Technická univerzita v Liberci
Fakulta strojní

DIPLOMOVÁ PRÁCE

Návrh, implementace a správa podnikového bezpečného úložiště dat

Proposal, implementation and administration of secure data storage in company environment

Liberec 2008

Marek Pažout

TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta strojní

Katedra aplikované kybernetiky Studijní rok: 2007/08

ZADÁNÍ DIPLOMOVÉ PRÁCE

Jméno a příjmení: **Marek PAŽOUT**
Studijní program: **M2301 Strojní inženýrství**

Obor: **3902T021 Automatizované systémy řízení v strojírenství**

Zaměření: **Automatizace inženýrských prací**

Ve smyslu zákona č. 111/1998 Sb. o vysokých školách se Vám určuje diplomová práce na téma:

Návrh, implementace a správa podnikového bezpečného úložiště dat

Zásady pro vypracování:
(uveďte hlavní cíle diplomové práce doporučené metody pro vypracování)

1. Seznamte se s problematikou zálohování a virtualizace dat
2. Popište současný stav a navrhněte komplexní řešení zálohování dat podle klíčových požadavků společnosti Denso Manufacturing Czech s.r.o.
3. Navrhněte a popište technickou i aplikační realizaci včetně prostředků administrace
4. Zhodnoťte vypracované řešení z hlediska zálohovacího okna, nepředvídatelného poškození dat a scénáře pro tzv. „Disaster Recovery", kdy dojde ke kompletní havárii datového centra

TECHNICKÁ UNIVERZITA V LIBERCI

Fakulta strojní

Jméno a Příjmení: Marek Pažout

Studijní obor : M2301 Strojní inženýrství - automatizované systémy řízení ve strojírenství

Zaměření : Automatizace inženýrských prací

Katedra aplikované kybernetiky

Návrh, implementace a správa podnikového bezpečného úložiště dat

Proposal, implementation and administration of secure data storage in company environment

Vedoucí diplomové práce : prof. Ing. Miroslav Olehla, CSc.

Technická univerzita v Liberci

Rozsah diplomové práce:

Počet stran.....59

Počet příloh..... 1

V Liberci dne 16.5.2008

Poděkování

Děkuji vedoucímu diplomové práce panu prof. Ing. Miroslavu Olehlovi, CSc. za odborné vedení a pomoc při zpracování diplomové práce a Ing. Markovi Čalounovi za odborné konzultace a praktické připomínky při realizaci.

ANOTACE

Technická univerzita v Liberci

Fakulta strojní

Katedra aplikované kybernetiky

Studijní obor :	M2301 Strojní inženýrství - automatizované systémy řízení ve strojírenství
Studijní zaměření :	Automatizace inženýrských prací
Diplomant :	Marek Pažout
Téma práce :	Návrh, implementace a správa podnikového bezpečného úložiště dat
Theme of work :	Proposal, implementation and administration of secure data storage in company environment
Rok obhajoby DP :	2008
Vedoucí DP :	prof. Ing. Miroslav Olehla, CSc.

ANOTACE:

Tato diplomová práce se zabývá problematikou zálohování a obnovy dat v podnikovém prostředí. V teoretické části diplomové práce jsou popsány možnosti a způsoby ukládání dat a technologie virtualizace zdrojů. Praktická část diplomové práce obsahuje návrh komplexního řešení zálohovacího systému a jeho implementaci včetně popisu technické i aplikační části.

ANOTATION:

The diploma thesis focus on data backups and recovery in company environment. The theoretical part contains a description of alternatives and methods used for data backups and recovery, technologies of resource virtualization. The practical part contains proposal for a complex solution of data backup system and it's implementation including description of technical and application part.

Místopřísežné prohlášení

„ Místopřísežně prohlašuji, že jsem diplomovou práci vypracoval samostatně s použitím uvedené literatury.“

V Liberci 16. 5. 2008

Marek Pažout

OBSAH

1. ÚVOD

Dnešní elektronická éra se vyznačuje především neustále rostoucím objemem dat a tedy i vyššími nároky na úložnou kapacitu. Informační systémy produkují obrovské množství dat, které je nutno uchovávat a chránit proti znehodnocení. Například veškerá obchodní korespondence, projektová dokumentace, plánování výroby nebo data pro zákaznické audity dnes prakticky existují pouze v elektronické podobě, takže bez potřebného zálohování hrozí ztráta těžko nahraditelných dat. Navíc se nejedná pouze o data, která potřebuje jen samotná organizace ale o spoustu dat, o něž se musí postarat podle předpisů pro nejrůznější úřady (finanční úřad, správa sociálního zabezpečení, zdravotní pojišťovny apod.), a to po různě dlouhou dobu. Obecně se jedná o informace finančního rázu, účetnictví, výkazy majetku, údaje o zaměstnancích apod., jejichž ztráta v případě nedostatečného nebo špatně zvoleného zálohovacího procesu může být skutečnou katastrofou.

Zálohovací proces musí navíc probíhat velice rychle a také podle vhodné strategie, protože v podnicích už dnes nebývá dlouhá doba nečinnosti, kdy podnikový systém není v provozu a data se mohou dlouhou dobu zálohovat, například v noci nebo o víkendech, neboť často je nezbytně nutné plně fungovat v režimu 24 hodin denně, 7 dní v týdnu.

Existují zde i další požadavky, které musí aplikované zálohovací řešení splňovat, jmenujme například :

- schopnost přizpůsobit se stále rostoucímu objemu dat
- eliminace odstávek aplikací z důvodu vytvoření skutečně plně konzistentních záloh
- snížení pořizovacích nákladů na implementaci a provoz robustního řešení
- automatizace zálohovacích procesů

Kritéria při návrhu zálohovacího řešení jsou mnohdy značně variabilní. Záleží na použité platformě, provozovaných aplikacích a hlavně na způsobu a úrovni ochrany

aplikačních dat. V případě tzv. Disaster Recovery scénáře pro obnovení chodu systémů po kompletní havárii datového centra je dnes minimálně vhodné zvážit mnohé výhody, které přinášejí moderní disková pole a především velice výkonná technologie Fibre Channel v rámci sítí typu SAN. Výsledné procesy zálohování a Disaster Recovery scénáře poté bývají výrazně výkonnější, flexibilnější a lépe škálovatelné.

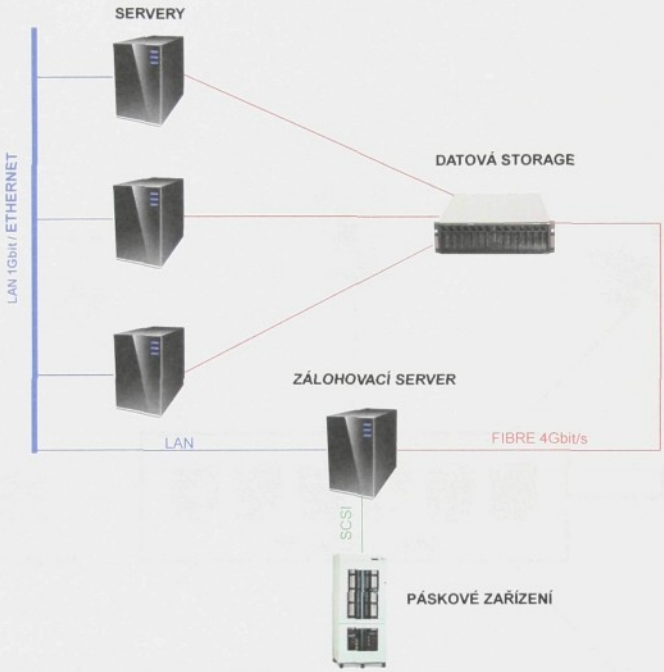
1.1. Představení DENSO MANUFACTURING CZECH s.r.o.

DENSO MANUFACTURING CZECH s.r.o. nacházející se v liberecké Průmyslové zóně – Jih je dceřinou firmou japonské nadnárodní společnosti DENSO CORPORATION, která vlastní 100% jejího základního jmění. DENSO sídlí v japonském městě Kariya, v prefektuře Aichi. Je předním světovým dodavatelem moderních technologií, systémů a jejich součástí. V oborech klimatizace, řídících systémů motorů, elektroniky, kontroly řízení a bezpečnosti silničních vozidel, stejně jako v oborech informatiky a komunikace spolupracuje DENSO s hlavními výrobci automobilů po celém světě. Své patentově chráněné technologie a poznatky v odvětví průmyslových systémů a klimatizace využívá DENSO i mimo automobilový průmysl. V současnosti zaměstnává přibližně 112 tisíc zaměstnanců v 32 zemích světa včetně Japonska.

Hlavním výrobním programem společnosti DENSO MANUFACTURING CZECH s.r.o. je výroba klimatizačních jednotek pro osobní automobily a jejich příslušenství (topná tělesa, kondenzátory a chladiče). Zákazníky jsou přední evropské automobilky – VW, BMW, Daimler Chrysler, Škoda Auto, Lamborghini, TPCA Kolín, Suzuki, NedCar a Mercedes Benz. V současnosti má firma 1800 zaměstnanců a její plánovaný obrat pro rok 2007 činí 7,1 mld.Kč

1.2. Výchozí Stav

Z potřeb společnosti DENSO MANUFACTURING CZECH vznikl požadavek na komplexní řešení nevyhovujícího mechanismu zálohování dat. Klíčovými problémy byly dlouhodobě neudržitelný stav zálohovacího procesu a fyzická odolnost dat.



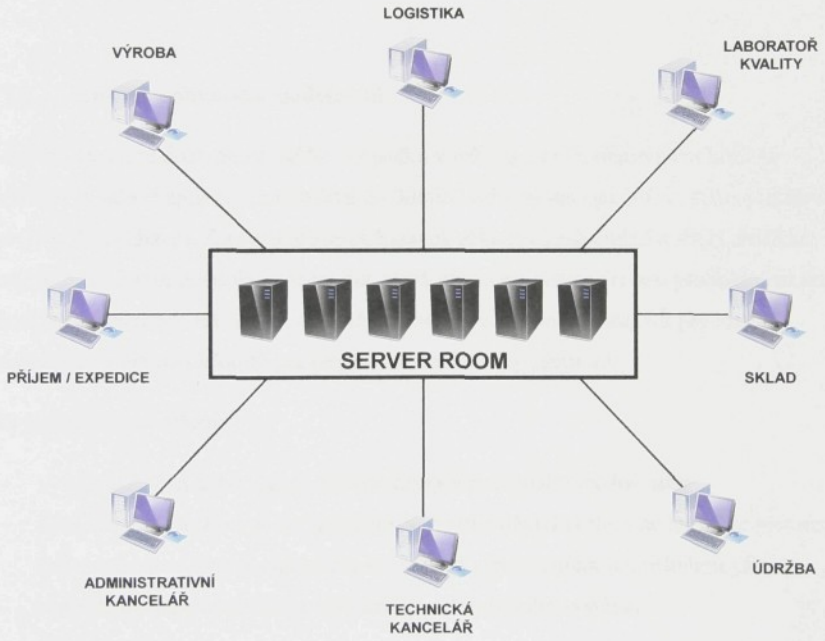
Obr. 1.: Výchozí stav datového centra (server room)

Zálohovací proces :

