# Vysoká škola ekonomická v Praze

**Fakulta informatiky a statistiky**

**Katedra informačních technologií**



| | |
|---|---|
| Student | : **Ondřej Salák** |
| Vedoucí bakalářské práce | : **Ing. Luboš Pavlíček** |
| Oponent bakalářské práce | : **Ing. Kateřina Martanová** |


**TÉMA BAKALÁŘSKÉ PRÁCE**

# BUSINESS CONTINUITY MANAGEMENT A VIRTUÁLNÍ STROJE

**ROK : 2010**

## Prohlášení

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

V Praze dne 10.04.2010 ..... .....

podpis

# Poděkování

Na tomto místě bych rád poděkoval panu Ing. Luboši Pavlíčkovi za vedení bakalářské práce, paní PhDr. Daně Salákové za pomoc při korektuře, panu Ing. Jaromíru Žákovi za výpomoc praktickou a společnosti TOTAL SERVIS s.r.o. v čele s panem ředitelem Václavem Novákem za poskytnutí hardware pro praktickou část.

# Abstrakt

Cílem této práce je poskytnout základní přehled možností, jak podpořit podnikové řízení kontinuity činností s využitím virtualizace. Čtenář je na začátku stručně seznámen s pojmem Business continuity management (řízení kontinuity činností) a pojmem virtualizace. Poté je rozebrán vztah těchto dvou oblastí, v čem se doplňují a naopak. Nakonec jsou podrobně rozebrány pomocné programy a moduly pro podporu BCM, které jsou obsaženy v komerčním produktu vSphere od společnosti VMware. Cílem praktické části je pak prověřit funkčnost některých z těchto nástrojů.

# Abstract

The aim of this work is to provide a basic overview of ways to improve business continuity management and planning using virtualization. First, the reader is briefly introduced to the concept of Business continuity management and the concept of virtualization. Then the relationship between these two areas is analyzed. Finally, I chose to analyze a set of utilities, which come with VMware vSphere product, which is the product of VMware Company. The aim of the practical part is to verify the functionality of some of these tools.

# Obsah

Úvod ... 8
1 Business Continuity Management ... 9
1.1 Pojem BCM ... 9
1.2 Světové standardy, které se týkají BCM ... 9
1.3 Popis technik ... 10
1.3.1 Zpracování informací o firmě ... 11
1.3.2 Plánování kontinuity a obnovy ... 12
1.3.3 Implementace ... 12
1.3.4 Fáze testovací a udržovací ... 12
1.4 Přínosy ... 13
2 Základy virtualizace ... 13
2.1 Pojem virtualizace ... 13
2.2 Schéma funkce virtualizace ... 15
2.3 Virtuální stroj, virtuální obraz ... 15
2.4 Druhy virtualizace ... 16
2.4.1 Aplikační virtualizace ... 16
2.4.2 Virtualizace na úrovni operačního systému ... 17
2.4.3 Paravirtualizace ... 17
2.4.4 Emulace ... 17
2.4.5 Plná virtualizace ... 18
3 BCM ve virtualizovaném prostředí ... 18
3.1 Oblast dostupnosti ... 19
3.2 Oblast obnovy dostupnosti služeb ... 20
4 Nástroje podporující BCM od společnosti VMware ... 21
4.1 Clustering ... 21
4.1.1 Funkce ... 21
4.1.2 Přínos ... 22
4.2 VMware vMotion ... 22
4.2.1 Funkce ... 22
4.2.2 Použití a přínos ... 23
4.2.3 Podmínky pro správnou funkčnost vMotion ... 23
4.3 VMware High Availability ... 24
4.3.1 Funkce ... 24
4.3.2 Přínos ... 25
4.3.3 Klíčové vlastnosti ... 25
4.4 VMware DRS ... 26
4.4.1 Funkce ... 26
4.4.2 VMware DPM ... 27
4.4.3 Přínosy ... 28
4.5 VMware Data Recovery ... 28
4.5.1 Funkce ... 28

4.5.2 Přínos ... 30
5 Praktická část ... 30
5.1 Testovací prostředí ... 31
5.1.1 Hardware ... 31
5.1.2 Software ... 31
5.1.3 Virtuální stroje ... 32
5.1.4 Schéma ... 34
5.2 Vytvoření clusteru ... 34
5.3 Nastavení VMware High Availability ... 35
5.4 Nastavení VMware DRS ... 36
5.5 Nastavení funkce vMotion ... 37
5.6 Migrace virtuálního stroje ... 39
5.7 Simulace výpadku ESX serveru ... 40
Závěr ... 42
Seznam použité literatury ... 43
Seznam obrázků ... 44

# Úvod

Oba dva pojmy obsažené v názvu práce, tedy business continuity management a virtualizace, jsou v současné době velice diskutovanými tématy. Ve stále více a více podnicích a společnostech dochází k nasazení business continuity plánování, ať už končí úspěšně, či ne. Stejně tak oblast virtualizace stále zaznamenává boom ve svém vývoji i ve svém rozšíření. Rád bych se na svět virtualizace podíval právě z pohledu business continuity managementu. I když se to na první pohled nemusí zdát, tak to, jestli firma ve své síti využívá virtualizace nebo ne, má na business continuity management v oblasti ICT (informační a komunikační technika) velký a zásadní vliv.

# 1 Business Continuity Management

## *1.1 Pojem BCM*

Pojem Business Continuity Management bývá většinou do českého jazyka překládán jako Řízení kontinuity činností organizace. V angličtině pro něj pak existuje ještě jedno synonymum, kterým je Business Continuity Planning. Tato technika řízení vychází z jednoho prostého faktu. Pokud se stane jakýkoliv incident, například dojde k výpadku významného serveru, společnost se stane terčem útoku nebo například dojde k zatopení kancelářských prostor společnosti včetně serverovny, je vždy v našem zájmu, abychom dali systém co nejdříve do alespoň provizorního stavu, který ale bude schopen podporovat a umožňovat běh firemních procesů. Z předešlého vyplývá, že se vyplatí vynaložit jisté prostředky, případné možné incidenty předvídat a mít již dopředu připraveny jakési scénáře pro co nejefektivnější vypořádání se s jednotlivými problémy. [1]

„Mezi nejčastější příčiny přerušení kontinuity činností organizace patří technická selhání (výpadek dodávek energie, selhání technického nebo programového vybavení), přírodní živly (požár, povodeň), lidský faktor (hrozby úmyslné i neúmyslné - chyby uživatelů, podvody, krádeže, napadení IS) apod. Řízení kontinuity činností je proces, který připraví organizaci na řešení těchto nepředvídatelných situací a zmírní jejich případné následky.“ [3]

## *1.2 Světové standardy, které se týkají BCM*

Prvním dílem, ve kterém se objevují techniky řízení, podobné řízení kontinuity činností, je Umění války (The Art of War) od čínského vojevůdce Sun-c′. Až do sedmdesátých let dvacátého století zůstala problematika kontinuity činností pouze na poli vojenském. Za rok vzniku BCM se považuje rok 1973. V tomto roce se poprvé metoda kontinuity řízení činností objevila na poli byznysu. V sedmdesátých a osmdesátých letech se tyto techniky řízení nijak výrazně nevyvíjely, co se kvality týče, ale stoupal počet společností, které je využívaly. Největší zájem o zavedení řízení kontinuity činností nastal v druhé polovině devadesátých let z důvodu šířící se paniky z toho, co udělá rok 2000 se světem výpočetní techniky (tzv. Y2K).

Na počátku nového tisíciletí dochází ke vzniku Business Continuity Institute, společnosti, která se zabývá BCM do hloubky. Tento institut vydal vůbec první oficiální doporučení pro BCM. V roce 2006 ho následoval Britský normalizační institut (British Standard Institution - BSI), který vydal dosud nejlepší souhrnný popis problematiky řízení kontinuity činností – BS 25999. Tento standard má dvě části. Část BS 25999-1:2006 ukazuje soubor postupů, návodů a doporučení, jak realizovat jednotlivá opatření související s kontinuitou řízení. Tyto postupy jsou doporučené, ne však závazné. Seznam závazných požadavků pro tuto metodiku najdeme v části druhé BS 25999-2:2007, kterou BSI vydal o rok později. Česká Republika přejala obě tyto normy pod názvy ČSN BS 25999-1 a ČSN BS 25999-2.

Nezávisle na britském normalizačním institutu vydala Mezinárodní organizace pro normalizaci (International Standard Organization – ISO) svoje standardy ISO/IEC 27001 a ISO/IEC 27002, zabývající se řízením bezpečnosti informací. V obou těchto standardech se dotýká problematiky řízení kontinuity činností. Dalším standardem vydaným touto organizací, který se zabývá BCM přímo, je ISO/IEC 22399:2007. V budoucnu by také měl vyjít standard ISO/IEC 27031, zabývající se problematikou řízení kontinuity činností v oblasti informačních a komunikačních technologií. [4]

## *1.3 Popis technik*

Všechny plány řízení kontinuity činností popisují povinnosti zaměstnanců, protože lidské zdroje jsou nejdůležitější oblastí podnikání, bez které by jiné obnovovací procesy byly zbytečné. Plány popisují komunikaci mezi zaměstnanci, jejich případnou evakuaci, přestěhování a celkově způsob zajištění pokračování v jejich práci. Detaily se liší u každého subjektu, protože vždy záleží na velikosti firmy, typu hrozby a v neposlední řadě také na oblastech podniku, které incident ochromí. Pro každou společnost je důležitá jiná oblast. Pro některé je to například proces zásobování, pro některé je to informační systém atd. Velice podstatným bodem je fakt, že dobrá politika řízení kontinuity činností nemůže zahrnovat jen oblast lidských zdrojů nebo jen oblast informačních technologií, ale musí obsahovat všechny oblasti podniku, kterých se problém týká. Jednou z hlavních podmínek pro úspěšnou implementaci řízení kontinuity činností je neustálá a kvalitní komunikace mezi jednotlivými zodpovědnými osobami. Ne náhodou je proto rovina komunikace osob vždy jednou z prvních, které plán

kontinuity činností řeší. Například v případě incidentu v podobě přírodní katastrofy ve větším měřítku (záplavy, hurikán) mohou být zaměstnanci postiženi i v soukromém životě na vlastním majetku a pak v případě nouze jen těžko dají přednost řešení problémů v zaměstnání. Díky zajištěné komunikaci lze tyto výpadky operativně řešit. [5]

Celý životní cyklus této metodiky lze rozdělit na 4 základní fáze. Jedná se o fázi analýzy, fázi tvorby plánů, fázi testovací a fázi implementační.




Obr. 1 - Životní cyklus BCM (Embedding BCM in the Organisation's Culture) – uprostřed je centrální vedení řízení kontinuity činností ve společnosti (Business Continuity Programme Management). Odshora směrem doprava následují jednotlivé fáze – fáze Poznávání společnosti (Understanding the Organization), fáze Plánování kontinuity a obnovy (Determining BCM strategy), fáze Implementace technik (Developing & Implementing BCM Response) a fáze Testovací a udržovací (Exercising, Maintaining & Reviewing).[Obr. 1]

### 1.3.1 Zpracování informací o firmě

Tato fáze by se také dala nazvat jako analytická. Nejdříve dochází k ustanovení celého Business Continuity Management procesu. Jedná se o obecné definování celého

projektu, stanovení jeho cílů, osob zodpovědných za jednotlivé fáze a vytvoření základní dokumentace. Po prvotním impulzu následuje analýza hrozeb. Výsledkem této analýzy je vyčerpávající seznam hrozeb, které mohou nastat. Tento seznam se dále zpracovává v analýze rizik zkoumající, která z hrozeb může ohrozit chod společnosti a která ne. Jako poslední se provádí analýza dopadu, v níž dochází k početnímu vyjádření dopadů jednotlivých hrozeb s různými riziky. Tyto údaje se roztřídí podle důležitosti a kritičnosti.

### 1.3.2 Plánování kontinuity a obnovy

V této fázi se již pracuje pouze s riziky, která byla vyhodnocena jako důležitá a která je třeba zohlednit v plánu kontinuity činností. U každého rizika se projdou jeho dopady a připraví se specifický plán zvládání rizika. Tento plán obsahuje součásti, které jsem popsal již v odstavci 2.4. Nezabývá se ovšem jen krátkodobou obnovou procesů, ale zabývá se i pohledem dlouhodobým, na jehož konci je v ideálním případě stav, který byl před vypuknutím incidentu.

