196 607 Kč bez DPH, tedy roční rozdíl přibližně **220 000 Kč bez DPH.**

5.2.3 Náklady na chlazení

S růstem počtu fyzických serverů roste nárok na jejich chlazení a s ním spojené náklady. Pokud porovnáme rozdíl v celkovém příkonu všech serverů s celkovým příkonem serverů virtualizovaného prostředí, získáme hodnotu 10 570W. To je hodnota elektrického příkonu, kterou musíme navíc uchladit v porovnání s virtualizovanou infrastrukturou. Obecně platí, že klimatizace na 1kW chladícího výkonu spotřebuje přibližně 1/3 elektrického příkonu, proto je nutné započítat i zvýšené nároky na chlazení u varianty fyzických serverů.

Cena = 1/3 x 10.57 x 8 760 x 4.75 = 146 605 Kč bez DPH za rok, **12 217 Kč bez DPH za měsíc**.

5.2.4 Doporučení

I přes určitá rizika, která virtualizace přináší se jedná o velice silný nástroj, jehož správné nasazení a používání při dodržování určitých pravidel vede k lepší efektivitě správy celé infrastruktury, vysoké dostupnosti a škálovatelnosti. Jak vyplývá z ekonomického zhodnocení, je virtualizace vhodný nástroj na snižování nákladů. Doporučení jsou v tomto trendu pokračovat a vše co je možné, přenést do virtualizovaného prostředí.

Jistá rizika představuje právě virtualizační vrstva. Je proto nezbytné sledovat zranitelnosti, zjištěné problémy, doporučení a adekvátně na ně reagovat. Zároveň je potřeba brát v úvahu fakt, že ne všechny fyzické servery jsou vhodné pro virtualizaci, popř. je virtualizace možná za určitých podmínek. Důležitou roli hraje správné a účinné nastavení monitoringu celého prostředí. Monitoring by měl pokrývat jednotlivé části prostředí jako jsou hardware, kde je virtualizace provozována, optimální využití zdrojů a sledování VM. Na základě podkladů z monitorovacích systémů následně přijímat vhodná opatření.

Ke správě virtualizovaného prostředí dává společnost VMware k dispozici dva nástroje. První a starší je vSphere Client. Osobně se mi s tímto nástrojem pracuje lépe, než s novějším nástrojem vSphere Web Client. Ten má ovšem oproti staršímu nástroji několik výhod. Není potřeba instalace žádného těžkého klienta na koncovou stanici, ze které prostředí spravujeme. Je spustitelný v jakémkoliv novějším internetovém prohlížeči. Lze pomocí něj konfigurovat kompletně celé prostředí včetně např. řízení replikací apod. To

starším klientem možné není. Je vhodné začít používat nového klienta, protože je pouze otázkou času, kdy společnost VMware podporu staršího klienta ukončí.

6 Závěr

Stanovené cíle byly splněny. Teoretická část práce obsahuje úvod a seznámení s pojmem virtualizace, stručně mapuje její historii a jsou v ní představeny základní vlastnosti. Zaměřena je na serverovou virtualizaci s využitím produktů společnosti VMware. Představeny jsou jednotlivé oblasti, do kterých virtualizace zasahuje. Jedná se o datová úložiště, souborové systémy, oblast sítí a oblast bezpečnosti. Další část diplomové práce představuje produkty a nástroje společnosti VMware. Představen je vSphere ESXi, vCenter Server, vCenter Operations Manager, Update Manager, vSphere Storage Appliance, vSphere Data Protection a vSphere Convertor.

Praktická část práce je zaměřena na nasazení virtualizace v podnikovém prostředí společnosti První novinová společnost a.s. (PNS). Je provedena analýza stávajícího prostředí a posouzena vhodnost virtualizace jednotlivých serverů. Na základě analýzy je navržena nová serverová infrastruktura na centrále PNS, hostingovém centru Nagano a sedmi pobočkách. Detailně je předvedena instalace, základní a pokročilá konfigurace jednoho ESXi serveru a jeho začlenění do podnikové sítě. Předvedena je rovněž instalace produktu vCenter Server od instalace operačního systému až po jednotlivé softwarové komponenty vCenter Serveru. Předveden je také použitý licenční model produktů společnosti VMware. Dále je na úrovni vCenter Serveru vytvořena logická struktura objektů a vysvětlena jejich konfigurace. V prostředí vCenter Serveru je ukázán systém správy aktualizací produktem Update Manager. V dalších kapitolách je vysvětlen P2V proces migrace stávajících fyzických serverů do nového prostředí za využití nástroje vCenter Converter Standalone Client. Kapitola věnovaná monitoringu a správě prostředí je zaměřena na představení způsobů a nástrojů, které je možné použít a které jsou reálně nasazeny v prostředí PNS.