- periodická každodenní plná záloha (cca 1TB dat) na páskové zařízení prostřednictvím sítě LAN
- proces zálohy iniciuje softwarový agent nainstalovaný na každém serveru
- parametry : záloha 1GB/min, obnova 500MB/min

Výchozí infrastruktura :

- aplikační IBM xSeries servery propojeny 1Gbit Ethernetem (síť typu LAN) k zálohovacímu serveru
- pásková jednotka připojená přes rozhraní SCSI k zálohovacímu serveru,
- datová storage (diskové pole) IBM DS 4300 připojená k aplikačním serverům a zálohovacímu serveru prostřednictvím 4Gbit Fibre Channel technologie (síť typu SAN)



Obr. 2: Výchozí Topologie

Problematické aspekty výchozího stavu:

- systém zálohování a obnovy dat nevyhovuje požadavku na rychlou obnovu kritických dat SQL databáze
- nevyhovující dostupnost dat pro nepřetržitý režim 24x7
- značná zátěž LAN sítě a serverů při zálohovaní dat
- obtížná správa serverů
- v případě havárie serverové místnosti nedostupnost IT systému a dat
- vyzářené teplo servery a jejich vysoké energetické nároky
- nutnost licencování zálohovacího software (agenta) pro každý fyzický server – drahé

1.3. Klíčové požadavky společnosti

Zajistit vysokou dostupnost dat bez výpadku v režimu 24x7 a obnovu dat kritické logisticko- skladové aplikace maximálně do 30min (velikost dat cca 20GB, plus aplikační server a SQL databáze). Zároveň je zde požadavek zákaznických auditů a ISO certifikací zajistit bezpečné a dlouhodobé uložení dat, která přímo souvisí s výrobou produktu zákazníka (zpětná dohledatelnost, reklamace atd.) Do budoucna je nutné také zajistit provoz IT infrastruktury v záložní lokalitě pro případ selhání lokality primární.

Další požadavky na řešení:

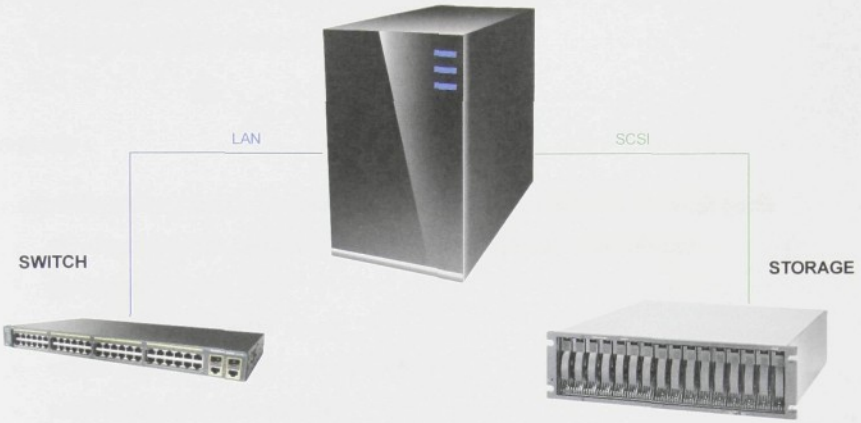
- využití stávající heterogenní infrastruktury v maximální možné míře
- konsolidace a snížení počtu fyzických serverů z důvodu omezené kapacity serverové místnosti a problému s chlazením serverů díky narůstajícímu tepelnému záření
- centralizovaná a intuitivní správa celého zálohovacího systému
- rychlá implementace
- bez navýšení počtu zaměstnanců IT oddělení

2. TEORETICKÁ VÝCHODISKA

Tato kapitola má za cíl poskytnout soubor informací pro seznámení s řadou klíčových technologií a výrazů z oblasti ukládání dat zmiňovaných nejenom v úvodní části,ale především později v části experimentální. Postupně jsou popsány a zhodnoceny topologie jednotlivých typů datových úložišť (DAS/NAS/SAN), dále problematika virtualizace serverů a úložných zařízení, princip tzv. Clusteru a protokol Fibre Channel.

2.1. DAS – Direct Attached Storage

Nejstarší řešení spočívající v připojení jedné či více úložných jednotek (typicky pevných disků) přímo k hostitelskému systému (serveru). Mezi DAS zařízení můžeme zařadit např. interní disky samotné serveru nebo jednoduché diskové pole postavené zpravidla na technologii SATA nebo SCSI disků připojených k serveru buď technologií SCSI nebo Fiber Channel v konfiguraci Point-to-Point. Pod DAS spadají i externí zálohovací zařízení typu páskových mechanik připojených přímo k serveru.



Obr. 3.: Direct Attached Storage

Využitá rozhraní a protokoly :

DAS systémy obvykle využívají rozhraní SCSI, ATA, SATA, IEEE 1394 nebo protokoly iSCSI a Fibre Channel. Disková pole v současné době používají především rozhraní Ultra160 SCSI a Ultra320 SCSI

Zálohování :

DAS jednotky umožňují zálohování z jednoho jejich disku na druhý bez účasti serveru. Pokud se zálohování provádí na jiné zařízení je nutné využívat služby serveru. V případě zálohování *na jiné místo v síti, je provoz sítě zpomalován přenosem zálohovaných dat* (provádí se po celých souborech) a tím může být nepříznivě ovlivněn chod či odezva podnikových aplikací.

Výhody :

- levné a dostupné řešení
- snadná údržba
- jednoduchá implementace

Nevýhody :

- škálovatelnost je značně omezena počtem volných EIDE/SATA/SCSI portů
- při výpadku serveru nedostupnost všech přímo připojených zařízení
- obtížné sdílení dat
- decentralizovaná správa zdrojů
- zálohovaní a obnova dat přes síť LAN
- nespolehlivost v režimu 24/365

V případě použití diskového pole je základním bezpečnostním konfigurace diskového pole pomocí technologie RAID.

Technologie RAID (Redundant Array of Independent Disks)

Touto technologií rozumíme seskupení dvou nebo více disků, které se tváří na straně serveru jako jedna logická jednotka. Většinou se jedná o zařízení s jednoduchou správou pomocí webového rozhraní. V dnešní době jsou nejrozšířenější seskupení disků v RAID 5, kdy se konfigurace skládá z datových disků a jednoho paritního disku. V poslední době se začíná u většiny výrobců diskových polí objevovat seskupení disků v RAID 6 , kdy konfigurace obsahuje datové disky a dva paritní disky. Disková pole tohoto typu bývají často vybavena funkcionalitou tzv. Hot-spare disku, který v případě havárie jakéhokoliv disku v diskovém poli zastoupí jeho funkci. Ztracená data jsou doplněna z redundantních kontrolních součtů vytvářených RAID kontrolerem, bohužel po dobu „dopočítávání" dat je výkon diskového pole znatelně snížený.

RAID 5

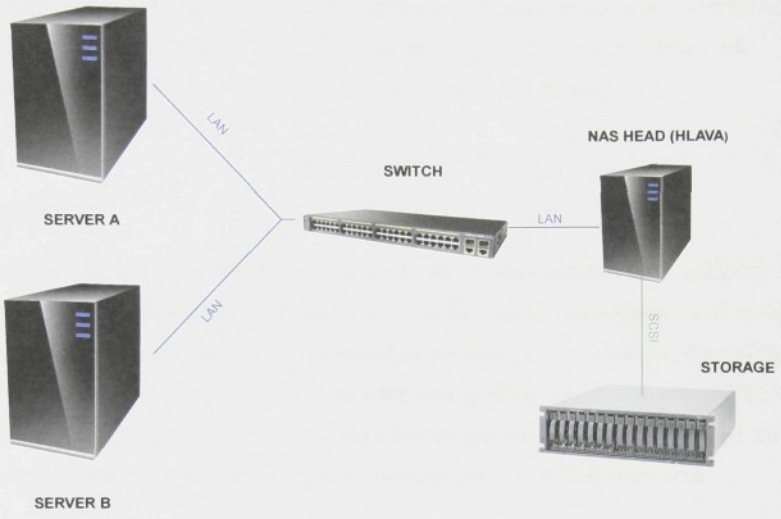
Paritní data jsou uložena střídavě na všech discích a ne pouze na jednom. Výhodou je, že jen jeden disk (i když pokaždé jiný) obsahuje redundantní informace a opět se dá využít paralelního přístupu k diskům, čímž se zkrátí doba odpovědi. Nevýhodou RAID 5 je ale pomalejší zápis.

RAID 6

Obdoba RAID 5, používá dva paritní disky, přičemž na každém z nich je parita vypočtena jiným způsobem. Opět kvůli přetížení paritních disků jsou paritní data uložena střídavě na všech discích. Výhodou je odolnost proti výpadku dvou disků. Rychlost čtení je srovnatelná s RAID 5, ale zápis je pomalejší než u RAID 5, právě díky výpočtu dvou sad paritních informací.

2.2. NAS – Network Attached Storage

Síťové úložné prostředky (NAS) vycházející z původní myšlenky souborových (file) serverů. Jedná se o specifická jednoúčelová zařízení pro ukládání dat připojená přímo do počítačové sítě. Tyto zařízení mají přiřazenou IP adresu a mohou tedy být dostupná klientům skrz jiný server, který působí jako brána k datům, nebo lze klientům povolit přímý přístup k datům bez nutnosti serveru jako prostředníka.



Obr. 4.: Network Attached Storage

Využitá rozhraní a protokoly :

Zařízení NAS se typicky připojuje prostřednictvím switche do TCP/IP LAN sítě (Ethernet, FDDI, ATM). Přenos dat je možné uskutečnit pomocí různých protokolů, obvykle se používají Common Internet File System (CIFS) pro Windows, Network File System (NFS) pro UNIX, Server Message Block (SMB) pro Windows, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) nebo AppleTalk pro Apple. NAS zařízení je možné ovládat přes vzdálený přístup, webovské rozhraní nebo prostřednictvím software přímo od výrobce.

Zařízení NAS zpravidla obsahuje jen zabudovaný (embedded) jednoúčelový operační systém optimalizovaný především pro rychlý přístup k souborům a jejich vyhledávání. NAS zařízení se skládá z tzv. NAS hlavy nebo též tzv. NAS boxu, která představuje rozhraní mezi

samotným diskovým zařízením a počítačovou sítí. NAS hlava řídí souborový systém na diskových zařízeních. Klient (stanice nebo server) se připojuje na NAS hlavu, která má přidělenu IP adresu. NAS hlava převezme požadavek od klienta, zpracuje ho a získá data z diskového pole. Tyto data poté NAS hlava pošle zpět klientovi. Tím je zajištěna plná transparentnost - klientovi se celé NAS zařízení jeví jako jeden fyzický disk.