### 1.3.3 Implementace

V této fázi dochází k oficiálnímu přijetí Business Continuity Managementu v daném podniku. Celá hlavní politika a jednotlivé plány jsou vydány ve formě vyhlášek zaměstnancům a dále můžou následovat různá školení apod. Tato fáze je pro zdárný úspěch asi nejkritičtější. Ke správnému a užitečnému implementování metodiky je totiž třeba splnit několik podmínek. Musí existovat vůle zaměstnanců se podle politiky chovat. Politika musí mít značnou podporu vedení a vedoucím řízení kontinuity činností musí být uvědomělá a zodpovědná osoba.

### 1.3.4 Fáze testovací a udržovací

Hotové a implementované plány kontinuity činností je třeba řádně otestovat. Samozřejmě, že ne všechny incidenty lze bezpečně a věrně simulovat. Výpadek serveru lze nasimulovat jednoduše jeho odstavením, ale případ přírodní katastrofy lze nasimulovat pouze obrazně. V pravidelných intervalech se musí politika kontinuity činností revidovat z důvodu měnících se hrozeb a jejich dopadů na společnost. Je také dobré provádět v rozumně zvolených časových intervalech průběžné kontrolní testy firemního povědomí o existenci politiky kontinuity činností a jejího plnění. Na výsledky

těchto testů je nutné rychle a správně reagovat pozměňováním a upravováním politiky. Podle výsledku testu jsou plány buďto ponechány v současném stavu, anebo je nutné je upravit a optimalizovat.

## *1.4 Přínosy*

Přínosů zavedení řízení kontinuity činností je mnoho. Jako příklad uvedu následující:

- Ochrana dobrého jména organizace.
- Zajištění hlavní podnikatelské činnosti - co nejrychlejší a odpovídající plnění závazků vůči zákazníkům.
- Snížení (finančních) ztrát v případě přerušení kontinuity činností.
- Prověření možných scénářů havárií.
- Zajištění kontinuity kritických byznys procesů.
- Přehledné, strukturované a na sebe navazující plány/postupy činností pro mimořádné události.
- Snížení délky výpadku a nedostupnosti ICT na minimum.
- informovanost všech zaměstnanců o jejich povinnostech a odpovědnostech při haváriích, živelných katastrofách a řešení bezpečnostních incidentů.

[6]

# 2 Základy virtualizace

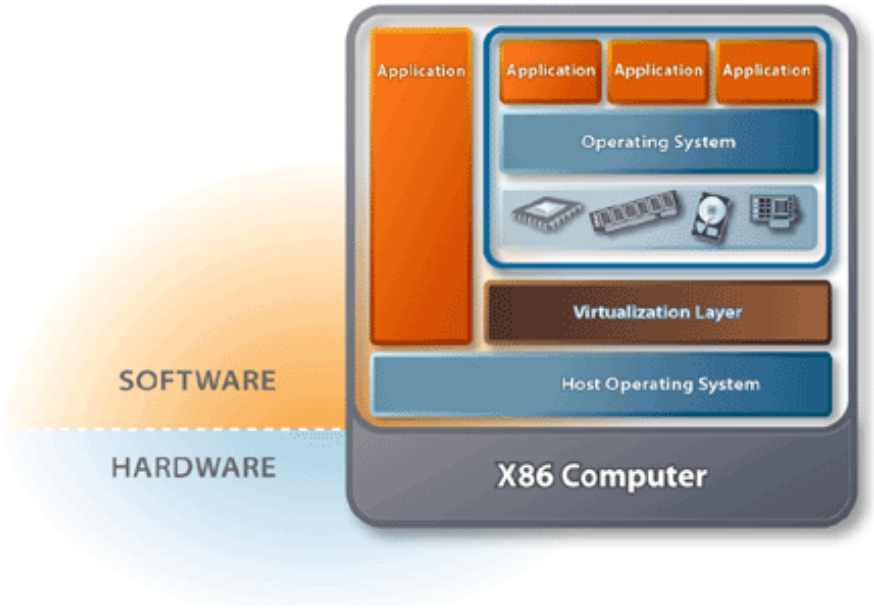
## *2.1 Pojem virtualizace*

Termín virtualizace se stal v současné době velice používaným pojmem v oblasti informačních technologií. Z posledních případových studií dokonce vyplývá potvrzení dřívější domněnky, že by měla být virtualizace použita v případě každé IT infrastruktury (všechny komponenty sítě, včetně počítačů a dalších hardwarových

prvků, které jako celek poskytují prostředí pro poskytování ICT služeb a běh informačních systémů). [7]

Různých definic pojmu virtualizace je mnoho. První možností, jak pojem definovat, může být například: „oddělení software od hardware“ [8]. To můžeme chápat jako takové uspořádání, ve kterém je možné k systémovým prostředkům přistupovat jako k jednomu zdroji se společným výkonem, bez ohledu na fyzické charakteristiky jednotlivých částí. Cílem virtualizace je pak zcela oddělit technické detaily systému, „schovat“ je pod virtualizační vrstvu, prostřednictvím které je pak prezentován jen jeho výpočetní výkon. Jiným vysvětlením pojmu virtualizace může být také soubor technik a postupů, které nám umožňují přistupovat k dostupným zdrojům odlišným způsobem, než jak fyzicky existují. V praxi to zjednodušeně vypadá tak, že nám virtualizační nástroj dokáže vytvořit takové virtuální hardwarové prostředí, ve kterém mohou běžet operační systémy zcela nezávisle na případném operačním systému hostujícím. Hardware, který „vidí“ operační systém virtuálního hardwaru, může být i zcela odlišný od fyzického hardwaru, na kterém virtuální stroj běží.

Veškeré operace s takovýmto virtuálním hardwarem jsou stejné jako operace s klasickým fyzickým hardwarem. Od instalace operačního systému, přes instalaci aplikací, až po jejich používání. Fyzickou podobou takového virtuálního hardwaru je pak na hostujícím fyzickém hardwaru jeden či více souborů, představujících samotný virtuální stroj, virtuální disk, či další nastavení a přizpůsobení. Tyto soubory lze samozřejmě volně přenášet mezi hosty se stejným virtualizačním prostředím a díky několika transformačním nástrojům někdy i mezi hosty s různými virtualizačními prostředími.




Obr. 2 – Názorná schematická ukázka virtualizace (překlad viz odstavec 2.2) [Obr. 2]

## 2.2 Schéma funkce virtualizace

Zjednodušeně lze funkci virtualizace vidět na obr. 2, který ukazuje schéma virtualizace. Velký tmavý obdélník představuje fyzický hardware. Na tomto hardwaru běží operační systém a v něm několik aplikací (modrý obdélník Host Operating Systém a na něm běžící Application). Jednou z těchto souběžně běžících aplikací je i aplikace umožňující virtualizaci (virtualization layer). Ta vytváří virtuální hardware (na obrázku prezentovaný modrým rámečkem s obrázky komponent), na kterém je nainstalován operační systém, pod nímž běží aplikace. [2]

## 2.3 Virtuální stroj, virtuální obraz

Právě pro už několikrát zmiňovaný virtuální hardware se používá také jiný pojem, a to virtuální stroj. Virtuální stroj se snaží v maximální možné míře simulovat prostředky fyzického stroje. K tomu využívá například emulaci jednotlivých komponent - disků, mechanik, přídavných zařízení. Jak jsem již nastínil výše, je virtuální stroj ukládán ve formě několika souborů. Tyto soubory se jako celek nazývají virtuální obraz. Tento obraz se může pomocí virtualizačního programu otevřít, lze v něm pracovat a při jeho zavření uložit změny, které po dobu otevření proběhly. S virtuálními obrazy lze provádět různé operace. Zejména se jedná o:

1. Práce se snapshoty – shapshot je přesným obrazem daného virtuálního stroje v jednu přesně danou chvíli. Systém si takto vytvořené snapshoty zpětně uchovává, aby nebyl v budoucnu problém se ke kterémukoliv z nich vrátit.
2. Klonování – v tomto případě je vytvořena identická kopie jednoho virtuálního obrazu. Tato tvorba se ještě může dít na dvou různých úrovních. Buď dojde k úplnému vytvoření kopie a alokování všech zdrojů, nebo dojde k vytvoření speciálního klonu, který je připojen ke své šabloně – v tomto případě se zaznamenávají hlavně změny, které v připojeném klonu proběhly oproti původnímu obrazu.
3. Přenositelnost obrazů – jak jsem již dříve uvedl, virtuální obrazy jsou přenositelné z jednoho hostitelského hardwaru na jiný. V případě stejné platformy to není nijak komplikovaný proces, v případě různých platforem se musí řešit pomocí speciálních konvertorů.

[9]

## *2.4 Druhy virtualizace*

Vlastní proces virtualizace může probíhat na různých úrovních. Každá z těchto úrovní má své výhody i nevýhody a je vhodná pro použití v jiném konkrétním případě. [http://cs.wikipedia.org/wiki/Virtualizace]

### 2.4.1 Aplikační virtualizace

Aplikační virtualizaci můžeme považovat za nejjednodušší druh virtualizace. V případě aplikační virtualizace nedochází k vytvoření celého virtuálního stroje, ale jen redukovaného virtuálního prostředí, kde jsou k dispozici všechny důležité prostředky pro funkčnost daných aplikací. Jedná se zejména o různé specifické prvky uživatelského rozhraní, registry, knihovny různých prvků nebo speciální ovladače. Tato metoda spouštění aplikací má mnoho nesporných výhod. První z nich je ta, že aplikace využívající stejné systémové soubory mohou na jednom PC běžet bez problémů současně, protože virtualizační nástroj vytvoří každé jejich vlastní kopii těchto souborů. Další nespornou výhodou je, že aplikace spouštěná ve virtuálním prostředí je zcela nezávislá na hostujícím operačním systému i hardwaru – tudíž nám stačí kompatibilita tohoto prostředí pouze s virtualizačním prostředím, ve kterém aplikaci spouštíme. Z obou těchto příkladů vyplývají další výhody – snížení nákladů na správu aplikací,

urychlení nasazení nových aplikací a v mnoha případech i rychlejší běh aplikací. Nově vytvořené aplikace nemusíme testovat pro chod na stovkách různých platforem a konfigurací. Stačí, když je optimalizujeme pro dané virtualizační prostředí, a víme, že na požadovaných konfiguracích je toto prostředí podporováno. Klasickým příkladem aplikační virtualizace je Java Virtual Machine – prostředí pro běh programů v jazyku Java. [2]

### 2.4.2 Virtualizace na úrovni operačního systému

Metoda virtualizace na úrovni operačního systému probíhá na úrovni jeho jádra. Spolu s paravirtualizací patří k nejefektivnějším druhům virtualizace. Jednoduše řečeno, jde o sdílení jednoho jádra více identickými operačními systémy. Izolace mezi jednotlivými virtuálními stroji je v tomto případě jen na úrovni procesů, diskových prostorů a síťového provozu serverů. Výhodami této metody virtualizace jsou bezesporu rychlejší obnovení systému, jednoduché zálohování a obnova dat, rychlejší instalace nového virtuálního stroje nebo například jednoduchá správa výkonu jednotlivých virtuálních strojů. Naopak nevýhodou je určitě nutnost provozovat na hostitelském stroji i na všech strojích virtuálních identický operační systém a také nemožnost instalace aplikací, které zasahují do jádra operačního systému (například antiviry, firewally atd.…). Nejrozšířenějšími představiteli tohoto druhu virtualizace jsou Virtuozzo, FreeBSD Jail a Solaris Containers. [10]

### 2.4.3 Paravirtualizace

První z hardwarových virtualizací je tzv. paravirtualizace. Jedná se o speciální druh virtualizace, při kterém dochází ke změnám částí operačního systému virtuálních strojů. Díky tomu je sice systém výrazně rychlejší, ale téměř to znemožňuje jakoukoliv přenositelnost. Příkladem paravirtualizace je open source projekt Xen. [2]

### 2.4.4 Emulace

Emulace (nebo také simulace) je taková virtualizace, kdy dochází k simulaci nějakého přesně specifikovaného hardwaru na zcela jiné hardwarové platformě. Jelikož se jedná o zcela jiný hardware a dochází i k simulaci procesoru, nemůže emulace využívat funkce procesorů optimalizovaných pro hardwarovou virtualizaci. Z tohoto důvodu je emulace oproti ostatním hardwarovým vizualizacím značně pomalejší.

Emulace se využívá při testování aplikací pro procesory, které se již nevyrábějí, nebo naopak které se ještě vyrábět nezačaly, apod. Asi nejznámějším emulátorem je pro širokou veřejnost DOSBox, což je emulátor starého x86 PC, pro optimální běh aplikací pro MS-DOS.