Na základě praktické části lze formulovat výsledky a doporučení. Nasazení technologie virtualizace v prostředí společnosti PNS vedlo ke zefektivnění a zlepšení ICT služeb. Snížily se náklady v podobě nákupu potřebného hardware, podpory a licencí na částku 1 912 300 Kč bez DPH oproti částce 3 200 000 Kč bez DPH, kterou stála obměna fyzických serverů koncem roku 2007. Roční úspory přibližně 220 000 Kč bez DPH bylo dosaženo na spotřebě elektrické energie ve prospěch virtualizovaného prostředí a roční úspory za chlazení dosáhly přibližně 146 605 Kč bez DPH.

7 Seznam použitých zdrojů

Bartolšic, Martin. 2013. Trendy v ukládání – Organizace jsou závislé na datech. *Computerworld.cz.* [Online] 16. 02 2013. [Citace: 06. 08 2014.] http://computerworld.cz/technologie/trendy-v-ukladani-organizace-jsou-zavisle-na-datech-49476.

Gleed, Kyle. 2011. What's in a VIB? | VMware vSphere Blog - VMware Blogs. *VMware vSphere Blog | Begin the journey to a private cloud with datacenter virtualization - VMware Blogs.* [Online] 13. 09 2011. [Citace: 19. 02 2015.] http://blogs.vmware.com/vsphere/2011/09/whats-in-a-vib.html.

Horák, Pavel. 2014. VMsafe: Bezpečnostní technologie pro virtuální prostředí. *VMware newsletter.* [Online] 2014. [Citace: 06. 08 2014.] http://www.vmwarenews.cz/vmw/vmwnews.nsf/0/B06EE0D07E6177C1C12576F8004E9425.

Kabelová, Alena a Dostálek, Libor. 2008. *Velký průvodce protokoly TCP/IP a systémem DNS.* Brno : Computer Press, 2008. str. 488. ISBN 978-80-251-2236-5.

King, Justin. 2014. Which vCenter Server platform should I use - Appliance or Windows? | VMware vSphere Blog - VMware Blogs. *VMware Blog.* [Online] 11. 06 2014. [Citace: 22. 02 2015.] http://blogs.vmware.com/vsphere/2014/06/vcapplianceorwindows.html.

Matyska, Luděk. 2011. Techniky virtualizace počítačů (2). *ÚVT MU zpravodaj.* [Online] 14. 11 2011. [Citace: 02. 08 2014.] http://ics.muni.cz/bulletin/articles/545.html.

Microsoft Corporation. 2012. Zásady společnosti Microsoft pro duplikaci disku, instalace systému Windows. *Microsoft Česká republika.* [Online] 21. 11 2012. [Citace: 02. 08 2014.] http://support.microsoft.com/kb/314828/cs.

Peterka, Jiří. 2011. Hypervisor. *earchiv.cz.* [Online] 2011. [Citace: 02. 08 2014.] http://www.earchiv.cz/l226/slide.php3?l=11&me=22.

Prodělal, Jaroslav. 2014. Clusterový filesystém. *OldanyGroup.* [Online] 2014. [Citace: 02. 08 2014.] http://www.oldanygroup.cz/index-stranek-115/clusterovy-filesystem/.

Prodělal, Jaroslav. 2014. Co je to virtualizace? *OldanyGroup.* [Online] 2014. [Citace: 02. 08 2014.] http://www.oldanygroup.cz/virtualizace-vmware-zakladni-informace-9/.

Prodělal, Jaroslav. 2010. Přednáška V3C - Historie virtualizace (část 4.). *Youtube.* [Online] 04. 01 2010. [Citace: 02. 08 2014.] https://www.youtube.com/watch?v=11iN_YYTlkY.