Zálohování :

Záloha v rámci jedné NAS jednotky probíhá zcela interně, data neopustí NAS jednotku a tedy nezatěžují počítačovou síť. V případě zálohy na jiné zálohovací zařízení, které se nachází na jiném místě v síti, jsou všechna zálohovaná data posílána přes síť LAN, čímž se snižuje její výkonnost. Aby při zálohování nebyla příliš zatěžována počítačová síť, řeší některá NAS zařízení tento problém přímým výstupem na páskovou jednotku, případně oddělenou sítí s páskovou jednotkou. Stejně jako u DAS se záloha provádí po celých souborech

Výhody :

- snadná implementace a rozšiřitelnost
- nízké náklady na údržbu a správu
- výpadek serveru neznamená nedostupnost dat
- emulace souborových služeb operačních systémů a široká podpora přenosových protokolů
- centralizovanost, všechna NAS zařízení mohou být na jednom místě

Nevýhody :

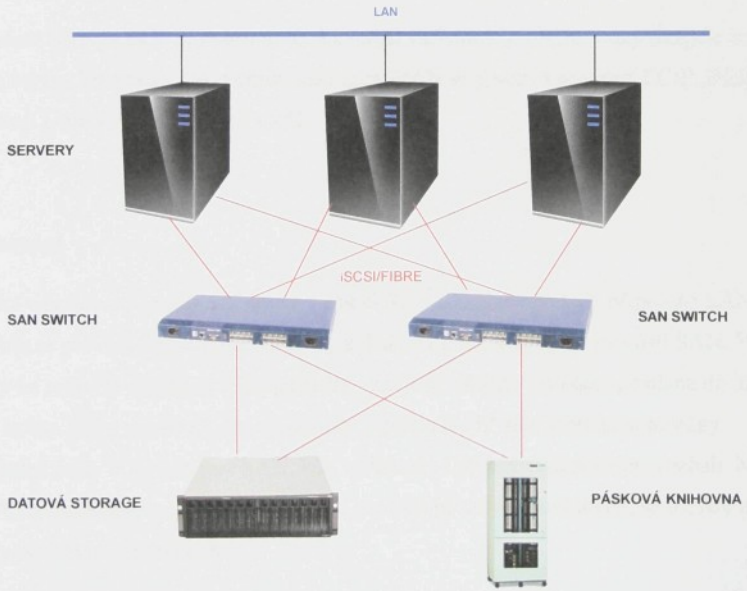
- v případě velkého počtu NAS zařízení značně komplikovaná administrace
- značné zatížení podnikové LAN sítě především při zálohování velkých objemů dat

2.3. SAN – Storage Area Networks

Nejmodernějším způsobem bezpečného a spolehlivého ukládání dat je Storage area network. SAN splňují řadu aktuálních IT požadavků na datová úložiště jako je například exponenciální růst diskové kapacity, řeší problém co nejefektivnějšího nasazení zálohovacích zařízení a jejich centrální správu a poskytují robustní základ plně vyhovující požadavku vysoké dostupnosti dat v režimu 24x7.

Topologie sítí SAN se od tradičního schématu DAS nebo síťových úložišť typu NAS zásadně liší především v následujících bodech :

- storage zařízení není přímo propojena se síťovými klienty
- storage zařízení není přímo propojena se serverem (servery)
- každé storage zařízení je propojeno (pomocí technologie přepínání) s každým serverem



Obr. 5.: SAN – Storage Area Network

Jedná se o oddělenou vysokorychlostní plně duplexní síť, nezávislou na podnikovém intranetu, specificky zaměřenou na propojení zálohovacích zařízení, která jsou mezi sebou navzájem propojena s (typicky) servery v clusteru, představujících přístupový bod do SAN. Oddělené sítě přispívají ke snazšímu zálohování i dostupnosti dat a k lepší bezpečnosti uložených dat, protože data mohou být chráněna mimo jiné i tím, že se mohou nacházet daleko od fyzického umístění podniku. SAN umožňuje zrcadlení disků (mirroring), zálohování a obnovu, migraci dat mezi jednotlivými úložnými zařízeními a také sdílení dat mezi různými servery v síti.

V rámci SAN je možné sdílet jednotlivá média, ať jsou to třeba virtuální logické disky nebo páskové knihovny. To se hodí například při budování clusterů, filesystémů na kterých požadujeme paralení operace a nebo LAN-less zálohování, kdy veškerý objem dat zálohujeme přes SAN síť a významně tím šetříme provoz na LAN síti.

Využitá rozhraní a protokoly :

Základem SAN je FCP protokol a FC. Levnější variantou je iSCSI, který funguje na Gigabitovém Ethernetu. Pro komunikaci přes WAN se používá protokol FCIP. Disková pole používají Ultra320 SCSI nebo FC-AL.

Zálohování :

Lokální zálohování se provádí pouze v rámci SAN a nezatěžuje tedy připojené LAN sítě. Obvykle se provádí na páskové jednotky a disková pole, která jsou součástí SAN. V případě zálohy na zařízení umístěné v geograficky vzdálené lokalitě jsou data posílána do lokální FCIP brány, která zabalí FC rámce do rámců příslušné IP sítě, které jsou poslány prostřednictvím WAN do jiné SAN, kde vzdálená FCIP brána rámce opět rozbalí. Na rozdíl od NAS a DAS, kde se proces zálohování provádí po celých souborech, se u SAN provádí záloha po diskových blocích.

Výhody :

- oddělení od podnikové LAN sítě
- definice redundantních cest ke zdrojům
- centralizovanost
- škálovatelnost
- rychlost (především v případě technologie Fibre Channel)
- možnosti zálohování a podpora Disaster Recovery lokalit

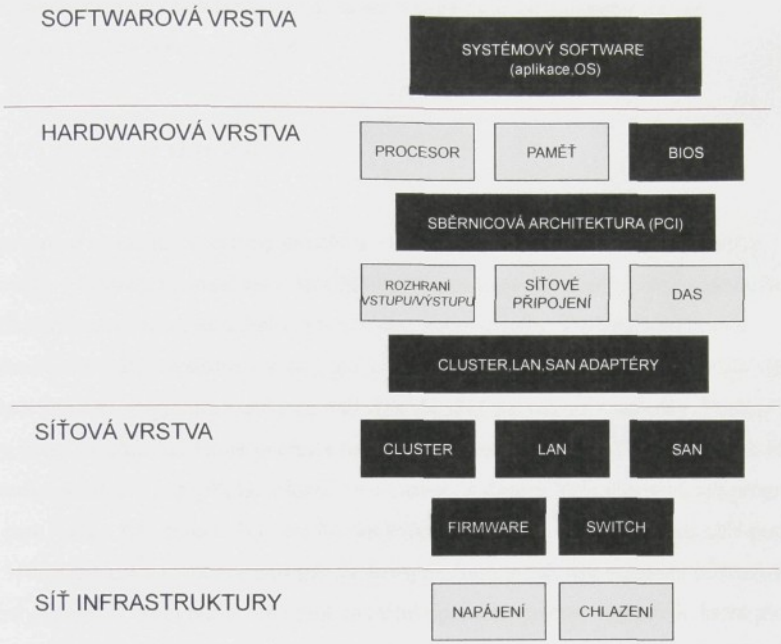
Nevýhody :

- pořizovací cena SAN prvků

2.4. Virtualizace

Pod pojmem virtualizace se v IT oboru obvykle rozumí uspořádání, ve kterém je možné k veškerým systémovým zdrojům přistupovat jako k souboru výkonu bez ohledu na jejich fyzické charakteristiky, pomocí kterých k nim uživatelé obvykle přistupují. Například pojem "server" se tak už neomezuje svou fyzickou konfigurací, ale pouze skupinou dostupných zdrojů hostitele (CPU, paměť ...) Virtualizace potom umožňuje na jednom fyzickém hostitelském serveru provozovat více serverů virtuálních. Dalším příkladem virtualizace je technologie RAID, která umožňuje zapojení několika fyzických disků, navenek se tvářících jako jediný virtuální disk, přičemž nabízí vyšší rychlost či odolnost proti chybám.

Každé IT centrum je složeno z několika vrstev :



Obr. 6.: Skladba IT centra

Primární myšlenkou virtualizace je vytvoření adaptivního centra, které umožňuje sdílet jakýkoliv zdroj prostřednictvím virtualizační vrstvy.

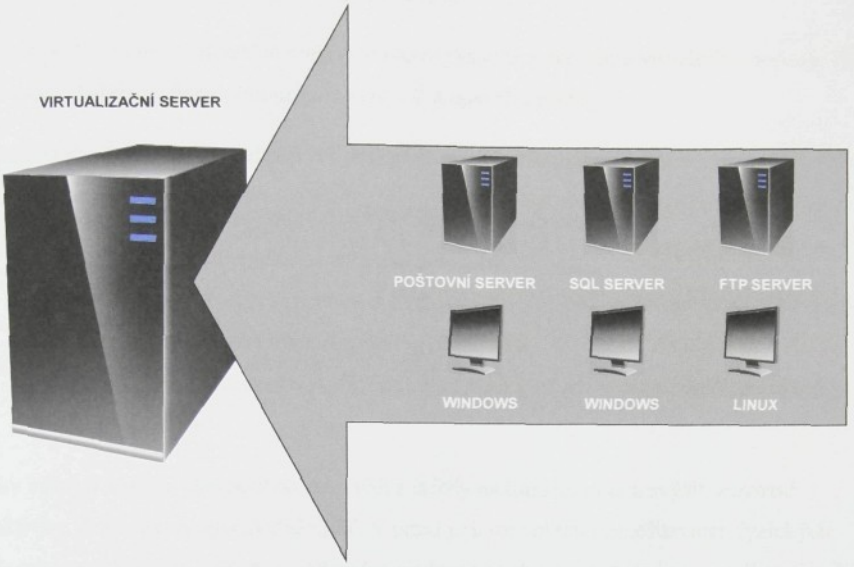
Serverová i storage virtualizace pracuje velmi obdobným způsobem.

Virtualizace zabírá fyzické hardwarové prostředky, tyto prostředky sdružuje dohromady a následně rozděluje podle potřeb daných aplikací. Mezi hlavní přednosti virtualizace zdrojů patří :

- flexibilita (zdroje je možné přesunovat podle potřeb)
- škálovatelnost, dynamické přiřazování
- snadný management
- zjednodušené zálohovaní a obnova dat včetně migrace a disaster recovery
- plně využitý potenciál zdrojů

2.4.1. Serverová virtualizace

Serverová virtualizace vytváří prostředí, ve kterém je množství virtuálních strojů aplikováno v poměru na malé množství fyzického hardware. Obecně to znamená vložení virtualizační vrstvy mezi samotný hardware a operační systém. Virtualizační vrstva přizpůsobuje architektonickou vrstvu počítače, nad kterou je vystavěna, a poskytuje vhodné prostředí pro běh programů, které jsou nad virtualizační vrstvou provozovány. Pomocí této vrstvy, která emuluje hardware počítače nebo jeho určitou část (využitím skutečných HW prostředků počítače) je například možné provozovat na daném fyzickém systému programy, které jsou jinak s HW prostředky daného počítače neslučitelné. Při virtualizaci celé potřebné škály HW prostředků je možné nad stávajícím operačním systémem nejenom provozovat některé „nenativní" programy, ale i celé virtuální operační systémy. Prostředí, které provádí virtualizaci celého fyzického hardwaru a které se jeví programům, které nad ním běží, jako skutečné hardwarové prostředí, nazýváme virtuálním strojem. Virtuální stroj je tedy obraz počítače, který však existuje jen jako model uvnitř jiného počítače. Programy běžící uvnitř tohoto stroje se chovají, jako by běžely na skutečném počítači, ale přitom nemohou nijak ovlivnit zbytek „vnějšího" počítače.



Obr. 7.: Serverová virtualizace

Existuje řada přístupů k virtualizaci platformy :

1) Hardwarová virtualizace

Nejrozšířenější varianta virtualizace - správa a přiřazování hardwarových zdrojů jednotlivým virtuálním serverům. Virtualizační vrstva je umístěna mezi hardwarem a virtuálními servery. Tento typ virtualizace podporuje více operačních systémů na jednom fyzickém serveru.