### 2.4.5 Plná virtualizace

Poslední a pro mne nejdůležitější metodou virtualizace je plná virtualizace (nativní). V případě plné virtualizace dochází k simulaci všech hardwarových součástí počítače. Velice se podobá emulaci, ale v případě plné virtualizace nedochází k virtualizaci zcela jiné platformy, a tudíž lze využívat speciální funkce novějších procesorů, podporující virtualizaci (AMD V a Intel VT). Přístup virtuálního hardwaru ke skutečnému není přímý, ale je zprostředkovaný. Tato metoda má několik výhod. Lze nastavit vyhrazenou operační paměť u jednotlivých strojů, zrychlí se všechny možné operace s virtuálními stroji (restart, reinstalace) a v neposlední řadě se zjednodušuje zálohování a obnovení. Zástupců této třídy virtualizačních nástrojů je mnoho. Lze je rozdělit do dvou hlavních skupin – podle toho, jaký typ hypervizoru (vrstva mezi fyzickým hardwarem a virtuálním strojem) používají. První kategorii tvoří ty produkty, které běží na hostitelském operačním systému. Za všechny bych uvedl například Microsoft Virtual PC, VMware Server/Workstation a Sun VirtualBox. Druhou kategorií jsou aplikace, které se instalují přímo na hardware. Sem patří hlavně aplikace VMware ESX server, VMware vSphere a Microsoft Hyper-V. Právě kvůli výše zmíněné VMware vSphere považuji tuto kategorii za nejdůležitější, protože toto řešení jsem využíval pro praktické testování. [2][9]

# 3 BCM ve virtualizovaném prostředí

Počet subjektů, které virtualizaci zavádějí, i nárůst jednotlivých složek informačních systémů, které se dají efektivně virtualizovat, stále roste. Proto se stále více a více subjektů, se zavedeným systémem řízení kontinuity činností musí potýkat s velice důležitými změnami, které v tomto plánu nastávají po implementaci virtuální infrastruktury. Pro subjekty, které zatím řízení kontinuity činností zavedeno nemají, by

právě přechod na virtualizaci mohl být odrazovým můstkem pro vytvoření koncepce řízení kontinuity činností a implementaci těchto technik.

První vlastností virtualizace, na kterou je důležité se podívat očima řízení kontinuity činností, je to, že virtualizace podporuje konsolidaci serverů. Počet fyzických serverů se díky virtualizaci může velice razantně zmenšit, protože virtualizace umožňuje efektivnější využívání systémových prostředků. Při přesunu několika virtuálních strojů na jeden fyzický ovšem úměrně narůstá ztráta, kterou společnost zaznamená při jeho výpadku. Dosud, pokud vypadl jeden fyzický stroj, došlo k výpadku jedné nebo více služeb, které na tomto stroji běžely. Pokud ovšem po přechodu na virtuální prostředí vypadne jeden z hostů, budou nedostupné služby na všech virtuálních serverech běžících na daném hostu – jelikož běžně bývá přibližně pět fyzických serverů přesouváno na jednoho hosta ve virtuální podobě (samozřejmě se to může měnit, záleží na službách, které na nich běží), vypadne v absolutním případě pětkrát více služeb. Tento příklad je dalším dobrým důvodem, proč při přechodu na virtuální infrastrukturu využít příležitosti a implementovat techniky řízení kontinuity činností. Vykompenzuje to částečně nárůst rizika spojený s konsolidací serverů.

Typickým znakem virtualizace, který přináší téměř jen výhody, jsou také virtuální obrazy. Díky tomu, že virtuální stroje jsou uchovávány v podobě virtuálních obrazů, je manipulace s nimi výrazně jednodušší. Můžeme je lehce klonovat, migrovat z jednoho hardware na jiný, či zálohovat. Možnost provedení všech právě uvedených operací defakto jen za pomoci jednoho kliknutí myší je v porovnání s migrací fyzického serveru na jiný hardware opravdu nesrovnatelně jednodušší a hlavně rychlejší.

## *3.1 Oblast dostupnosti*

Implementace virtuálního prostředí se v rámci informačního systému projevuje hlavně ve dvou oblastech řízení kontinuity činností. První oblastí je dostupnost. „Z definice dostupnost označuje pravděpodobnost, obvykle vyjádřenou v procentech, že systém bude provozuschopný v souladu se zadanými podmínkami. Jinak řečeno, dostupnost specifikuje čas, po který lze systém využívat podle zadaných podmínek, vztažený k celkové době jeho užívání za předpokladu, že doba používání systému je dostatečně dlouhá, aby bylo možné aplikovat pravděpodobnostní metodiky. Nedostupnost pak určuje pravděpodobnost, s jakou systém nebude při dlouhodobém využívání pracovat v souladu se zadáním.“ [17] Cílem každého subjektu je, aby jeho

vnitropodnikové i vnější služby měly dostupnost co největší. Ideálním stavem je dostupnost stoprocentní, které se ale dosahuje pouze velice obtížně. Jak jsem již uvedl dříve v této kapitole, dostupnost jedné konkrétní služby se při přesunu do virtuálního prostředí nijak nemění. Co se mění, je fakt, že při výpadku bude nedostupných služeb víc. Proto se musíme úměrně více snažit, aby ke snížení nedostupnosti nedošlo. Pomoci nám mohou například nástroje, monitorující zatížení jednotlivých host serverů a včas upozorňující na přetížení, které by mohlo vést k jeho výpadku. I přes upozornění je ale třeba situaci řešit co nejrychleji. V ideálním případě program, jinak lidská síla v podobě administrátora, musí na situaci zareagovat tím, že příliš zatíženému hostu uleví a sníží velikost jeho použitých systémových prostředků.

## *3.2 Oblast obnovy dostupnosti služeb*

Druhou, neméně důležitou oblastí řízení kontinuity činností, kterou virtualizace v informačních systémech mění, je oblast zálohování a hlavně s ním souvisejícího obnovení systému. V tomto případě již došlo k výpadku služby a ta je díky tomu nedostupná. Nastupuje tedy plán řízení kontinuity činností, který řeší, jak službu co nejrychleji opět učinit dostupnou v co největším rozsahu. Díky virtuálním obrazům je tento proces oproti klasickým fyzickým serverům značně zjednodušen. Stejně jako ve fázi, kdy ještě k výpadku dostupnosti nedošlo, ale jen hrozila, tak i v této fázi umí některé nástroje jednat automaticky. Základní reakcí je upozornění administrátora. Některé nástroje poté samy začnou problém řešit – najdou v rámci infrastruktury volný hardware a na něm vypnuvší se virtuální stroj restartují. Pokud toto není možné, musí problém řešit sám administrátor. To, že pracuje s virtuálním prostředím, mu ovšem práci opět velice zjednodušuje. Pomohou mu právě již zmiňované virtuální obrazy a hlavně nástroje pro práci s nimi. Pokud si takový administrátor dobře nastavil zálohovací proceduru, neměl by pro něj být problém se pomocí pár kliknutí dostat k uloženému snapshotu daného virtuálního stroje, či přímo k jeho záložnímu obrazu a ten během velice krátké doby spustit na novém host serveru. Odpadá tak fáze, kdy v případě klasické fyzické infrastruktury musel administrátor složitě vybalovat zálohu a server z této zálohy obnovovat.

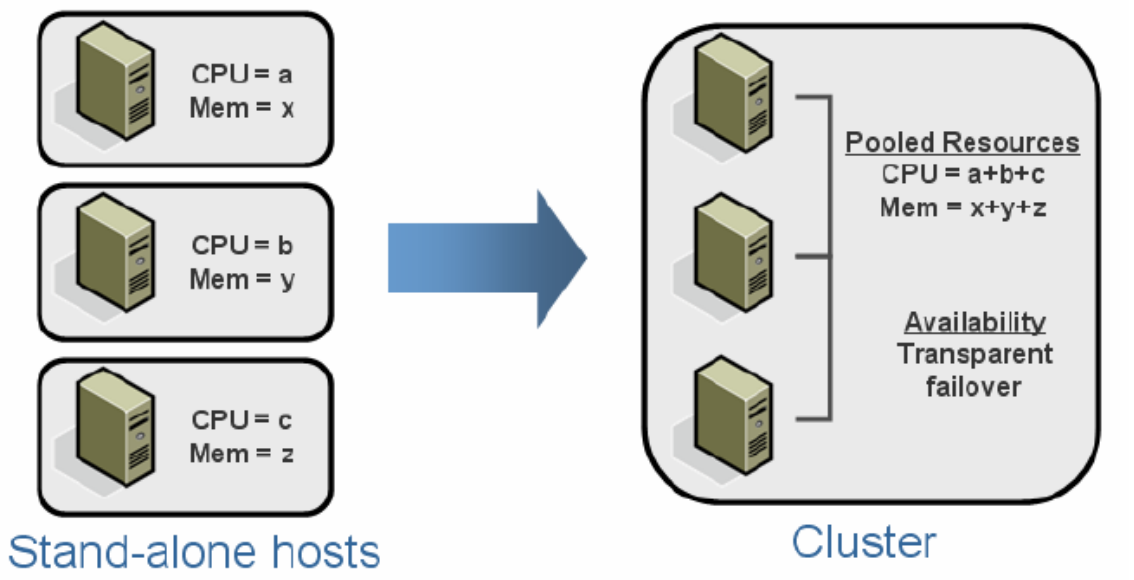
# 4 Nástroje podporující BCM od společnosti VMware

Společnost VMware je předním dodavatelem virtualizačních řešení na celosvětovém trhu. Nástrojů, které napomáhají při svém nasazení technikám BCM, postupným vývojem přibývá a v současné době jich společnost VMware nabízí celou řadu. Všechny jsou součástí placené verze virtuálního prostředí – produktu vSphere. Ve freeware produktu VMware ESXi server bohužel chybí. Jak jsem již uvedl v kapitole 3, pro podporu řízení kontinuity činností slouží hlavně dva základní druhy nástrojů. Zaprvé jde o nástroje, které pomáhají předcházet dlouhodobým výpadkům služeb. V rámci produktu VMware vSphere jsou tyto nástroje reprezentovány zejména technologiemi High Availability, vMotion a DRS. Chod všech předchozích technologií je podmíněn funkcí VMware vSphere, která se jmenuje Clustering – tedy tvoření tzv. clusterů z ESX serverů. Druhou skupinou nástrojů jsou nástroje, které v případě již existujícího výpadku některé ze služeb zajistí, že k obnovení její funkčnosti dojde co nejdříve. Nejdůležitějšími zástupci v této kategorii jsou v rámci vSphere hlavně Consolidated Backup a Data Recovery. [11]

## *4.1 Clustering*

### 4.1.1 Funkce

Clustering (česky také někdy klastrování) je způsob řízení systémových prostředků. Jedná se o vytváření tzv. clusterů, což jsou skupiny několika ESX serverů, jejichž systémové prostředky jsou v clusteru spojeny dohromady. Ve výsledku se tváří jako jeden prvek, který se tím pádem snadněji spravuje. Výborně ilustruje techniku clusterů obr. 3 – v levé části vidíme jednotlivé samostatné ESX servery a v pravé části z nich vytvořený cluster. Vidíme, že došlo ke spojení systémových prostředků (procesor a paměť) dohromady. [13]




Obr. 3 – Princip clusterů [Obr. 3]

### 4.1.2 Přínos

Hlavním výhodou, kterou clustering přináší, je zefektivnění řízení systémových prostředků a zdrojů. Sdružení několika ESX serverů nám umožňuje spravovat jejich systémové prostředky jako jeden velký celek. V praxi tak například můžeme na jednom hostu spustit virtuální stroj, který bude mít přiděleny větší systémové prostředky, než je host schopen poskytnout – zbylé prostředky dostane virtuální stroj přiděleny z jiného ESX serveru, který je nevyužívá. Tato technologie je základem všech pokročilejších nástrojů podporujících virtualizaci od společnosti VMware. Zejména pak nástroje VMware DRS a VMware High Availability. [13]

## *4.2 VMware vMotion*

### 4.2.1 Funkce

Technologie VMware vMotion nám umožňuje přenesení virtuálního stroje z jednoho hostitelského ESX Serveru na jiný hostitelský ESX Server. Samozřejmě se jedná o stroj běžící a celý proces přenosu probíhá bez výpadku dostupnosti tohoto přenášeného virtuálního počítače. Tato technologie se využívá v rámci funkce VMware DSR, která stroje přesouvá z důvodů přehlcení některého z hostů. Dalším případem užití je manuální migrace virtuálního stroje na jiný hostující ESX server. Sama firma VMware deklaruje, že při procesu přesunování virtuálního počítače z jednoho

hostitelského serveru na jiný hostitelský server může dojít pouze ke krátkodobým výpadkům síťového spojení. Praxe toto tvrzení potvrzuje. Je ověřeno, že pokud se monitoruje síťové spojení např. utilitou zvanou PING, ztratí se při samotném procesu přesunování virtuálního počítače nanejvýš dva až tři pakety. Uživatelé proces samotného přesunu ve většině případů vůbec nezaznamenají. Pokud si toho všimnou, projevuje se tento proces zamrznutím virtuálního počítače na maximálně 2 – 3 sekundy, protože po tuto dobu virtuální počítač nekomunikuje.[13]