Ruest, Danielle a Ruest, Nelson. 2010. *Virtualizace: podrobný průvodce.* Vyd. 1. Brno : Computer Press, 2010. str. 408. ISBN 978-80-251-2676-9.

Skohoutilová, Martina. 2011. Lepší dříve, nežli později. *Inflow.* [Online] 07. 11 2011. [Citace: 02. 08 2014.] http://www.inflow.cz/lepsi-drive-nezli-pozdeji.

VAHAL s.r.o. 2009. Ukládání dat - přímo připojená úložiště. *Vahal s.r.o. - hardware a software.* [Online] 2009. [Citace: 02. 08 2014.] http://www.vahal.cz/cz/podpora/technicke-okenko/ukladani-dat-das.html.

VCRITICAL. 2009. VM Encapsulation. *VCritical.* [Online] 17. 02 2009. [Citace: 02. 08 2014.] http://www.vcritical.com/2009/02/vm-encapsulation/.

VMware Inc. 2014K. Compare VMware vSphere Editions and Kits Comparison | United States. *VMware Virtualization for Desktop & Server, Application, Public & Hybrid Clouds | United States.* [Online] 2014K. [Citace: 24. 02 2015.] http://www.vmware.com/products/vsphere/compare.html.

VMware Inc. 2014I. Configure SNMP for ESXi. *vSphere Documentation Center.* [Online] 23. 09 2014I. [Citace: 19. 02 2015.] https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.monitoring.doc_50%2FGUID-8EF36D7D-59B6-4C74-B1AA-4A9D18AB6250.html.

VMware Inc. 2014C. vCenter Server Virtualization Management Software Features | VMware. *VMware Virtualization for Desktop & Server, Application, Public & Hybrid Clouds.* [Online] 2014C. [Citace: 07. 08 2014.] http://www.vmware.com/cz/products/vcenter-server/features.html.

VMware Inc. 2012. vmfs-best-practices-wp. *vSphere Distributed Switch, Virtual Machine Networking: VMware | United States.* [Online] 2012. [Citace: 06. 08 2014.] http://www.vmware.com/files/pdf/vmfs-best-practices-wp.pdf.

VMware Inc. 2014J. VMware KB: Methods for installing vCenter Server 5.5. *VMware Virtualization for Desktop & Server, Application, Public & Hybrid Clouds.* [Online] 11. 03 2014J. [Citace: 22. 02 2015.] http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2053142.

VMware Inc. 2014N. VMware KB: VMware ESXi 5.x host experiences a purple diagnostic screen mentioning E1000PollRxRing and E1000DevRx. *VMware Virtualization for Desktop & Server, Application, Public & Hybrid Clouds.* [Online] 29. 01 2014N. [Citace: 25. 02 2015.] http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2059053.

VMware Inc. 2014H. VMware vCenter Converter: P2V Virtual Machine Converter | United States. *VMware Virtualization for Desktop & Server, Application, Public & Hybrid Clouds.* [Online] 2014H. [Citace: 07. 08 2014.] http://www.vmware.com/products/converter/.

VMware Inc. 2014D. VMware vCenter Operations Manager Documentation. *VMware Virtualization for Desktop & Server, Application, Public & Hybrid Clouds.* [Online] 2014D. [Citace: 07. 08 2014.] https://www.vmware.com/support/pubs/vcops-pubs.html.

VMware Inc. 2014F. VMware vSphere Storage Appliance (VSA) for Shared Storage. *VMware Virtualization for Desktop & Server, Application, Public & Hybrid Clouds.* [Online] 2014F. [Citace: 07. 08 2014.] http://www.vmware.com/cz/products/vsphere-storage-appliance.html.

VMware Inc. VMware vSphere Storage Appliance (VSA) for Shared Storage | VMware | Česká republika. [Online] [Citace: 24. 02 2015.] http://www.vmware.com/cz/products/vsphere-storage-appliance.

VMware Inc. 2014E. VMware vSphere Update Manager: Compliance & Configuration Management. *VMware Virtualization for Desktop & Server, Application, Public & Hybrid Clouds.* [Online] 2014E. [Citace: 07. 08 2014.] http://www.vmware.com/cz/products/vsphere/features/update-manager.