2) Para-virtualizace

Podobná konceptu hardwarové virtualizace, pouze se snahou optimalizovat zátěž virtualizační vrstvy. Podporuje více operačních systémů na jednom serveru, ale operační systém musí být na tento způsob běhu připraven.

3) Virtualizace na úrovni operačního systému

Virtualizační vrstva je umístěna mezi operačním systémem serveru a virtuálními servery. Na jednom fyzickém serveru podporuje pouze jeden operační systém.

Virtualizační řešení na úrovní serverů poskytuje zejména následující vlastnosti:

- kompletní virtualizace od stolních počítačů až po serverové farmy
- řízení dostupnosti aplikací a automatizaci provozu
- jednoduché a rychlé poskytování dalších zdrojů (takzvaný rapid server provisioning)
- snadné přerozdělování výkonů a datových kapacit
- symetrický multiprocessing (přidělení více procesorů jednomu virtuálnímu stroji)
- vzdálená správa

Díky výše uvedeným vlastnostem lze snížit náklady na transformaci a zvýšit provozní efektivitu, flexibilitu a úroveň služeb IT. V praxi pak lze omezit počet hlavních fyzických serverů, konsolidovat jejich stav a případně sjednotit hardware na požadovaný výkon všech provozovaných aplikací. Je výhodnější využít menší počet podnikových serverů vyšší třídy a aplikace provozovat na oddělených virtuálních strojích. Nový hardware také zabezpečí lepší škálovatelnost a vyšší odolnost proti výpadku.

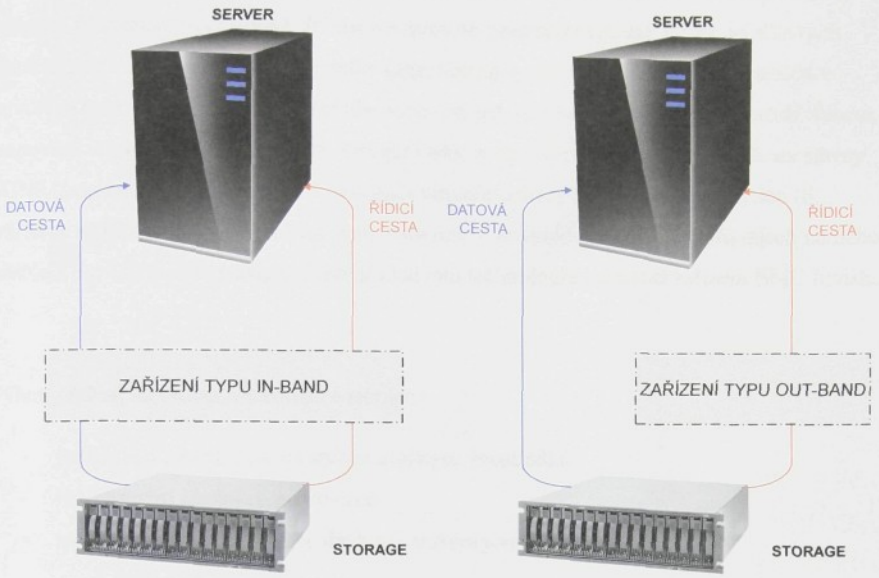
2.4.2. Virtualizace Storage (úložišti dat)

Neustále rostoucí objem podnikových dat staví IT administrátory do situace, kdy musí řešit dvě otázky: jak pořídit co nejlevněji další diskový prostor a co udělat se starším a mnohdy kapacitně nevyhovujícím datovým úložištěm. Pro většinu starších diskových polí je limitujícím prvkem jejich rozšiřitelnost a rychlost. Řešením tohoto stavu je zakoupení nových výkonnějších polí, která jsou schopna vyhovět současným požadavkům. Vzhledem k tomu, že velká disková kapacita v korporátních řešeních vyžaduje vysoké finanční náklady, lze využít starší pole i jako doplněk k novým. K tomu, abychom mohli používat starší datové kapacity souběžně s novými, slouží virtualizace.

Myšlenka storage virtualizace spočívá v konsolidaci úložných systémů, jako jsou například disková pole, od více poskytovatelů do jediného zasíťovaného prostředí, které může být následně spravováno jako jediný storage pool. Z hlediska uživatele je storage pool zásobník, ze kterého může požadovat jakékoliv množství diskového prostoru, až po určité stanovené maximum. Cílem zprostředkujících virtualizačních vrstev je řídit rozkouskovaný diskový prostor tak, že vypadá a chová se jako jeden připojený disk. Po sjednocení heterogenních síťových disků může administrátor zavést jednotnou politiku, která zahrne všechna datová úložiště. Častým řešením je poolové sdružení rychlých Fibre Channel disků pro aplikace vyžadující vysoký výkon při čtení a zápisu dat (typicky transakční databáze). Je také snazší implementovat jednotné zálohovací schéma. Virtuální rozhraní pomáhá zabezpečit, aby byla využívána celková kapacita zařízení pro ukládání dat rozmístěných po síti. Virtuální zásobník je navíc škálovatelný - přidání více disků je pro uživatele neviditelné.

Při virtualizaci se využívají většinou samostatné virtualizační kontroléry (servery), ale některá disková pole podnikové třídy mají tyto kontroléry již implementovány přímo výrobcem, zde hovoříme o tzv. Controller based virtualizaci. Virtualizační server je tak schopen na jedné straně připojit všechna úložná zařízení a na straně druhé je nabízet serverům jako diskovou kapacitu. To umožňuje složit jednu logickou jednotku (LUN) z disků umístěných v různých polích (a přesouvat data mezi diskovými poli bez nutnosti výpadku serveru) nebo rozšiřovat kapacitu logické jednotky při zapojení například nového diskového pole. Pro administraci systému má toto řešení hlavní výhody v jednotném ovládání a využití všech dostupných datových kapacit. Další výhodou je i snazší replikace dat, neboť virtualizace také odstraňuje potřebu plné redundance. Bez virtualizace úložných systémů musí IT oddělení obvykle kopírovat celé svazky z jednoho typu úložiště na jiný, aby zajistilo, že jsou všechna související data v jednom prostředí. Díky virtualizaci je jednodušší kopírovat částečná data, jako jsou snapshoty typu point-in-time a udržovat je propojená s celým souborem dat mezi fyzickými zařízeními.

Podle umístění virtualizační platformy přitom rozlišujeme u sítí typu SAN virtualizace typu in-band a out-of-band.Základní princip in-band i out-of-band virtualizace je stejný a spočívá v „odchytávání" I/O operací vydávaných servery, analýze FC paketů, přemapování adres a případně řadě dalších činností v závislosti na tom, jakou funkcionalitou je příslušné virtualizační zařízení vybaveno.



Obr. 8.: In-Band / Out-Band virtualizace

Virtualizace v síti In-Band, někdy označována jako symetrická, je realizována mezi server/host systémy a úložnými zařízeními. V tomto případě probíhá proces mapování, tj. překladu „virtuálních adres" (tj. těch, které používá server) na „reálné adresy" (tj. adresy disků v diskových polích) na virtualizačním serveru (kontroleru), které leží přímo na datové cestě mezi servery a datovým úložištěm, data tímto zařízením protékají a zařízení samo provádí jejich přesměrování. Je ideální pro použití jak heterogenních host systémů, tak i pro použití heterogenních úložných zařízení, a to s jednotným centrálním managementem. Umožňuje například on-line rozšíření prostoru, přidělování prostoru podle skutečných potřeb, snapshoty typu point-in-time, CDP žurnál, synchronní i asynchronní zrcadlení (a to také pro clustery) či duální cesty k úložným zařízením. Jako příklad této technologie lze uvést zařízení Falcon IPStor.

V případě out-of-band technologie, někdy označované jako asymetrické, probíhá proces mapování na zařízení, které samo leží vně datových cest mezi servery a virtuálním datovým úložištěm, to znamená, že samo neprovádí přesměrování dat, nýbrž po datových cestách pouze posílá příkazy programům (agentům) pracujícím na host-bus adaptérech v serverech nebo na switchích. Vlastní přemapování pak provádějí výše zmínění agenti. Proces mapování ve skutečnosti nepřekládá virtuální adresy na reálné diskové adresy, ale na adresy LUNů (Logical Unit Number), což jsou opět virtuální adresy oblastí představujících (tj. tvářících se jako) disky v diskovém poli. Toto řešení se využívá zejména v případech nutného oddělení dat od řídících příkazů. Jako příklad této technologie lze uvést zařízení EMC Invista.

Výhody řešení na úrovni virtualizace storage :

- jednotná a centralizovaná správa úložných prostředků
- lepší využití úložných prostředků
- snadná migrace a replikace dat bez narušení provozu

2.4.3. Virtualizační server (kontroler)

Virtualizační server je dedikovaný server pro práci s jednotlivými LUNy. Umožňuje propojení těchto logických jednotek od různých výrobců diskových úložišť a vytvářet vlastní virtuální jednotky, tzv. VLUN. Tyto jsou následně nabízeny serverům v prostoru SAN architektury. Hojně využívanou funkcionalitou, která dnes představuje základní bezpečnostní řešení v rámci podnikových dat, je vzdálená replikace dat, respektive mirroring. Tato replikace se provádí mezi controllery umístěných v různých lokalitách tvořících tzv. geografický cluster. Toto řešení je typické pro heterogenní SAN sítě, kde jsou jednotlivé lokality propojeny do jediné SAN sítě prostřednictvím technologie fibre channel (FC). Toto řešení představuje nejjednodušší formu zálohy dat - pomocí zrcadlení jsou ve dvou geograficky oddělených lokalitách stejná data.

2.5. Cluster

Častým termínem spojeným s virtualizací zdrojů je tzv. cluster. Jedná se obecně o skupinu počítačů nebo jiných zařízení (jednotlivě označovaných jako Node), obvykle vzájemně propojených počítačovou sítí, s cílem paralelního zpracování úlohy pro zvýšení výpočetního výkonu, nebo zvýšení spolehlivosti než by mohl poskytnout jediný počítač či zařízení. Koncovému uživateli se tato skupina několika propojených zdrojů jeví, jako kdyby používal zdroj jediný.

Výpočetní cluster

Výpočetní cluster (anglicky High-performance computing (HPC) clusters) slouží k zvýšení výpočetního výkonu pomocí více počítačů, které na výpočtu spolupracují. Tímto způsobem vznikne vysoce výkonný celek, který je mnohonásobně levnější, než jeden vysoce výkonný počítač.