### 4.2.2 Použití a přínos

Jak jsem již nastínil v kapitole 4.1.1, je vMotion primárně využíván funkcí VMware DSR. Tuto funkci lze nastavit i takovým způsobem, že jednotlivé virtuální počítače v případě nedostatku hardwarových prostředků na jednom hostitelském ESX serveru se automaticky přesunou na jiný ESX Server s dostatečně volnou hardwarovou kapacitou tak, aby nedošlo k omezení dostupnosti a výkonu jednotlivých virtuálních počítačů. Lze tak jednoduchým způsobem nastavit automatické rozkládání zátěže mezi jednotlivými hostitelskými ESX Servery. V neposledním případě lze této funkcionality využít při plánované odstávce ESX Serveru, kdy bude tento hostitelský počítač nedostupný a nebude schopen poskytovat virtualizační služby. Aby se tak zamezilo nutné odstávce jednotlivých virtuálních počítačů běžících na tomto hostitelském serveru, kde se bude provádět plánovaná odstávka, přesunou se všechny běžící virtuální počítače „za chodu“ na jiný hostitelský počítač bez přerušení jejich dostupnosti. Nebudou tak omezeny služby, které poskytují tyto jednotlivé virtuální počítače. [12]

### 4.2.3 Podmínky pro správnou funkčnost vMotion

Podmínek pro správné fungování technologie VMware vMotion je několik. První velice důležitou podmínkou je sdílené úložiště, kde je obraz virtuálního stroje, který chceme pomocí funkce vMotion přenášet. Tento obraz nemůže být uložen na daném ESX serveru lokálně, ale musí být uložen na tzv. sdíleném úložišti virtuálních obrazů. Tuto funkci mohou plnit dvě technologie. Buď diskové pole, nebo běžný NFS server (NFS = network file system – standard sdílení souborů v Linuxu). K tomuto úložnému prostoru musí mít přístup jak host, na kterém běží stroj, který chceme přesunout, tak i host, který má být při přesunu cílovým. V obou případech musí mít povoleno čtení i zápis do sdíleného umístění.

Druhou, také bezpodmínečně nutnou podmínkou, je shodnost masek procesorů jednotlivých ESX hostů. Pokud tedy přenášíme virtuální stroj mezi dvěma ESX hosty, které mají stejnou hardwarovou konfiguraci (typ procesoru), bude vMotion bez problémů fungovat. Problém nastává, když se jedná o rozdílné modely procesoru. Tento problém nám ale pomůže jednoduše vyřešit přímo základní ESX server. Ten totiž umožňuje u virtuálních strojů nastavovat nejen počet jader procesoru, počet samotných procesorů, jejich takt atd., ale obsahuje i funkci, která nám pomáhá emulovat jednotlivé procesorové masky, tzv. CPU ID. Díky němu může vMotion pracovat i se dvěma různými procesory, pokud na virtuálním stroji, který chceme přesouvat, nastavíme napevno masku procesoru, jakou potřebujeme.

Poslední a neméně důležitou podmínkou je existence tzv. servisního virtuálního vMotion switche v daném virtuálním prostředí. Podsíť, kterou tento switch spojuje všechny hosty s ovládacím serverem – server s aplikací vCenter – slouží čistě pro účely technologie vMotion a probíhají přes ni veškeré datové přesuny virtuálních strojů atd.… Do této podsítě by měly být jednotlivé ESX servery připojeny (podle doporučení společnosti VMware) pomocí separátní síťové karty. Vzniká tak vlastně druhé paralelní propojení mezi ESX hostem a vCenter serverem – jedno slouží pro klasické účely managementu virtuálních strojů, jejich tvorbu a operaci s nimi a druhé slouží čistě pro funkci vMotion. Připojení pomocí separátní síťové karty ovšem není zcela nezbytné, prakticky jsem ověřil, že lze oba výše popsaná „paralelní spojení“ realizovat přes jedno síťové rozhraní ESX serveru. [13]

## *4.3 VMware High Availability*

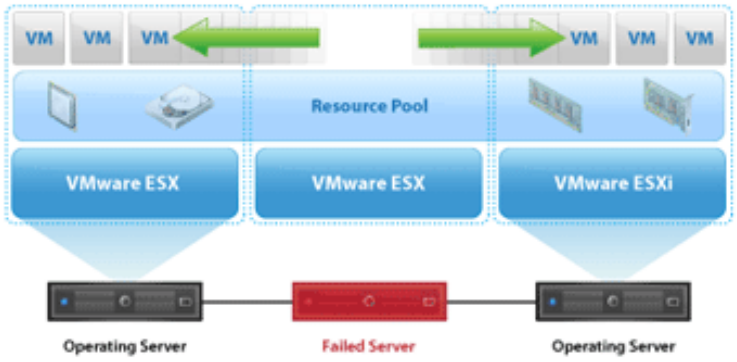
### 4.3.1 Funkce

Již název High Availability (vysoká dostupnost) nám napovídá, že tato funkce aplikace VMware vSphere bude zajišťovat co největší dostupnost důležitých služeb. VMware High Availability neustále monitoruje všechny servery ve zdrojovém clusteru a hlídá jejich případné selhání. Na jednotlivých serverech, které chceme monitorovat, je nainstalován tzv. agent, pomocí kterého udržuje High Availability s těmito virtuálními servery pravidelné spojení (pomocí tzv. „heartbeatů“). Při ztrátě spojení spustí proces restartování všech dotčených virtuálních strojů na jiném ESX hostu. Program VMware High Availability sám zajišťuje, aby byl ve zdrojovém clusteru neustále dostatek

dostupných zdrojů, a bylo tedy možno v případě selhání nějakého serveru restartovat virtuální stroje na jiných fyzických serverech. Funkce je dobře ilustrována na obr. 4. [13]

### 4.3.2 Přínos

VMware High Availability umožňuje podniku zajistit vysokou dostupnost libovolné aplikace provozované na virtuálním stroji. Vysokou dostupnost lze takto zajistit kterékoliv aplikaci běžící na virtuálním stroji, který sám běží na ESX serveru, na němž je funkce High Availability (HA) aktivní. Řešení pro vysokou dostupnost bývají poměrně složitá a nákladná, a obvykle jsou proto vyhrazena pouze pro kritické podnikové aplikace. VMware High Availability naopak nabízí řešení sice jednoduché, ale přesto velice účinné. Jeho funkčnost je podmíněna pouze dostatečnými záložními systémovými prostředky a existencí alespoň dvou fyzických hostujících ESX serverů spojených v jednom clusteru. Dobře nakonfigurovaný profil v aplikaci High Availability většinou ušetří podniku velké prostředky, protože minimalizuje dobu nedostupnosti kritických služeb na úplné minimum.




Obr. 4 – Princip funkce VMware High Availability [Obr. 4]

### 4.3.3 Klíčové vlastnosti

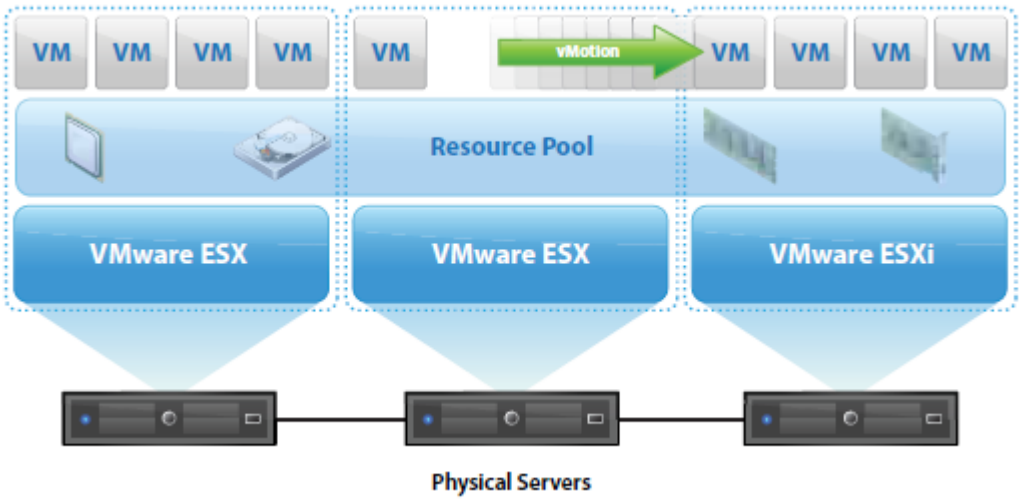
„Mezi hlavní vlastnosti patří automatická detekce selhání serveru. Monitorování dostupnosti fyzických serverů lze automatizovat tak, že když HA detekuje selhání serveru, iniciuje restartování virtuálního stroje bez jakéhokoliv lidského zásahu. Další užitečnou funkcí je kontrola zdrojů. VMware HA zajistí, aby pro restart virtuálních strojů byla k dispozici vždy potřebná kapacita. Nepřetržitě monitoruje kapacitu využití zdrojového poolu a „rezervuje“ záložní kapacitu tak, aby bylo možno kdykoliv provést

restart všech virtuálních strojů. Výběr záložního serveru, na kterém je virtuální stroj restartován, se neřídí náhodou, nýbrž ho systém sám chytře vybere, aby rozložení bylo co nejoptimálnější.“ [14]

## *4.4 VMware DRS*

### 4.4.1 Funkce

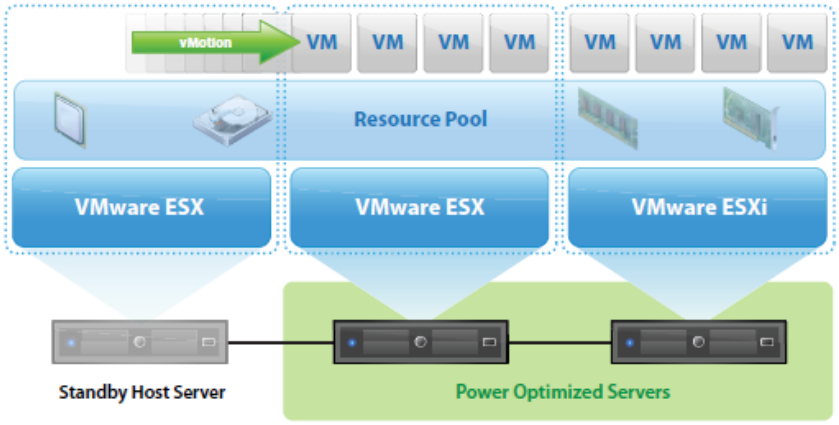
VMware DRS, neboli Distributed Resource Scheduler (volně přeloženo jako rozdělovač sdílených systémových prostředků) je druhá představovaná funkce, kterou umožňuje clusterové zapojení ESX serverů. Základní funkcí je vyrovnávání výpočetního výkonu a výpočetních zdrojů, které jsou přidělovány jednotlivým virtuálním strojům. S tím samozřejmě souvisí neustálé monitorování zatíženosti ESX hostů a také aktuální potřeby zdrojů jednotlivých virtuálních strojů. To, jak se bude DRS chovat, je vyřešeno tzv. pravidly – jedná se o soubor podmínkových příkazů definovaný člověkem, ve kterém je přesně zadáno např., že když stoupne zatížení procesoru daného ESX hostu nad 90%, DRS okamžitě pomocí funkce VMotion přesune jeden z virtuálních strojů běžících na tomto serveru na jiný, méně vytížený ESX host. Schematicky je princip tohoto nástroje zobrazen na obr. 5. Nejspodnější vrstva představuje fyzické servery, nad nimi je vrstva hypervizorů, které jsou spojeny do jednoho clusteru a tvoří hromadné systémové prostředky – šipka zde představuje DRS v akci, když přesouvá pomocí nástroje vMotion virtuální stroj z prostředního serveru na pravý proto, aby mohlo prostřední server vypnout, a tak šetřit jak energii, tak hardware.




Obr. 5 – Princip nástroje VMware DRS [Obr. 5]

### 4.4.2 VMware DPM

VMware DPM, neboli Distributed Power Management, je velice praktickou součástí DRS. Jedná se o nástroj, který neustále monitoruje energetické využití jednotlivých hostů a v případě, že pro virtuální stroje běžící na daném hostu se najde místo na hostech jiných, přesune DRS tyto virtuální stroje na jiné hosty a DPM může volný ESX server uvést do režimu stand-by, či úplně vypnout. Funkci DPM ilustruje obr. 6.