VMware Inc. 2014G. vSphere Data Protection Advanced: Backup & Recovery in vSphere Environments | United States. *VMware Virtualization for Desktop & Server, Application, Public & Hybrid Clouds.* [Online] 2014G. [Citace: 07. 08 2014.] http://www.vmware.com/products/vsphere-data-protection-advanced.

VMware Inc. 2014A. vSphere Distributed Switch, Virtual Machine Networking: VMware | United States. *VMware Virtualization for Desktop & Server, Application, Public & Hybrid Clouds.* [Online] 2014A. [Citace: 06. 08 2014.] http://www.vmware.com/products/vsphere/features/distributed-switch.html.

VMware Inc. 2014B. vSphere ESXi Bare-Metal Hypervisor: VMware | VMware. *VMware Virtualization for Desktop & Server, Application, Public & Hybrid Clouds.* [Online] 2014B. [Citace: 07. 08 2014.] http://www.vmware.com/cz/products/vsphere/features/esxi-hypervisor.html.

VMware® Education Services. 2011. *VMware vSphere: Install, Configure, Manage Student Manual - ESXi 5.0 and vCenter Server 5.0.* Revision A. England : VMware, Inc., 2011. str. 651. EDU-ENG-ICM5-LEC1-STU a EDU-ENG-ICM5-LEC2-STU.

8 Seznam použitých zkratek

AD	Active Directory
AFP	Apple Filing Protocol
API	Application Programming Interface
BSD	Berkeley Software Distribution
CA	Certificate Authority
CD	Compact Disc
CDP	Cisco Discovery Protocol
CIFS	Common Internet File System
CLI	Command Line Interface
CMS	Content Management System
CPU	Central Processing Unit
CSV	Cluster Shared Filesystem
CUCM	Cisco Unified Communications Manager
DAS	Direct Attached Storage
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DPH	Daň z přidané hodnoty
DRAC	Dell Remote Access Controller
DRS	Distributed Resource Scheduler
EXT2	Second Extended Filesystem
EXT3	Third Extended Filesystem
FAT	File Allocation Table
GB	Gigabyte
Gbps	Gigabits Per Second
GFS	Global File System
GPFS	General Parallel File System
HA	High Availability
HW	Hardware
IAS	Internet Authentication Service
IBM	International Business Machines

ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
iDRAC	Integrated Dell Remote Access Controller
IEEE	Institute of Electrical and Electronics Engineers
IOPS	Input/Output Operations Per Second
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPv6	Internet Protocol version 6
iSCSI	Internet Small Computer System Interface
IT	Informační technologie
KC	Kontaktní Centrum
KVM	Kernel Virtual Machine
L2	Layer 2
LAN	Local Area Network
LUN	Logical Unit Number
MB	Megabyte
Mbps	Megabits Per Second
MS	Microsoft
MSI	Microsoft Installer
NAS	Network Attached Storage
NBD	Next Business Day
NFS	Network File System
NIC	Network Interface Card
NTFS	New Technology File System
NTP	Network Time Protocol
OID	Object identifier
OS	Operační Systém
OVF	Open Virtualization Format
P2V	Physical-to-Virtual
PC	Personal Computer
PDF	Portable Document Format
PERC	PowerEdge RAID Controller

PRTG	Paessler Router Traffic Grapher
PSOD	Purple Screen Of Death
RAID	Redundant Array of Inexpensive/Independent Disks
RAM	Random Access Memory
RDM	Raw Device Mapping
RJ45	Registered Jack-45
SAN	Storage Area Network
SAP	Systems Applications Products
SCSI	Small Computer System Interface
SEP	Symantec Endpoint Protection
SFP	Small form-factor pluggable
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPOF	Single Point Of Failure
SQL	Structured Query Language
SSH	Secure Shell
SW	Software
TB	Terabyte
TCP/IP	Transmission Control Protocol/Internet Protocol
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VIB	vSphere Installation Bundle
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMDK	Virtual Machine Disk
VMFS	Virtual Machine File System
VMM	Virtual Machine Monitor
VPN	Virtual Private Network
VSA	vSphere Storage Appliance
WAN	Wide Area Network

9 Seznam obrázků

10 Seznam tabulek