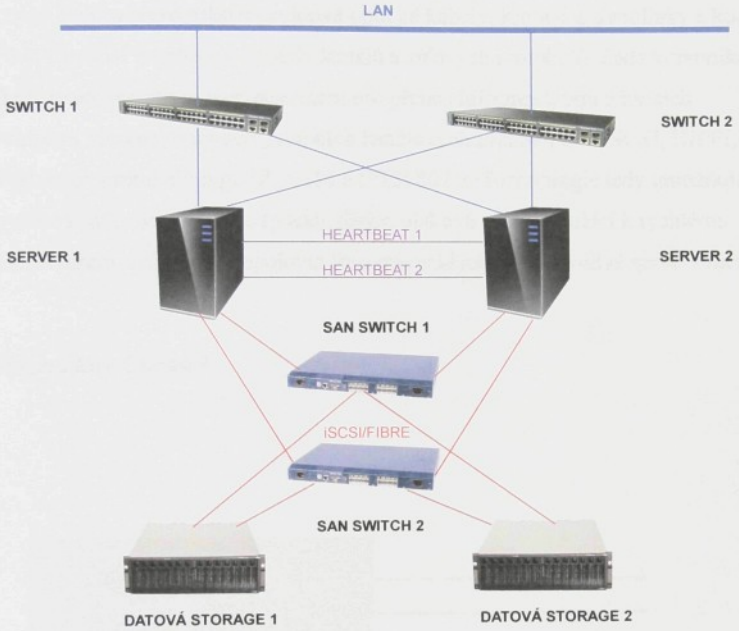
Cluster s vysokou dostupností (HA Cluster)

Cluster s vysokou dostupností (anglicky High-availability) zajišťuje pomocí několika počítačů se stejným obsahem nepřetržité poskytování nějaké služby i při výpadku počítače z důvodu hardwarové závady nebo plánované údržby. Služby, které cluster poskytuje, mohou být v zásadě nakonfigurovány buď jako "failover" (služba běží na jednom počítači, pokud se pomocí tzv. heart beat signálu zjistí, že služba není dostupná, startuje se na jiném počítači clusteru), nebo jako "scalable" (daná služba běží paralelně na všech počítačích clusteru, jednotliví klienti jsou obsluhováni různými počítači clusteru -- tzv. "load balancing", tedy rozložení zátěže mezi jednotlivé počítače clusteru).

Úložný cluster

Úložný cluster (Storage cluster) zprostředkovává přístup k diskové kapacitě, která je rozložena mezi více počítačů z důvodu dosažení vyššího výkonu nebo pro zajištění vyšší

spolehlivosti. Toho je dosahováno speciálními souborovými systémy, které jsou schopny zajistit rozložení zátěže, redundanci dat, pokrytí výpadků jednotlivých uzlů, distribuovaný mechanismus zamykání souborů a další doprovodné služby.

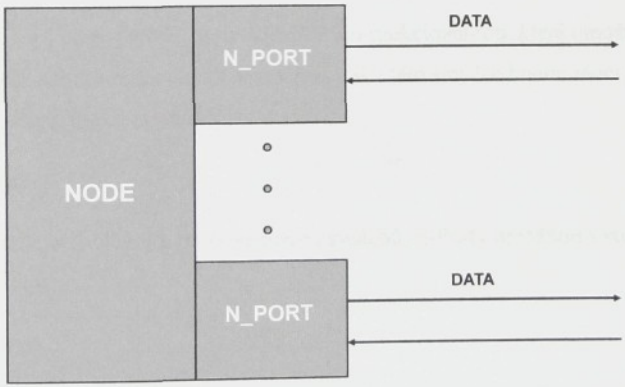


Obr. 9.: Příklad 2-NODE HA/Storage Clusteru

2.6. Fibre Channel

Fibre Channel je novým komunikačním standardem navrženým organizací ANSI pro propojení a připojení vysoce výkonných záznamových zařízení a periferií pomocí optických kanálů. Fibre je obecný název, který zahrnuje různá fyzická média, které může využívat Fibre Channel, např. jednovidové nebo vícevidové optické kabely, kroucené dvoulinky a koaxiální kabely. Fibre Channel kombinuje výhody kanálů a síťových protokolů. Sada komunikačních protokolů FC je univerzálním mechanizmem pro přenos informací, umožňujících vysokorychlostní přenosy vstupně/výstupních kanálových rozhraní typu SCSI, HIPPI,IPPI a zároveň i síťových protokolů typu IP, ATM a IEEE 802.2. Technologie tedy umožňuje vytvářet rychlé kanály pro periferie (pásky, disky, disková pole) sloužící k rychlému připojení k serverům a zároveň propojovat formou rychlých sítí jednotlivé servery mezi sebou.

Terminologie Fibre Channel



Obr. 10.: Fibre Channel Node a porty

Každé fyzické zařízení připojené do Fibre Channel infrastruktury je označováno jako "Node" (uzel) a obsahuje minimálně jeden N_port (Node port) určený pro fullduplexní vysílání (TR) a přijímání (RX) dat. Každý typ portu má své vlastnosti a lze ho propojit s omezenou podmnožinou typů portů.

- **N_Port**

Nejjednodušším typem jsou N (Node) porty. Používají se na všech serverech a zálohovacích zařízení. Umožňují pouze point-to-point propojení s jiným N_Portem nebo F_Portem na switchy.

- **NL_Port**

NL (NodeLoop) nebo též L (Loop) porty jsou N_Porty s dodatečnou funkcionalitou, která jim umožňuje zapojení do Fibre Channel Arbitrated Loop.

- **F_Port**

F (Fabric) porty se používají na Fibre Channel switchy. Mohou být propojeny pouze s N_Portem.

- **FL_Port**

FL (FabricLoop) porty jsou F_Porty s rozšířenou funkcionalitou, která umožňuje zapojení do Fibre Channel Arbitrated Loop. Všechna zařízení v této smyčce budou moci přistupovat ke všemu co je zapojené do switche.

- ***E_Port***

E (Expansion) porty slouží k propojení dvou switchů. E-Porty umožňují vytvářet složité Fabric topologie.

- **G_Port**

G (Generic) porty jsou speciální porty na switchy, které se mohou chovat jako E_Porty nebo F_Porty, podle toho se kterým portem jsou propojeny.

- **GL_Port**

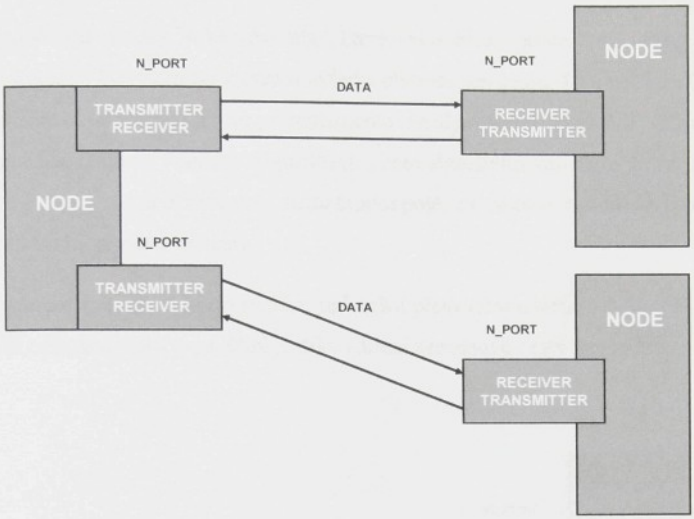
GL (GenericLoop) porty jsou G_Porty s rozšířenou funkcionalitou, která umožňuje zapojení do Fibre Channel Arbitrated Loop.

2.6.1. Topologie Fibre Channel

1) Topologie Point to Point

Nejjednodušší topologií Fibre Channel je tzv. Point to Point, kdy jsou prostřednictvím N_portů mezi sebou propojeny dvě zařízení (Nodes, uzly), příkladem může být propojení serveru a diskového pole. Tato topologie nepotřebuje žádné vyšší řízení přenosové cesty, protože vysílač jednoho uzlu je přímo propojen s přijímačem druhého uzlu. Topologii také není možné nijak dále rozšiřovat, vždy bude zahrnovat pouze dvě propojená zařízení.

Pokud periferie disponuje dvěma N_porty (opět např. diskové pole) , přístup k poli může být současně sdílen dvěma servery . V tomto případě hovoříme o tzv. spojení "Two point to point".



Obr. 11.: Topologie Two point to point

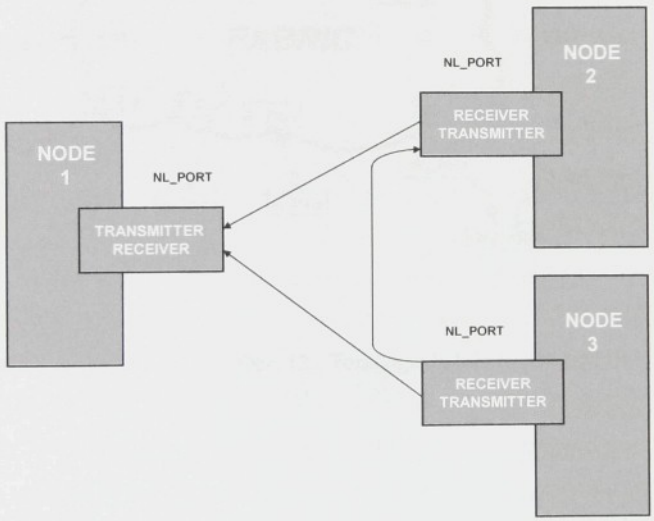
2) Topologie Arbitrated Loop

Do arbitrované smyčky , nazývané Fibre Channel Arbitrated Loop (FC-AL), může být sériově připojeno až 127 portů. Například vysílač Node 1 je připojen k přijímači Node 2, vysílač Node 2 je připojen k přijímači Node 3 a vysílač tohoto posledního uzlu je připojen k přijímači prvního uzlu Node 1. Tímto propojením je tedy realizována kruhová topologie bez nutnosti použít Fiber Channel přepínače. Protože přenosová cesta je sdílená mezi všemi zařízeními na smyčce, může v jeden okamžik vysílat pouze jedno zařízení. K tomu aby mohlo zařízení začít vysílat, musí vyhrát tzv. arbitraci. Proces zahájení přenosu dat tu lze popsat asi takto: Když je zařízení připraveno k předání dat, musí se nejprve ucházet o řízení smyčky. Jakmile ho získá, realizuje bodové spojení (point to point) mezi dvěma zařízeními. Všechna ostatní zařízení mezi nimi jednoduše dále přeposílají data posílaná mezi uvedenými uzly a

fungují tedy jako opakovače. Když obě zařízení uvolní řízení smyčky, ostatní zařízení k němu mohou získat přístup.

Na rozdíl od metody "token-passing", která se používá v sítích Token Ring, zde není limitována doba, po kterou může zařízení ovládat přenosovou cestu. To umožňuje Fibre Channelu pracovat jako kanál. Proto je implementován algoritmus, který řídí přístup zařízení k přenosové cestě (Access Fairness Algorithm). Tento algoritmus zajišťuje, že zařízení se může znovu pokusit získat přenosovou cestu teprve poté, co všechna ostatní zařízení, dostala příležitost k získání přenosové cesty.

Topologie Arbitrated Loop nachází uplatnění především u síťových úložišť typu NAS, pro primární nasazení u sítí typu SAN je díky sdílení přenosové cesty nevhodná.