Obr. 6 – Princip funkčnosti nástroje VMware DPM – popis je podobný jako u obr. 5, jen v tomto případě se ESX server, ze kterého jsou přesunuty všechny virtuální stroje, přepnul do stand-by modu. [Obr. 6]

### 4.4.3 Přínosy

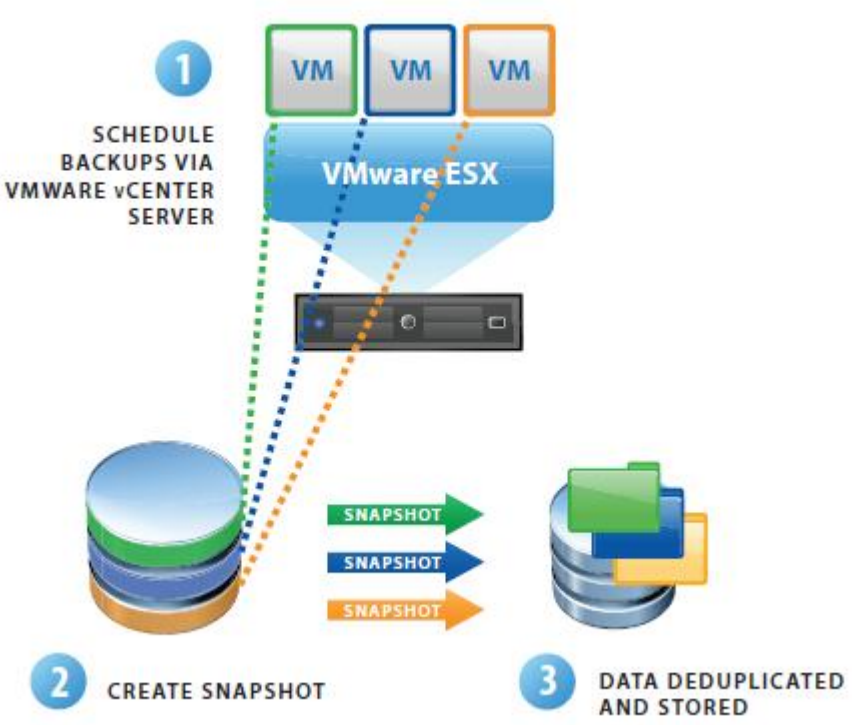
Přínosů nástroje VMware DRS je několik. Tím, že kontroluje nadměrné zatížení ESX serverů, předchází jejich přetížení. Stejně tak pomáhá virtuálním strojům najít vždy optimální množství systémových zdrojů. Může se jednat o tak časté přesuny virtuálních strojů mezi jednotlivými servery, že by se stroji ve fyzické podobě ani nešly provést. Naopak, když objeví DRS v clusteru větší množství málo zatížených ESX hostů, přesune virtuální stroje tak, aby DPM mohlo jednoho z hostů vypnout nebo převést do režimu stand-by. [15]

## *4.5 VMware Data Recovery*

### 4.5.1 Funkce

Tento produkt společnosti VMware je dostupný pouze ve vSphere vyšší verze, verze Essentials Plus. Jedná se o velice účinný nástroj pro zálohování celých virtuálních strojů pomocí tvorby jejich shapshotů (viz kap. 2.3). Data Recovery zvládá zálohovat kompletně, ale i inkrementálně a zálohovací úlohy lze samozřejmě plánovat. Program při spuštění zálohovací procedury vytvoří aktuální snapshot daného virtuálního stroje, který uloží do vybraného úložiště.

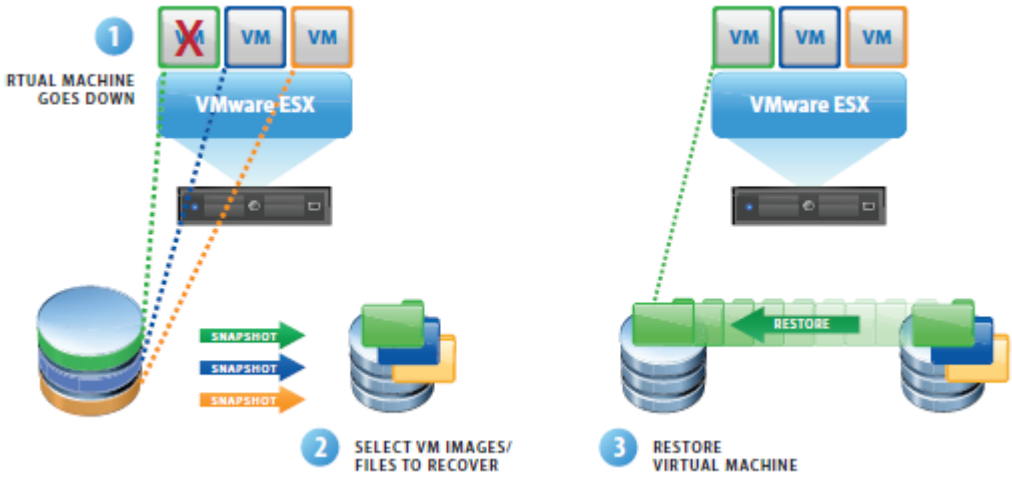
Program se skládá ze tří základních komponent. První částí je uživatelské rozhraní pro konfiguraci programu a pro možnost spuštění zálohy/obnovy. Toto uživatelské rozhraní se instaluje jako plug-in přímo do aplikace vCenter server. Tak můžeme zálohování ovládat ze stejného prostředí jako všechny ostatní produkty, které jsou součástí VMware vSphere. Druhá část se přímo stará o provádění záloh, jejich přesouvání apod. Poslední částí je speciální úložiště, kam se snapshoty ukládají. Toto úložiště je řízeno speciálním nástrojem, nazvaným De-duplicated storage manager, který vyhledává v obrazech duplicitní data, sjednocuje je, a tím výrazně šetří místo. [16]




Obr. 7 – Proces tvorby zálohy pomocí nástroje VMware Data Recovery [Obr. 7]

Na obr. 7 vidíme schéma tvorby záloh pomocí tohoto nástroje. V první fázi naplánujeme zálohovací úlohy pomocí aplikace VMware vCenter server – vybereme, které stroje zálohovat, zda půjde o plnou zálohu, inkrementální, či jen o vybrané adresáře nebo soubory, a nakonec vybereme, kam se bude zálohovat. V druhé fázi dojde k vytvoření obrazů virtuálních strojů, které jsme požadovali. Ve třetí fázi jsou pak tyto obrazy přesunuty na vybrané úložiště záloh a zpracovány technologií Data De-Duplication, aby se zefektivnilo množství úložného prostoru, zabraného těmito obrazy.

Obr. 8 nám ukazuje druhý důležitý proces, kterým je obnovení některého ze strojů ze zálohy. V tomto případě dojde nejdříve k výpadku některého z virtuálních strojů (bod 1). Po tomto zjištění administrátor opět pomocí rozhraní programu VMware vCenter server vybere, který z obrazů daného virtuálního stroje či která jeho část, se má obnovit. Tento obraz je pak vyhledán v úložišti záloh, odkud se nahraje na konkrétní ESX server a zde je spuštěn. V případě obnovy pouze části dat jsou tato data nakopírována do zvoleného úložiště ve vybraném virtuálním stroji.




Obr. 8 – Obnovení dat pomocí nástroje VMware Data Recovery [Obr. 8]

### 4.5.2 Přínos

VMware Data Recovery má oproti jiným zálohovacím programům obrovskou výhodu v tom, že pracuje s virtuálními obrazy. Není proto problém zálohovat i virtuální stroj, který je vypnutý, či který zrovna migruje z jednoho ESX serveru na jiný. Na strojích, které zálohujeme, také nemusí běžet žádný agent a nemusí být nainstalován žádný zálohovací software. Veškeré ovládání záloh, jejich spuštění, plánování, či obnova dat ze zálohy se provádí přes aplikaci vCenter server, čímž nám odpadá nutnost užívání více aplikací pro řízení virtuálního prostředí. Díky výše zmíněné technologii de-duplikace dat na cílovém zálohovacím úložišti dochází k redukci velikosti úložného prostoru, který zálohy zabírají.

# 5 Praktická část

Pro praktickou část práce jsem si vybral vyzkoušení několika nástrojů pro podporu BCM od firmy VMware v praxi.

## 5.1 Testovací prostředí

### 5.1.1 Hardware

Jako hardware mi posloužily 3 servery a jeden notebook jako klient. Dva ze serverů plnily funkci hostů a třetí byl v roli síťového úložiště. Všechny tyto prvky byly propojeny gigabitovou ethernetovou sítí.

| Název | Role | Typ | CPU | RAM |
|---|---|---|---|---|
| ESX1-245 | ESX host | IBM x3650 | 8 x 2,0GHz | 16 GB |
| ESX2-246 | ESX host | IBM x3550 | 8 x 2,27 GHz | 16 GB |
| NFS | Síťové úložiště | IBM x226 | 2 x 2,0 GHz | 4 GB |
| Klient | Klient | Fujitsu Siemens Amilo Pro V3205 | Intel Core 2 Duo T5200 1,6 GHz | 3 GB |

Tab. 1 – Seznam použitého hardwaru

### 5.1.2 Software

Jako hlavní virtualizační řešení jsem použil 60ti-denní zkušební verzi produktu VMware vSphere Essentials Plus. Tato verze produktu vSphere obsahuje všechny v této práci zmíněné a popisované nástroje pro podporu business continuity managementu ve virtuálním prostředí. Jako hypervizory jsem použil VMware ESX servery. V balíku vSphere je ještě k dispozici ESXi verze hypervizoru, ale jedná se o redukovanou verzi, která nepodporuje některé z testovaných funkcí.

| Název | Role | Typ OS | Licence OS | Software |
|---|---|---|---|---|
| ESX1-245 | ESX host | VMware ESX 4.0 hypervizor | 60ti-denní zkušební | |
| ESX2-246 | ESX host | VMware ESX 4.0 hypervizor | 60ti-denní zkušební | |
| NFS | Síťové úložiště | openSUSE Linux 11.2 | opensource | Vestavěný NFS klient |
| Klient | Klient | MS Windows 7 Professional | Školní MSDN | VMware vSphere client |

Tab. 2 – Seznam použitého softwaru

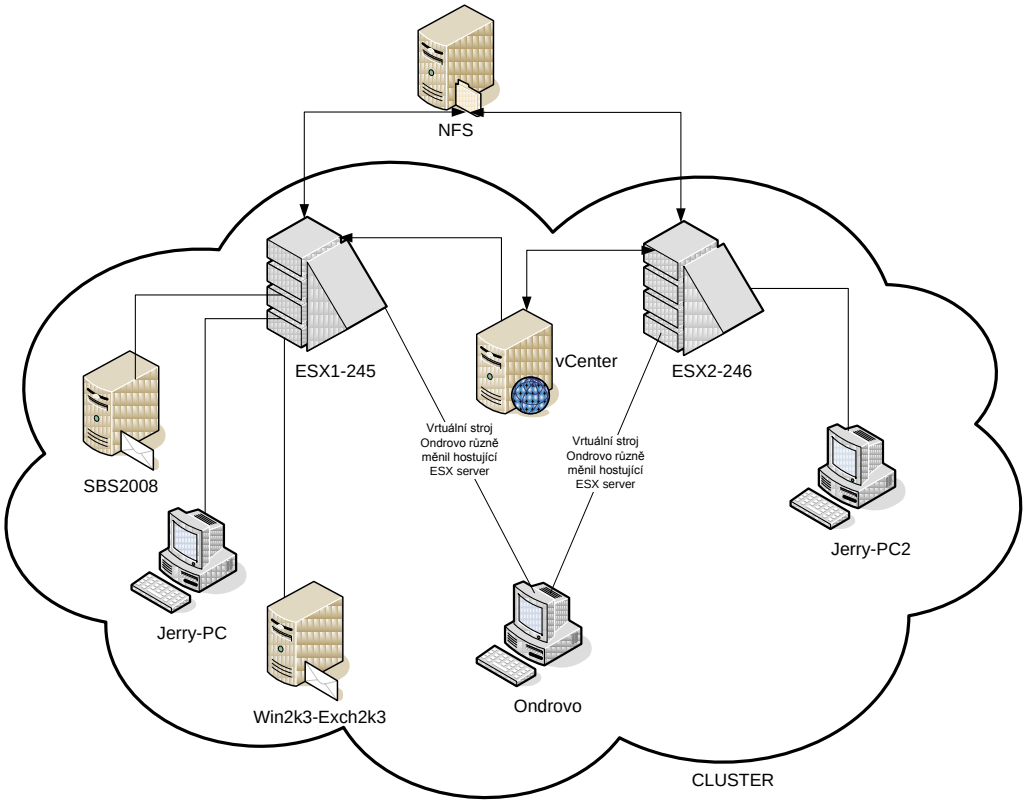
### 5.1.3 Virtuální stroje

V normálních reálných podmínkách by byl vyžadován ještě jeden fyzický server navíc, jako platforma pro nainstalovaný VMware vCenter server. Jelikož jsem už víc testovacích serverů k dispozici neměl, musel jsem tento fyzický stroj nahradit strojem virtuálním běžícím přímo na jednom z hostů. V praxi je toto řešení velice nevhodné a nemělo by se nikde objevit, ovšem pro testovací účely je dostačující, pouze zamezuje jakémukoliv odstavení ESX hostu, na kterém běží. K tomuto virtuálnímu stroji jsem vytvořil (někdy jen zkopíroval) ještě několik jiných různě nakonfigurovaných virtuálních strojů, abych mohl alespoň částečně simulovat skutečnou podobu virtuální infrastruktury. Virtuálním strojem, na kterém jsem testoval různé nástroje, pak byla hlavně virtuální pracovní stanice s názvem „Ondrovo“.