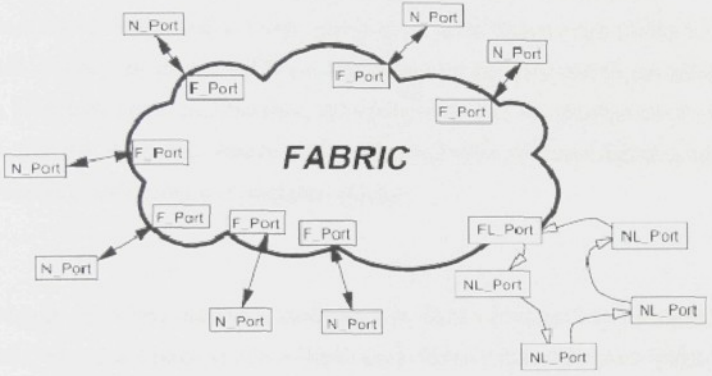


Obr. 12.: Topologie Arbitrated Loop

3) Topologie Fabric

Topologie Fabric používaná u sítí typu SAN je realizována propojením mnoha zařízení pomocí přepínačů (switchů). Hlavní výhodou oproti kruhové topologii (FC-AL) je, že může více zařízení komunikovat současně, protože přenosová cesta zde není sdílená.

Každý Node může být v topologii Fabric zapojen protřednictvím N_Portu nebo NL_Portu. Port na přepínači je označen jako F_Port, ke kterému se připojuje N_Port. Pokud je na F_Port připojen NL_Port, port přepínače je FL_Port.



Obr. 13.: Topologie Fabric

Výhody použití Fibre Channel pro síťové úložiště dat typu SAN :

1) Propojení na velké vzdálenosti – periferie může být umístěna až 10km od serveru
2) Vysoká přenosová rychlost – Fibre Channel technologie umožňuje teoreticky přenosovou rychlost až 8000 Mbps. Propustnost je tedy několikanásobně vyšší než u běžných sítí typu Ethernet, FDDI a Token Ring.
3) Škálovatelnost a snadné připojení dalších zařízení do infrastruktury – Fibre Channel podporuje mnoho přenosových rychlostí, medií a konektorů.

2.7. Metody zálohování a technologie Snapshot

Pro zálohování dat existují tři základní možnosti: plné zálohování, diferenční zálohování a inkrementální zálohování. Při plném zálohování se všechna data zapisují na archivační médium a soubory se označí jako zálohované tím, že se nastaví archivační bit. Při diferenčním (rozdílovém) zálohování se ukládají data na základě archivačního bitu všechny soubory, které vznikly od posledního plného zálohování, nebo které byly v mezičase modifikovány. Archivační bit je přitom stále nastaven. To znamená, že další diferenční zálohování je znovu zaznamená na pásku. Výhodou je, že pro obnovu jsou potřebné pouze pásky posledního plného zálohování a posledního diferenčního zálohování. U inkrementálního (přírůstkového) zálohování je tomu jinak. Tato metoda zálohuje rovněž nové a změněné soubory, ale nuluje archivační bit. Další inkrementální průběh pak zálohuje jen ty soubory, které byly nově modifikovány, nebo jsou nové. Tím se zmenšuje množství zálohovaných dat. Pro plnou obnovu dat je však nutné vedle posledního plného zálohování vyvolat všechny následující inkrementální zálohy.

Metoda vytvoření snapshotu spočívá v tom, že se v jednom okamžiku systém souborů na okamžik zmrazí a zhotoví se odpovídající kopie (často označována jako "point-in-time") informací o struktuře souborů. Pro vytvoření snapshotů existují dva přístupy: buď kopírují strukturu celého systému souborů, nebo (tzv. delta snapshot) kopírují o jednu úroveň níže tím, že vytvoří paměťové bloky patřící k příslušným souborům přímo na systémové sekci disku nebo na jiný vyhrazený (diskový) prostor. Kopie systému souborů obsahuje soubor mapování po blocích, který přesně registruje bloky patřící ke kterým souborům a snímkům. Jakmile se soubor změní, program zapíše změněný blok či přidané bloky na volné místo na disku. Původní bloky zůstávají zachovány a tvoří spolu s dosud nezměněnými bloky konzistentní verzi snapshotu tohoto souboru.

3. EXPERIMENTÁLNÍ ČÁST

Úvodní podkapitoly této části mají za cíl představit v logickém sledu jednotlivou problematiku návrhu řešení, další kapitoly představují technické a aplikační řešení včetně individuálního zhodnocení konkrétních přínosů vyplívající z jejich realizace.

3.1. Prvotní analýza provozovaných aplikací

Nedílnou součástí navrhovaného řešení musí být především prvotní analýza jednotlivých aplikací informačních systémů a návrh vhodného mechanismu zabezpečení dat podle jejich kritičnosti a citlivosti. Při analýze jednotlivých aplikací informačního systému s ohledem na možnosti obnovení funkcí a dat po výpadku se zaměříme zejména na stanovení parametrů obnovy.

Po provedení analýzy požadavků na obnovu všech aplikací můžeme pro každou aplikaci specifikovat individuální parametry obnovy. Při specifikaci parametrů obnovy vycházíme ze dvou hlavních časových parametrů:

Bod obnovy - Recovery Point. Bod v čase, ke kterému musejí být obnovena data aplikace (tj. aktuálnost dat).

Doba obnovy - Recovery Time. Doba, která uplyne od bodu selhání do doby obnovy dat a uvedení aplikace do stavu online.

Na základě definování parametrů obnovy pro všechny aplikace můžeme přistoupit k výběru nejvhodnějších technologie dostatečně vyhovující potřebám jednotlivých aplikací a posléze definovat následující strukturu návrhu jednotlivých postupů a technologií pro:

- zálohování a obnova dat
- replikaci dat a Snapshot Management
- vysokou dostupnost aplikací a dat
- záložní centra a scénář Disaster Recovery

3.1.1. Zálohování a obnova dat

Příčiny výpadků je možno rozdělit do tří kategorií:

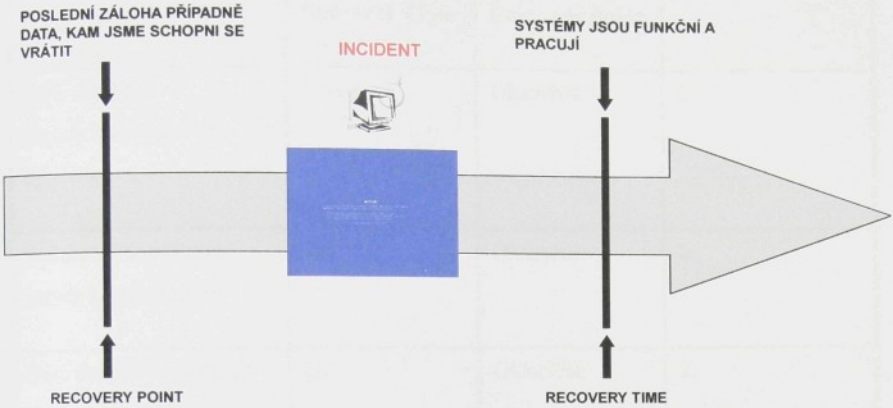
- fyzické: např. selhání hardwaru, komponent infrastruktury nebo aplikace.
- logické: například poškození databáze nebo napadení virem.
- katastrofy: povodeň, požár, zemětřesení apod.

Podle zkušeností lze konstatovat, že nejčastější příčinou výpadků bývá selhání hardware, systémového software a chyba obsluhy.

Řešení pro obnovení fungování systémů po havárii by měla podnik chránit několika různými způsoby:

- zabránit fyzickým a logickým hrozbám ohrožujících kontinuitu chodu podniku
- zajistit, aby v případě výpadku celého centra bylo možné co nejrychleji obnovit provoz v náhradních (záložních) prostorách.

Zálohování dat je prvním krokem pro zajištění ochrany dat proti fyzickým i logickým hrozbám. Podle požadavků stanovených na Recovery Time a Recovery Point se definují pravidla pro zálohování a obnovu dat pro jednotlivé aplikace. Aplikace se zařadí do dvou příslušných skupin, pro které se navrhnou odlišné strategie pro ukládání a obnovu dat. Jako orientační měřítko pro zařazení do dvou skupin můžeme zvolit například rychlost zápisu dat z páskové jednotky do aplikačních diskových systémů.



Obr. 14.: Recovery Time / Recovery Point

Do první skupiny se zařadí aplikace, pro které je parametr Recovery Time delší než doba potřebná pro obnovu dat (čtení dat z pásek a zápis na disky aplikačního serveru). Pro zajištění obnovy dat lze využít klasický způsob zálohování dat. Zálohovaná data se budou ukládat na disky nebo pásky a bezpečnostní kopie na pásky.

Do druhé skupiny se zařadí aplikace, pro které je parametr Recovery Time kratší než doba potřebná pro obnovu dat. Pro zajištění rychlé obnovy dat se zde nepoužije klasické zálohování dat na pásku, ale například technologie pro zrcadlení nebo replikaci dat v kombinaci s technologií Snapshot. Bezpečnostní kopie se budou stejně jako u první skupiny ukládat na pásky.

Aplikace	Požadovaný Recovery Time	Přístup k Recovery Point	Skupina
SQL databáze logisticko/skladového systému	30min	Okamžitě	2.
Aplikační/databázový server Lotus Domino	1h	Okamžitě	2.
Data dalších prioritních aplikace	2h	Okamžitě	2.
Ostatní data (např. uživatelská data)	4h	6h	1.

Tab. 1.: Stanovené požadavky na parametry obnovy

3.1.2. Replikace dat a Snapshot Management

Pro druhou skupinu aplikací, kde požadavky na Recovery Time přesahují fyzické možnosti obnovy dat z pásek na disky, je pro zajištění ochrany dat nutno zvolit jiné technologie. Mezi tyto technologie je možno zařadit zejména produkty pro vytváření synchronních a asynchronních kopií dat, nástroje pro vytváření Point-in-Time (PiT) kopií dat s využitím Snapshot technologie a CDP žurnál.

Synchronní a asynchronní kopie zajišťují ochranu proti fyzickému poškození primárních diskových prostor a Snapshot typu PiT kopie zajišťují ochranu proti logickým chybám jsou zdrojem pro vytváření konzistentních záloh. Replikace dat a Snapshot Management se zpravidla provádí prostřednictvím speciálního programového vybavení na úrovni:

- serveru (Logical Volume Manager ...)
- řadičů diskových polí (EMC SRDF, Hewlett Packard CA...)
- virtualizačních storage serverech (FalconStor, NetApp ...)

3.1.3. Vysoká dostupnost aplikací a dat

Vysoká dostupnost aplikací je velmi důležitým prvkem především tam, kde je potřeba provozovat systémy 24 hodin denně bez nebo s minimálním časem odstávky. Cílem řešení zabezpečení nepřetržitého chodu aplikací a dostupnosti dat je realizace tzv. „nerozbitného serveru" a „nerozbitné storage".

Nerozbitný server umožňuje v případě výpadku běh operačního systému a aplikací bez ohledu na hardware s transparentní migrací mezi fyzickými servery. Pro zabezpečení nepřerušitelné funkce těchto systémů je třeba spojit minimálně dva servery do clusteru v režimu high availability, který zajistí, aby v případě, že jeden ze serverů selže, se jeho aplikace zcela transparentně přesunuly na server druhý. V případě, že dojde k opravě havarovaného serveru a je posléze opět připojen do infrastruktury clusteru, může tento server automaticky převzít své aplikace zpět.

Nerozbitná storage umožňuje transparentní a neustálou dostupnost diskových svazků bez ohledu na jejich fyzické umístění a výpadky jednotlivých diskových polí. Neustálá dostupnost diskového svazku je řešena pomocí zrcadlení či replikace dat a transparentnost je zajištěna tzv. failoverem na sekundárním diskovém poli. Nezávislost na fyzickém umístění znamená migraci dat mezi diskovými poli za plného chodu aplikací.