| ESX host | Jméno virtuálního stroje | OS virtuálního stroje | Funkce |
|---|---|---|---|
| ESX1-245 | SBS2008 | MS Win Server SBS 2008 | Modelový stroj, tvořící zátěž hosta |
| ESX1-245 | Jerry–PC | MS Windows 7 Professional | Modelový stroj, tvořící zátěž hosta |
| ESX1-245 | Ondrovo | MS Windows 7 Professional | Hlavní stroj pro testování |
| ESX1-245 | Win2k3-EXCH2k3 | MS Win Server2003+Exchange2003 | Modelový stroj, tvořící zátěž hosta |
| ESX2-246 | Jerry-PC2 | MS Windows 7 Professional | Modelový stroj, tvořící zátěž hosta |
| ESX2-246 | vCenter | MS Win Server 2003 + VMware center server | Platforma pro center server, spravující celý cluster |

Tab. 3 – Seznam virtuálních strojů

### 5.1.4 Schéma

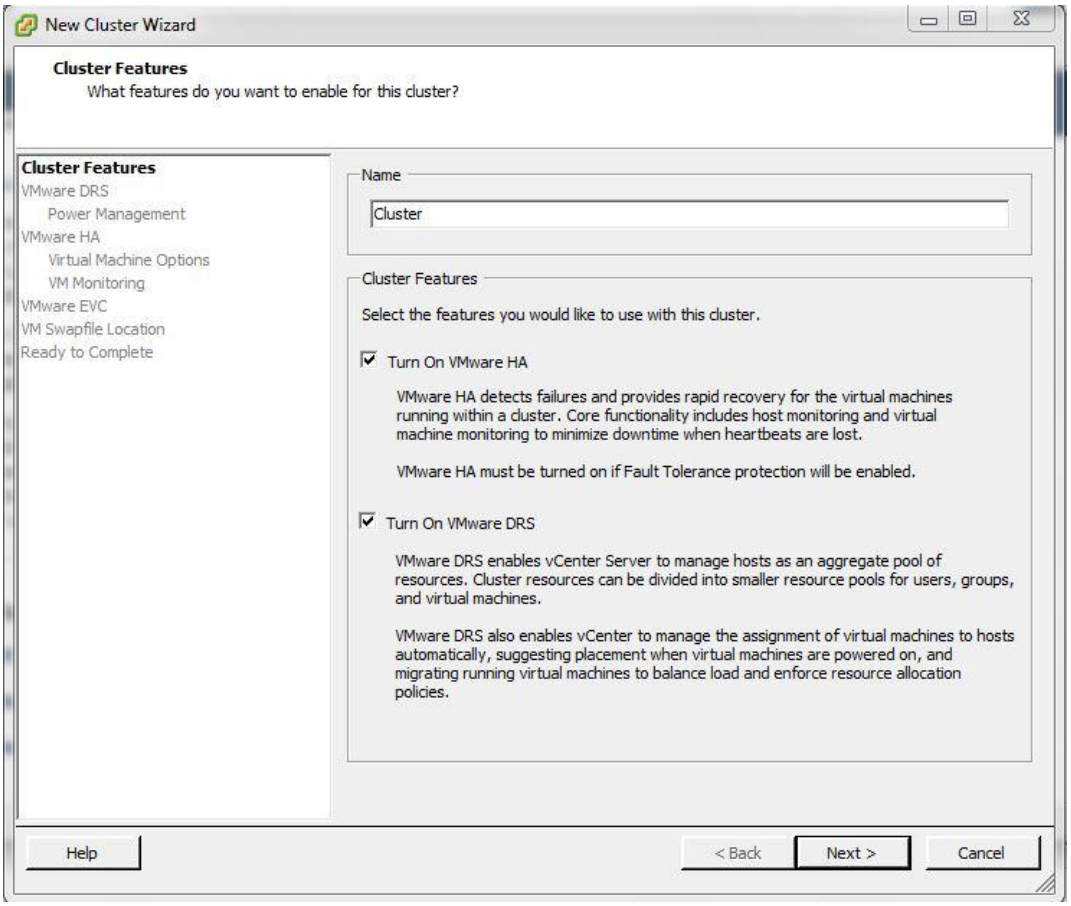



Obr. 12 – Schéma testovacího prostředí [Obr. 12]

## *5.2 Vytvoření clusteru*

Vytvoření clusteru je základem pro všechny další testované nástroje. Cluster umožňuje správu více ESX hostů jako jednoho celku s tím, že jejich systémové zdroje sloučí dohromady a pak je rozděluje jednotlivým virtuálním strojům, které v clusteru běží (na kterémkoliv z ESX serverů, které jsou součástí daného clusteru).

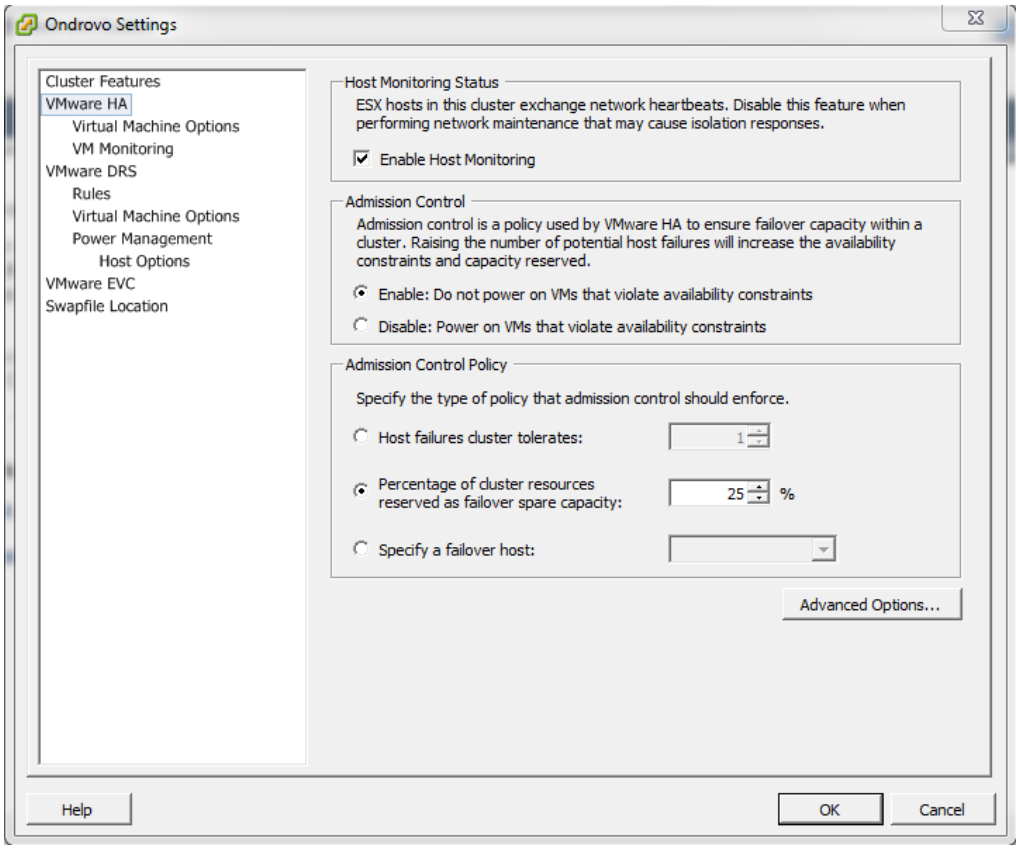
Vytvoření clusteru je velice jednoduchý proces. V základním okně vCenteru vybereme organizační jednotku a jednoduše vybereme v menu vytvoření nového clusteru. Cluster pojmenujeme a dále si můžeme vybrat, zda v rámci clusteru bude zapnuta funkce VMware High Availability a funkce VMware DRS. Konfiguraci těchto dvou funkcí popíšu dále. Po vytvoření clusteru do něj můžeme jednotlivé hosty jednoduše přesunout myší.




Obr. 9 – Vytvoření nového clusteru [Obr. 9]

## *5.3 Nastavení VMware High Availability*

Po vybrání možnosti, že je VMware High Availability aktivní, se nám při vytváření clusteru (i při pozdější změně jeho vlastností) objeví nové možnosti nastavení. Jedná se právě o nastavení funkce High Availability. Můžeme si vybrat, zda chceme, aby fungovalo monitorování jednotlivých hostů pomocí funkce heartbeat. Dále máme možnost nastavit omezení, které zabrání zapnutí virtuálního stroje, pokud by tím mělo dojít k ohrožení běhu ostatních, či celého hostu. Může to být z důvodu přetížení systémových prostředků nebo z důvodu konfliktu IP adres apod. Jako poslední nastavíme, kde se má virtuální stroj restartovat – buď můžeme High Availability nechat, aby pro takové případy udržoval určitou část systémových zdrojů clusteru volných, nebo můžeme vybrat konkrétní ESX host, na kterém se stroj spustí.




Obr. 10 – Nastavení funkce High Availability [Obr. 10]

## 5.4 Nastavení VMware DRS

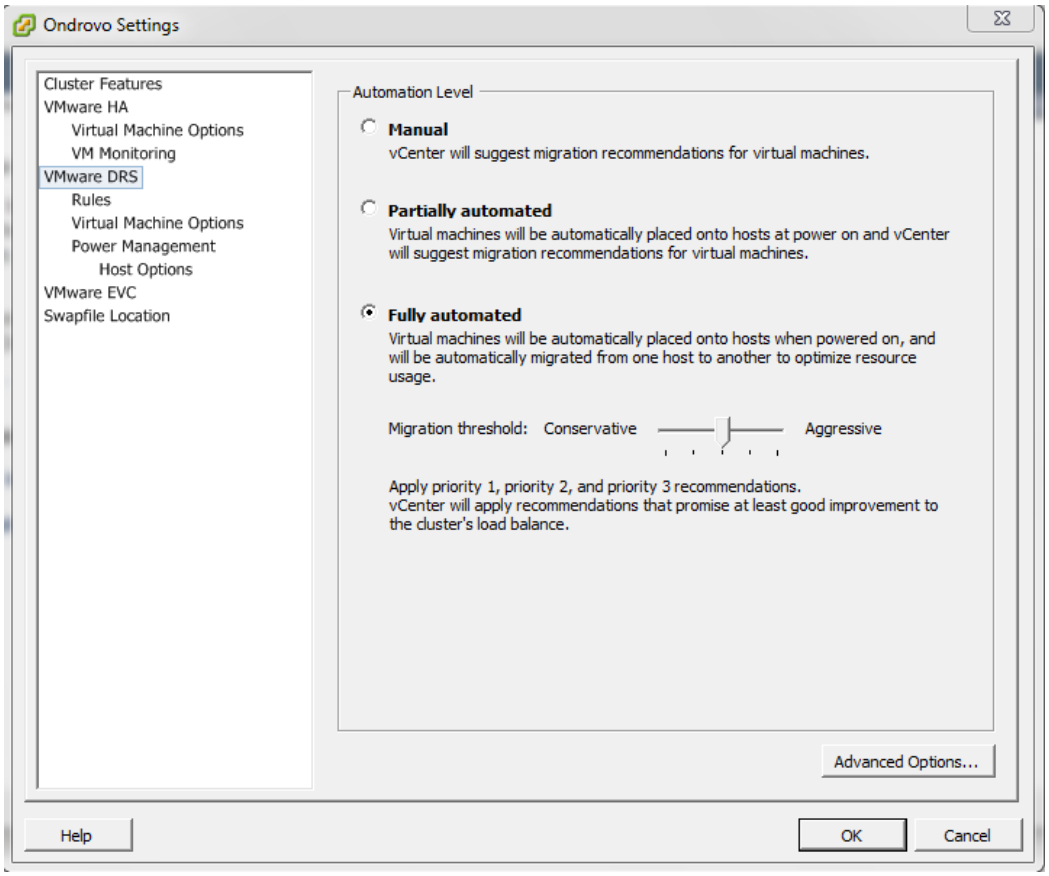
Nastavení funkce VMware DRS je stejně jako u High Availability velice srozumitelné a relativně jednoduché. Na první záložce vybíráme základní úroveň funkce DRS. Na výběr máme ze tří možností:

1) Manuální – DRS pouze zahlásí, že by některý stroj měl být přesunut, ale je na administrátorovi, aby tak učinil

2) Částečně automatická – při startu virtuálního stroje DRS automaticky vybere, na kterém ESX hostu se spustí. Poté již jen monitoruje stav a stejně jako u manuálního modu dává doporučení, který stroj kam přesunout.

3) Plně automatická – v tomto případě DRS při startu virtuálního stroje samo určí, na kterém hostu se stroj spustí, poté monitoruje stav a v případě potřeby bez jakéhokoliv zásahu administrátora samo virtuální stroj přesune, když je třeba.

Dále můžeme definovat pravidla, umožňující nám nastavit dvě možnosti. Můžeme si vybrat skupinu virtuálních strojů, které vždy chceme mít spuštěny na jednom hostu, a naopak si můžeme vybrat skupinu virtuálních strojů, které nikdy nechceme mít spuštěny na jednom hostu. Dále můžeme nastavit součást modulu VMware DRS, kterou je VMware DPM, popsaný v kapitole 4.4.2. Opět máme na výběr ze tří úrovní správy napájení. První možností je, že je tato funkce vypnuta. Při zapnutí máme možnost buď manuálního, nebo automatického modu. V manuálním modu funkce navrhuje vypnutí, či zapnutí ESX hostů a je na administrátorovi, zda tento krok provede nebo ne. V případě automatického modu vypíná a zapíná hosty funkce sama.



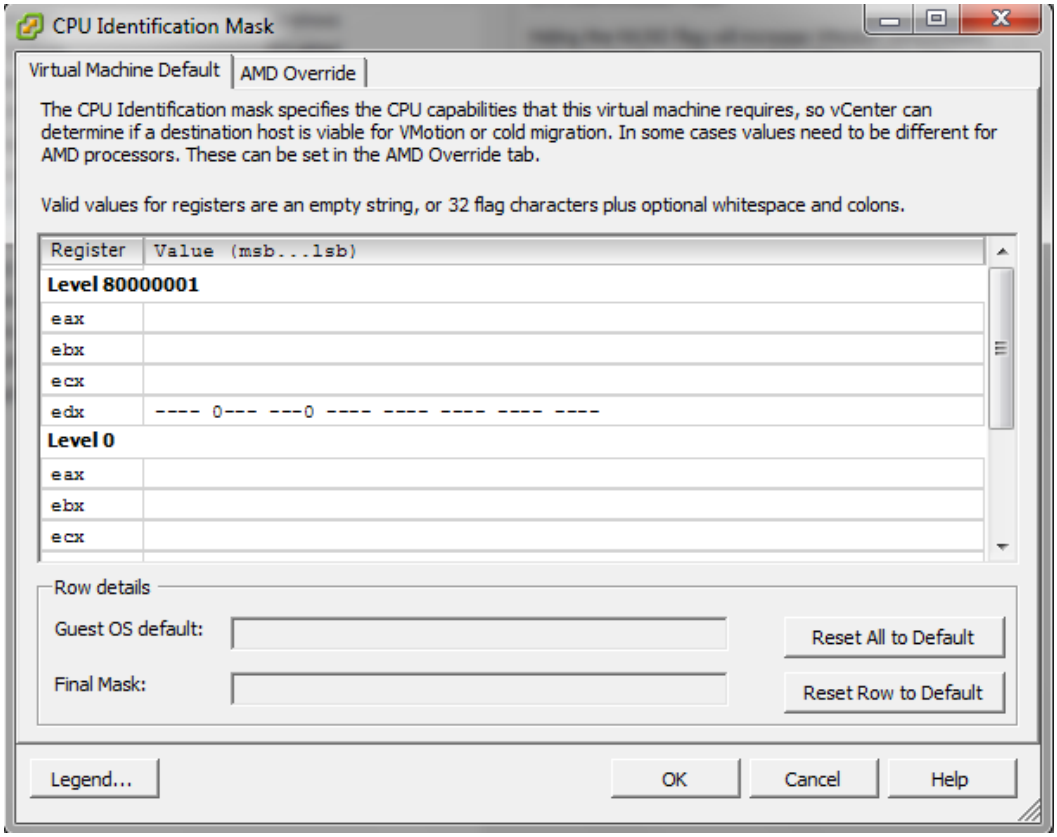

Obr. 11 – Nastavení funkce VMware DRS [Obr. 11]

## 5.5 Nastavení funkce vMotion

Jak jsem uvedl již v kapitole 4.2, funkce vMotion je podmínkou pro správný chod obou předchozích nástrojů – VMware High Availability i VMware DRS. Samotný nástroj vMotion ovšem potřebuje pro chod několik specifických nastavení a podmínek. Ty jsem popsal v kapitole 4.2.3. První podmínkou je užití síťového úložiště dat, aby

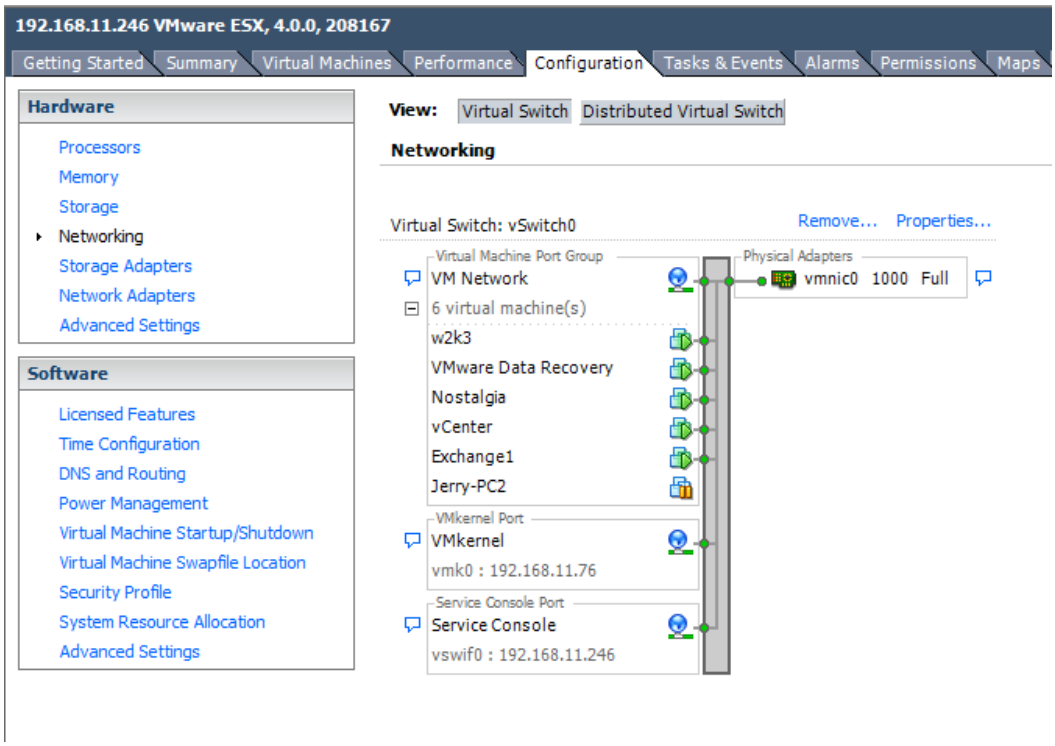
k němu měly přístup všechny ESX servery v daném clusteru. Bohužel se mi nepodařilo sehnat diskové pole, takže jsem musel zvolit variantu síťového NFS serveru. Jako operační systém jsem zvolil openSuse Linux verze 11.2. Po vytvoření tohoto serveru a nasdílení adresáře pro ukládání virtuálních strojů již stačilo jen připojit toto úložiště k jednotlivým ESX serverům.

Problematiku různých masek procesorů lze efektivně vyřešit nastavením výchozí masky přímo ve vlastnostech virtuálního stroje. Seznam jednotlivých kódů masek lze nalézt v dokumentaci programu VMware center server.




Obr. 13 – Nastavení masky CPU [Obr. 13]

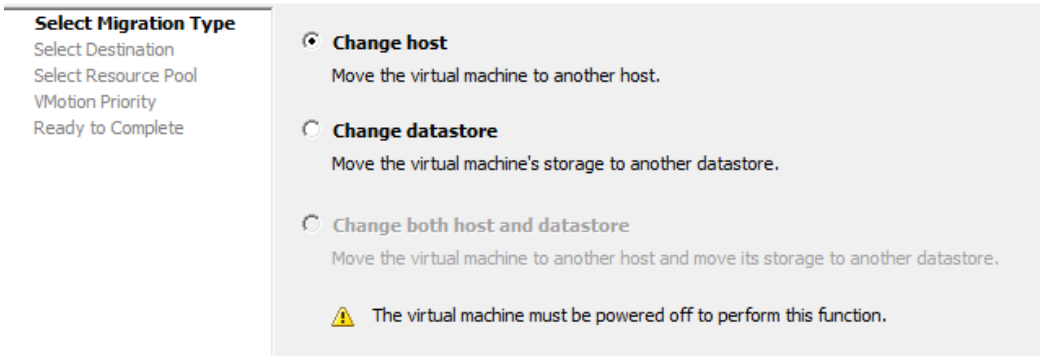
Nakonec je nutné všechny ESX servery propojit pomocí speciálního vMotion virtuálního switche. Tento switch nám zabezpečuje pásmo pro komunikaci a přesun dat nástroje vMotion mezi jednotlivými ESX servery. Jedná se o switch typu VMkernel. Lépe je nastavení síťového připojení vidět na obr. 14 – vpravo vidíme fyzický adaptér hosta a vlevo všechny sítě, do kterých je připojen.




Obr. 14 – Síťové nastavení ESX serveru s podporou funkce vMotion [Obr. 14]

## 5.6 *Migrace virtuálního stroje*

Provedení migrace je velice jednoduché. Stačí označit virtuální stroj, který chceme migrovat, stisknout pravé tlačítko a vybrat volbu Migrate. Vyskočí nám nabídka, jakou migraci chceme provést. Na výběr máme migraci mezi úložišti, migraci mezi ESX servery nebo migraci obojího, ovšem pro tuto volbu musí být virtuální stroj vypnutý.



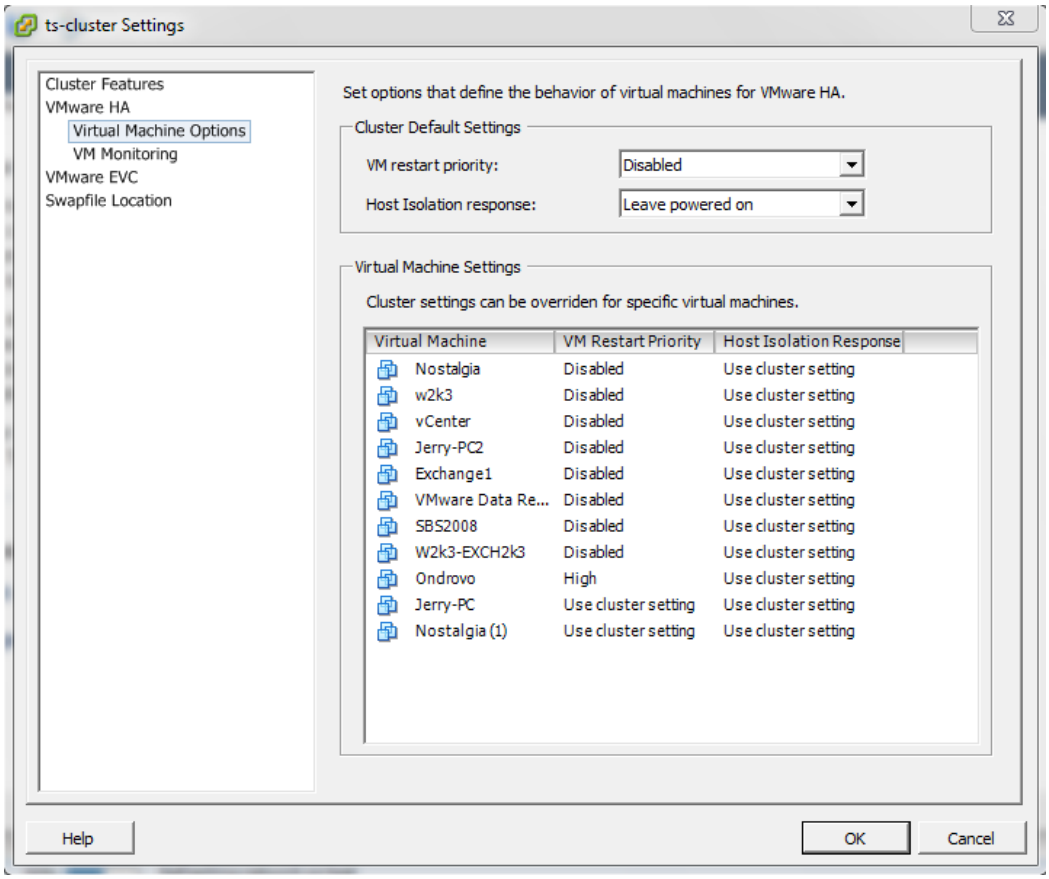

Obr. 15 – Výběr typu migrace [Obr. 15]

Po vybrání typu migrace nás průvodce migrací vyzve k vybrání cílového místa podle zvoleného typu migrace. Po vybrání a potvrzení již proběhne samotná migrace.