3.1.4. Záložní centra a scénář Disaster Recovery (scénář obnovy po katastrofě)

V tomto případě není řešena obnova aplikačních dat, ale obnova celého datového centra nebo alespoň jeho kritických částí po jeho havárii způsobené například živelnou pohromou či požárem. Pokud vezmeme v úvahu nejhorší scénář, nezbude v datovém centru žádný funkční server, diskové pole nebo síťové prvky. Scénář pro Disater Recovery se typicky neobejde bez jedné nebo několika geograficky vzdálených lokalit, mezi kterými bude

možné pomocí replikace nebo zrcadlení diskových svazků zajistit použitelné zálohy nejenom aplikačních, ale také systémových disků pro zajištění obnovy všech serverů (nainstalovaných a nakonfigurovaných operačních systémů).

Návrh efektivnějšího scénáře obnovy je jedním z hlavních důvodů, proč dnes často dochází ke kompletní virtualizaci datových center. Provozování většího množství virtuálních strojů na několika fyzických serverech může v případě plně zajištěné kontinuální zálohy virtuálních strojů a dat do vzdálené lokality zcela zásadním způsobem urychlit obnovu celého datového centra.

Základní myšlenka a vize komplexního řešení zálohování a vysoké dostupnosti dat musí tedy nezbytně akceptovat následující body :

- zajištění fyzické a logické odolnosti dat
- zajištění rychlého přístupu k datům z minulosti pro účely obnovy
- dostupnost aplikačních serverů a dat v případě výpadku datového centra

3.2. Vize řešení :

Po provedení prvotní analýzy s uvážením níže uvedených nevýhod samotného zálohovacího procesu, tak i infrastruktury datového centra je možné přistoupit ke stanovení konkrétních požadavků na odpovídající zálohovací systém a infrastrukturu datového centra.

Původní zálohovací proces :

- vysoká zátěž LAN sítě
- velikost zálohovacího okna
- složitá a pomalá obnova dat
- licencování zálohovacího agenta pro každý další fyzický stroj (drahé)

Původní infrastruktura centra :

- topologie typu hvězda

- vysoké zatížení aplikačních serverů a sítě LAN při zálohovacím procesu
- problematické chlazení serverů
- vysoké energetické nároky
- obtížná údržba a správa serverů
- nevyužitý potenciál sítě SAN

Na základě těchto problémových aspektů a rozboru požadavků společnosti můžeme určit následující cíle pro realizaci:

Primární cíle :

- vybudování dvou plnohodnotných datových center (topologie SAN fabric a protokol Fibre Channel) v konfiguraci high availability clusteru
- virtualizace serverů a datových storage
- možnost provozu kritických aplikací z obou těchto center
- vysoká odolnost proti logickým i fyzickým chybám dat
- vysoká dostupnost aplikací a diskových úložišť v režimu 24x7
- rychlý přístup k datům z minulosti a jejich obnova
- řešení bez navýšení počtu zaměstnanců IT oddělení

Sekundární cíle :

- škálovatelnost výpočetního výkonu aplikačních serverů
- škálovatelnost diskového prostoru
- centralizovaná správa zálohovacího systému

Společné požadavky na technické řešení na virtualizační bázi :

- snadná a rychlá migrace bez přerušení chodu ze stávajících systémů
- clusterový high availability režim s transparentním fail over
- pozitivní reference a vhodnost nasazení v prostředí velkého podniku (enterprise)
- cenová dostupnost

Hlavní požadavky na technické řešení serverové virtualizace :

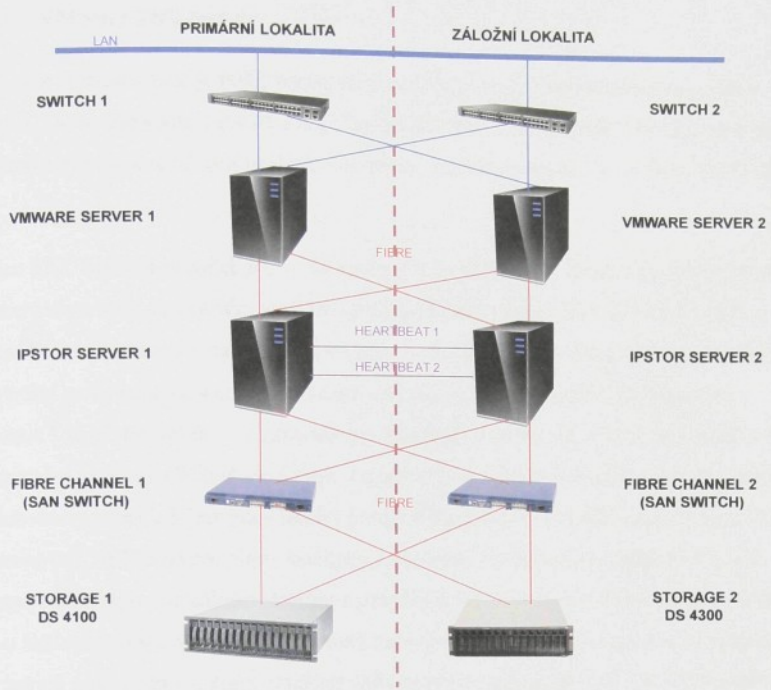
- vysoká stabilita
- maximální efektivita využití zdrojů
- dynamické rozložení zátěže
- přenositelnost virtuálních strojů

Hlavní požadavky na technické řešení storage virtualizace :

- dedikovaný storage server
- jednotná správa všech úložných zařízení
- připojení stávající páskové jednotky pro účely archivace
- komplexní služby pro zálohování a obnovu dat

Kritéria zcela splňují produkty **VMWare Infrastructure** (ESX server) pro serverovou virtualizaci společně s **IPStor** serverem pro virtualizace storage.

Realizované řešení vychází z vybudování dvou oddělených fyzických datových center v clusterovém režimu sdružených do virtuálního prostředí. Platformou vytvořeného serverového clusteru je virtualizační technologie VMWare Virtual Infrastructure. Datové centra jsou realizována jako plně redundantní, v každém je umístěn jeden server VMWare, virtualizační storage server IPStor, disková storage a potřebná síťová infrastruktura včetně záložních zdrojů elektrické energie. Data na primární datové storage (diskové pole v konfiguraci RAID5) jsou kontinuálně replikovány na datovou storage v záložní lokalitě, replikace a vytváření snapshotů typu point-in-time je automaticky řízeno pomocí serveru IPStor.



Obr. 15.: Infrastruktura řešení

3.3. VMWare Infrastructure

VMware Infrastructure (dále VMI) je softwarová sada používaná ke kompletní virtualizace serverů. VMI virtualizuje a seskupuje standardní fyzické servery a k nim připojené sítě a datová úložiště do jednotných souborů zdrojů. Ve virtuálních strojích, jež jsou nezávislé na hardwaru, jsou umístěna kompletní prostředí včetně operačních systémů a aplikací. Díky distribuované optimalizaci zdrojů umožňuje dynamické a inteligentní přidělování dostupných zdrojů mezi virtuální stroje a lze tedy dosáhnout podstatně lepšího využití hardwaru podle potřeb a priorit administrátora.

3.3.1. VMware ESX Server

VMware Infrastructure je balík řešení založený na původně samostatném produktu VMware ESX Server spolu s dalšími doplňky a službami. VMware ESX Server představuje samostatný virtualizační nástroj provozovaným na vlastním operačním systému RedHat Linux.

Instalace ESX Serveru probíhá přímo na serverový hardware neboli na tzv. „bare-metal", mezi hardware a operační systém je vložena virtualizační vrstva. ESX Server provádí rozdělení fyzického serveru na více bezpečných a přenositelných virtuálních strojů, které mohou běžet vedle sebe na tomtéž fyzickém serveru. Každý takovýto virtuální stroj představuje kompletní systém – s procesorem, operační pamětí, sítí, diskovou pamětí a BIOS, takže operační systémy (Windows, Linux..) a jednotlivé softwarové aplikace běží v plně virtualizovaném prostředí bez jakýchkoliv nutných modifikací a zásahů. Architektura bare-metal poskytuje ESX Serveru plnou kontrolu nad všemi serverovými zdroji, které jsou přiděleny jednotlivým virtuálním strojům a umožňuje téměř nativní výkon virtuálních strojů a vysokou škálovatelnost. Virtuální stroje mají zabudovány funkce pro vysokou dostupnost, správu zdrojů a bezpečnost, které zajišťují softwarovým aplikacím vyšší úrovně služeb než běžná fyzická prostředí.

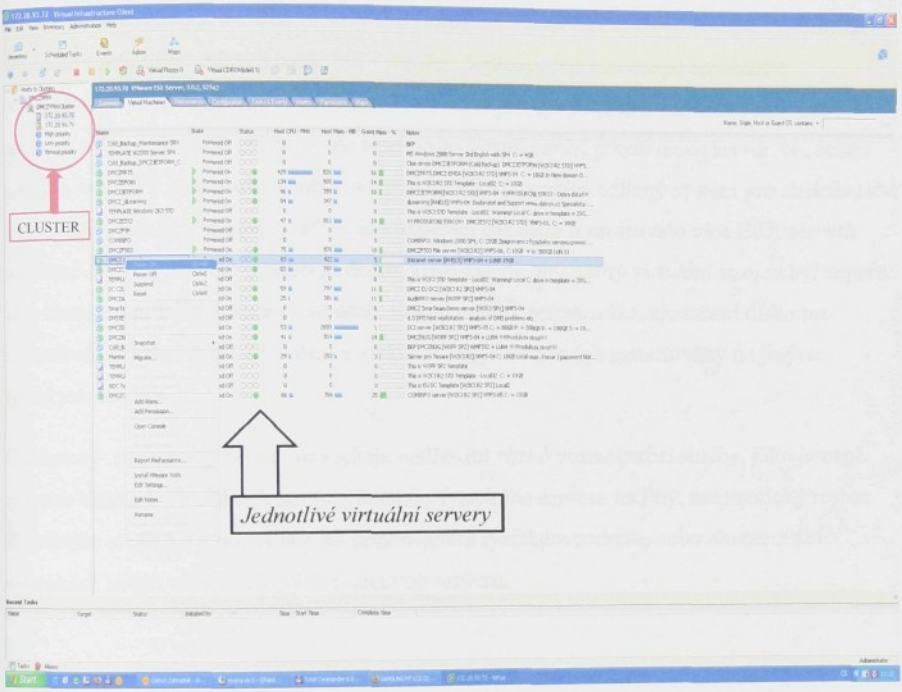
Každý virtuální disk virtuálního serveru je reprezentován jedním souborem, dále existuje konfigurační soubor virtuálního serveru. Např. v nejjednodušším případě je tedy celý virtuální server reprezentován dvěma soubory - souborem reprezentujícím systémový disk virtuálního serveru a konfiguračním souborem. Tato reprezentace poskytuje velké možnosti operací s virtuálními operačními systémy. Pokud chceme např. kopii celého operačního systému instalovaného v prostředí VMware, stačí udělat kopii pouze několika souborů. Stejně tak lze virtuální stroje přesouvat mezi různými fyzickými servery s nainstalovaným VMware.