V případě migrace mezi ESX servery je ještě nutné vybrat, zda si má vMotion alokovat systémové prostředky pro svůj chod, či zda má využívat volné systémové prostředky.

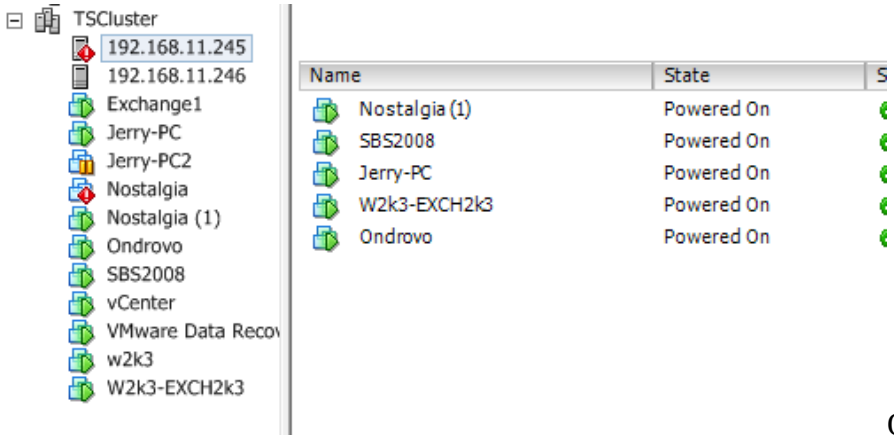
## 5.7 Simulace výpadku ESX serveru

Pro otestování bezpečnostního incidentu, který bude mít za následek výpadek jednoho z ESX hostů, a tím výpadek důležité služby, demonstrované v tomto případě virtuálním strojem Ondrovo, jsem vybral výpadek proudu – prosté odpojení hosta od zdroje elektrické energie. Vypadnuvším serverem byl ESX1-245 a automatický restart byl nastaven jen pro stroj Ondrovo – viz obr. 16.



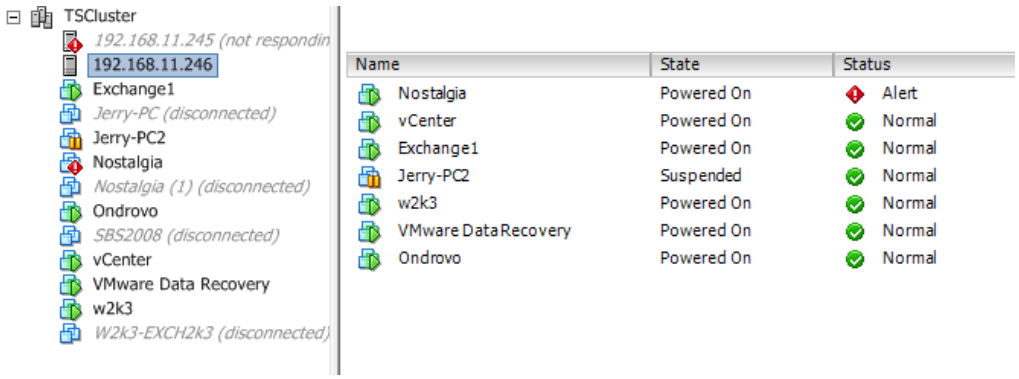

Obr. 16 - Nastavení priorit restartu jednotlivých virtuálních strojů. [Obr. 16]

Po vytáhnutí kabelu měla tedy VMware High Availability sama po krátké době zrestartovat virtuální stroj Ondrovo na druhém ESX serveru ESX2-246. Výchozí stav ilustruje obr. 17.




Obr. 17 – Výchozí stav před simulovaným výpadkem [Obr. 17]

Po vytažení kabelu trvalo přibližně 15 sekund, než High Availability zjistila, že host ESX1-245 není dostupný. Okamžitě se začal stroj Ondrovo restartovat na druhém, stále běžícím ESX hostu, na serveru ESX2-246. Výsledný stav zobrazuje obr. 18.




Obr. 18 - Výsledný stav po simulovaném výpadku. [Obr. 18]

# Závěr

Nastupující fenomén virtualizace pohled na řízení kontinuity činností v oblasti informačních systémů opravdu značně mění. Stále více a více podniků i státních organizací nahrazuje svoji stávající infrastrukturu infrastrukturou virtuální, protože vidí převažující pozitiva, která tato technologie přináší. Vždyť snížení nákladů na provoz, zjednodušení správy či zvýšení dostupnosti je v zájmu každé společnosti, která provozuje nějaký informační systém s jen trochu složitější infrastrukturou. Jak jsem již zmínil, je to právě zjednodušení správy a snížení počtu fyzických serverů, které velmi zjednodušují implementaci technik řízení kontinuity činností ve společnosti. Díky tomu je implementace této součásti řízení bezpečnosti informačního systému reálná i pro menší subjekty. Pro subjekty větší je to, troufnu si prohlásit, téměř nutnost, protože každý výpadek důležité služby bývá v dnešní době v praxi spojen s ohromnou finanční ztrátou.

Produkt společnosti VMware, vSphere 4 mne jednoznačně přesvědčil o tom, že je užitečný a že se jeho implementace ve firmě rozhodně vyplatí. Pokud se podaří produktu vytvořit vhodné hardwarové prostředí a dobře ho nakonfigurovat, není téměř vůbec nutné se o něj starat. Systém je robustní a má mnoho užitečných nástrojů, které ušetří administrátorovi minimálně polovinu času stráveného správou tohoto systému.

Stálé oblíbenější se stává kombinace využití virtuálního prostředí a dnes velmi moderních blade-serverů – serverů, které mají společnou napájecí, klimatizační a většinou síťovou část a které jsou snadno škálovatelné díky jednoduchému přidávání jednotlivých žiletek – bladů. Dalším využití vizualizovaných řešení se jeví tzv. cloud computing, kde dostupnost služeb hraje klíčovou roli, a tudíž i tam je řízení kontinuity činností velice důležitou oblastí. Doufám, že i tato práce přispěla alespoň částečně k potvrzení této důležitosti.

# Seznam použité literatury


[1] DOUCEK, P. -- SVATÁ, V. -- NOVÁK, L. *Řízení bezpečnosti informací.* Praha: Professional Publishing, 2008. ISBN 978-80-86946-88-7.

[2] RUEST, Danielle, RUEST Nelson. Virtualizace: Podrobný průvodce. Praha: Computer Press, 2010. ISBN 9788025126769.

[3] *aec_rizeni_kontinuity_cinnosti.pdf* http://www.aec.cz/download.php?f=6537fccedf2ea324b3f04d736d9a62a7 [cit. 2010-05-01].

[4] *Wikipedia, the free Encyclopedia:* Business continuity planning. http://en.wikipedia.org/wiki/Business_continuity_planning [cit. 2010-05-01].

[5] *BS25999.com:* BS25999 BCMS summary. http://www.bs25999.com/2009/12/bs25999-bcms-summary/ [cit. 2010-05-01].

[6] AEC – Řízení kontinuity činnosti. http://www.aec.cz/cz/sluzby/rizeni-kontinuity-cinnosti [cit. 2010-05-01].

[7] *Microsoft virtualization:* Virtualization Case Studies. http://www.microsoft.com/virtualization/en/us/case-studies-switchers.aspx#Mamut [cit. 2010-05-01].

[8] *Wikipedia, the free Encyclopedia:* Virtualization. http://en.wikipedia.org/wiki/Virtualization [cit. 2010-05-01].

[9] VLČEK, Michal. *Virtualizace stanic*. Praha, 2009. 53 s. Bakalářská práce. Vysoká škola ekonomická v Praze.

[10] Virtualizace na úrovni jádra operačního systému. http://www.abclinuxu.cz/clanky/system/virtualizace-na-urovni-jadra-operacniho-systemu [cit. 2010-05-01].

[11] VMware homepage. http://www.vmware.com/ [cit. 2010-05-01].

[12] VMware vMotion Datasheet. http://www.vmware.com/pdf/vmotion_datasheet.pdf [cit. 2010-05-01].

[13] LOWE, Scott. *Mastering: VMware vSphere 4*. Canada: Wiley Publishing, 2009. 673 s. ISBN 978-0-470-48138-7.

[14] VMware High Availability Datasheet. http://www.vmware.com/files/pdf/ha_datasheet.pdf [cit. 2010-05-01]

[15] VMware DSR Datasheet. http://www.vmware.com/files/pdf/drs_datasheet.pdf [cit. 2010-05-01].

[16] VMware Data Recovery Datasheet. http://www.vmware.com/files/pdf/data_recovery_datasheet.pdf [cit. 2010-05-01].

[17] DOSTUPNOST = BEZPEČNOST?. http://www.netguru.cz/10/04/2-odolnost-a-vysoka-dostupnost-ip-siti/dostupnost-a-nedostupnost.html [cit. 2010-05-01].

# Seznam obrázků

[Obr. 1] *Životní cyklus BCM* http://www.analytix.co.za/Portals/0/Diagrams/Training---Business-Continuity-Management-Diagram.jpg

[Obr. 2] *Názorná schematická ukázka virtualizace* http://www.pds-site.com/vmware/images/ws_arch.gif

[Obr. 3] *Princip clusterů* http://www.vmware.com/files/pdf/VMwareHA_twp.pdf

[Obr.4] *Princip funkce VMware High Availability* http://www.vmware.com/files_inline/images/DGRM_vSphere_HighAvailabillity.gif

[Obr. 5] *Princip nástroje VMware DRS* http://www.vmware.com/files/pdf/drs_datasheet.pdf

[Obr. 6] *Princip funkčnosti nástroje VMware DRM* http://www.vmware.com/files/pdf/drs_datasheet.pdf

[Obr. 7] *Proces tvorby zálohy pomocí nástroje VMware Data Recovery* http://www.vmware.com/files/pdf/data_recovery_datasheet.pdf

[Obr. 8] *Obnovení dat pomocí nástroje VMware Data Recovery* http://www.vmware.com/files/pdf/data_recovery_datasheet.pdf

[Obr. 9] *Vytvoření nového clusteru.* Vytvořeno autorem pomocí funkce PrintScreen

[Obr. 10] *Nastavení funkce High Availability.* Vytvořeno autorem pomocí funkce PrintScreen

[Obr. 11] *Nastavení funkce VMware DRS.* Vytvořeno autorem pomocí funkce PrintScreen

[Obr. 12] *Schéma testovacího prostředí.* Vytvořeno autorem v program Microsoft Visio 2003

[Obr. 13] *Nastavení masky CPU.* Vytvořeno autorem pomocí funkce PrintScreen

[Obr. 14] *Síťové nastavení ESX serveru s podporou funkce vMotion.* Vytvořeno autorem pomocí funkce PrintScreen

[Obr. 15] *Výběr typu migrace.* Vytvořeno autorem pomocí funkce PrintScreen

[Obr. 16] *Nastavení priorit restartu jednotlivých virtuálních strojů.* Vytvořeno autorem pomocí funkce PrintScreen

[Obr. 17] *Výchozí stav před simulovaným výpadkem.* Vytvořeno autorem pomocí funkce PrintScreen

[Obr. 18] *Výsledný stav po simulovaném výpadku.* Vytvořeno autorem pomocí funkce PrintScreen