Pro centrální správu VMware ESX serveru se používá nástroj Virtual Center umožňující ovládat především tyto klíčové moduly :

- VMotion : přesun VM za chodu z jednoho fyzického serveru na druhý bez narušení dostupnosti OS a aplikací
- HA (High Availability) : automatický restart virtuálního serveru na jiném fyzickém VMWare serveru v případě havárie

- VMware convertor : převedení stávajícího „normálního" operační systému do virtualizované podoby

Připojení k virtuálním serverům je možné prostřednictvím libovolného RDP (Remote Desktop) klienta (lze i z prostředí Virtual Center).



Obr. 16.: ukázka prostředí Virtual Center – výpis virtuálních serverů

3.3.2. Virtuální server v režimu High Availability

Modul VMware HA nepřetržitě monitoruje veškeré dostupné servery a detekuje jejich případné selhání .Agent umístěný na jednotlivých serverech udržuje pravidelné spojení pomocí tzv. Heart Beat signálu s ostatními servery a při ztrátě spojení iniciuje proces restartování všech havarovaných virtuálních strojů na jiném fyzickém serveru. VMware HA zajišťuje, aby byl neustále dostatek dostupných zdrojů a bylo tedy možno v případě selhání nějakého serveru restartovat virtuální stroje na jiných fyzických serverech. Restart virtuálních

strojů je možný díky clusterovému souborovému systému VMFS, který poskytuje více instancím ESX Serveru přístup pro čtení a zápis ke stejnému virtuálnímu stroji současně.

3.3.3. Clusterový filesystém VMFS (Virtual Machine File System)

VMFS je clusterový souborový systém, který provádí virtualizaci systémů pro ukládání dat optimalizovanou pro virtuální stroje. Systém VMFS ukládá kompletní stav virtuálního stroje do centrálního místa a může být vytvořen dopředu, což umožňuje nepřetržité poskytování virtuálních strojů. U běžných souborových systémů může mít ke stejnému souboru v daný okamžik přístup typu read-write (čtení, zápis) pouze jeden server. Na rozdíl od toho je VMFS clusterový souborový systém, který využívá sdílený systém pro ukládání dat a umožňuje, aby ve stejném systému pro ukládání dat četlo a zapisovalo více ESX serverů současně. VMFS provádí uzamčení disku, které zajistí, aby určitý virtuální stroj nebyl zapnut více instalacemi ESX Serveru současně. Pokud nějaký server selže, uzamčení disku pro jednotlivé virtuální stroje se uvolní a virtuální stroje mohou být restartovány na jiných fyzických serverech.

Clusterový souborový systém umožňuje realizovat různé virtualizační služby, jako je např. migrace běžících virtuálních strojů z jednoho fyzického serveru na jiný, automatický restart virtuálního stroje po jeho selhání na samostatném fyzickém serveru, nebo clusterování virtuálních strojů v rámci různých fyzických serverů.

Stěžejní přínosy nasazení serverové virtualizace prostřednictvím VMWare :

	Původně	Po virtualizaci
Vytížení zaměstnanců IT oddělení	3 na 5 fyzických serverů	1 na 17 serverů
Zřízení nového serveru	1-5 dní HW instalace 1-3 hodiny instalace OS	maximálně 10 minut pomocí předpřipravených Template (šablon) OS
HW správa a upgrade	výluka několik hodin (pokud vůbec možná)	bez přerušení činnosti (VMotion technologie)
Počet instalovaných aplikací na serveru	až 5 na jednom fyzickém serveru	pro každou aplikaci vlastní virtuální server
Zatížení CPU serverů	Až 100% (kritické)	přibližně 4%

Tab. 2.: Porovnání stavu před a po virtualizaci serverů

Mezi další podstatné výhody nasazení VMWare serverů patří nižší spotřeba elektrické energie a tím i menší vyzářené teplo.

3.4. Virtualizační server IPStor

In-Band virtualizační dedikovaný server IPStor poskytuje komplexní a centralizovanou správu všech datových úložišť v rámci vybudované infrastruktury. Veškeré úkony spojené se zálohováním a obnovou dat (replikace dat do záložní lokality a vytváření snapshotů) probíhá zcela v režii tohoto virtualizačního serveru. Administrace probíhá zadáváním příkazů do příkazového řádku přímo na konzoli serveru nebo využitím grafického java-klienta na bázi vzdáleného připojení.

Mezi další klíčové vlastnosti IPStor serveru patří:

- podpora heterogenního prostředí (k serveru lze připojit disková pole a páskové zařízení od různých výrobců)
- přítomnost rozhraní Fibre Channel, SCSI, Ethernet

Vysoká dostupnost dat :

IPStor v clusterovém režimu společně s redundatní infrastrukturou poskytují vysokou dostupnost celého úložného systému v rámci SAN:

1. v případě nedostupnosti primární datové cesty mezi IPStor serverem a klientem (VMWare server) využije alternativní uživatelsky definovanou cestu
2. automaticky detekuje všechny možné datové cesty mezi IPStor serverem a datovými storages a umožňuje v případě jejich výpadku plně automatické přepínání
3. v případě výpadku primární datové storage zcela transparentně a okamžitě zpřístupní data aplikačním serverům ze záložní replikované storage ve vzdálené lokalitě
4. vzájemný monitoring stavu IPStor serverů (pomocí heart-beat signálu) umožňuje v případě nedostupnosti jednoho ze serverů okamžité a transparentní převzetí identity druhým IPStor serverem

Replikace dat – ochrana proti fyzickému poškození dat

Server IPStor kontinuálně zprostředkovává vzdálené replikaci dat mezi primární a záložní lokalitou v synchronním režimu přenosu. Kompletní replikační proces probíhá pouze na úrovni diskových polí a tedy bez účasti operačního systému (tzn. nulová zátěž aplikačních serverů).

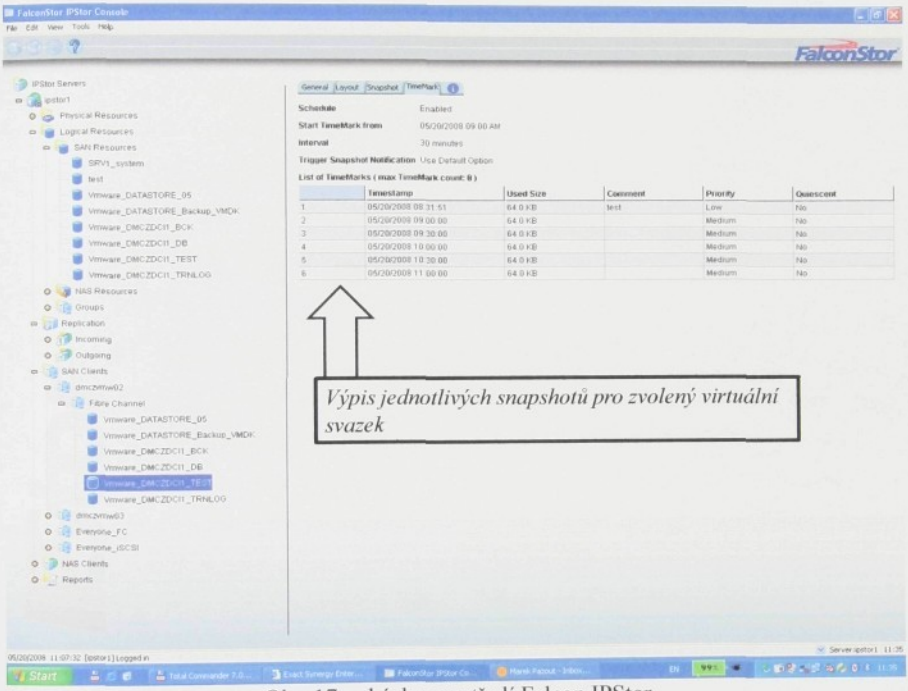
Záložní lokalita je nadefinována v režimu „stand-by" a v případě výpadku či havárie primární datové storage je okamžitě a transparentně (zachování identické číselné struktury logických jednotek LUN) zpřístupněna všem aplikačním serverům. Pro pozdější účely obnovy dat na primární datové storage je využita snímková technologie snapshot.

Snapshot - ochrana proti logické chybě dat

V případě logické chyby (např. smazání dat) v umožňuje IPstor obnovit požadovaný soubor nebo celý diskový svazek pomocí technologie rozdílových (delta) snapshot snímků na úrovni diskových bloků. Vytvoření snapshotů jednotlivých virtuálních svazků probíhá zcela automaticky v administrátorem stanovených časových intervalech (snapshot lze vytvořit i okamžitě v případě potřeby), podporováno je 256 snapshot snímků na jeden virtuální svazek.

Perioda automatického vytvoření snapshotu (čili maximální parametr RPO) je pro kritické aplikace stanovena na 30minut, pro další aplikace je stanovena na 4 hodiny.

Obnova dat probíhá podle potřeb přímým zpřístupněním dat z minulosti (tzv. „rollback") na úrovni virtuálního diskového svazku prostřednictvím příslušného snapshot snímku automaticky vytvořeného k určitému času. Tento svazek obsahuje veškerá původní data včetně jejich struktury vztažena k tomuto časovému okamžiku a svazek lze okamžitě zpřístupnit kterémukoliv aplikačnímu serveru pro účel obnovy a rekonstrukce struktury dat.



Obr. 17.: ukázka prostředí Falcon IPStor

Stěžejní přínosy nasazení virtualizačních serverů IPStor :

- synchronní kopie dat v jiné lokalitě
- žádné zálohovací okno (čas pro vytvoření zálohy)
- okamžitý přístup k datům z minulosti prostřednictvím snapshot snímků
- jednotná správa datových storage

- snadné vytvoření a správa storage poolů
- nulové zatížení aplikačních serverů při zálohovaní

4. ZÁVĚR

Cílem diplomové práce bylo realizování komplexního návrhu pro bezpečné úložiště podnikových dat. Návrh a výběr zálohovacího systému a vyhovující infrastruktury datového centra trval přibližně měsíc, v této době byly definovány konkrétní požadavky na technickou i aplikační realizaci. Vlastní realizace návrhu a migrace z původních systémů probíhala po dobu tří měsíců včetně důkladného testování před nasazením do ostrého provozu. V současné době je realizované datové centrum v ostrém provozu již druhý měsíc a z dosavadních zkušeností lze konstatovat , že splňuje stanovené požadavky na odolnost proti fyzické i logické chybě dat, eliminaci zálohovacího okna a požadavek na vysokou dostupnost dat i aplikací v režimu 24x7. Záložní datové centrum pro clusterový režim, které bude po dokončení výstavby druhé podnikové serverové místnosti umístěno v odlehlejší lokalitě, je již nyní okamžitě připraveno a nakonfigurováno k provozu a poskytuje robustní platformu pro rychlou dostupnost dat i aplikací v případě kompletní havárie primárního datového centra (disaster recovery).

V průběhu implementace řešení bylo mnohokrát potvrzeno, že vhodně zvolená a dodržovaná strategie ukládání a zálohování dat společně s odpovídající infrastrukturou datového centra je dnes naprosto nezbytná pro nepřerušený chod celého podniku. Každá společnost by měla být schopna vyčíslit, jakou ztrátu znamená případný výpadek činnosti za určitý časový úsek a jaká další navazující a dlouhodobá rizika mohou po výpadku vzniknout - patří mezi ně například ztráta důvěry zákazníků a jejich následný přechod ke konkurenci. Ztráty tohoto typu lze pouze odhadovat, neboť zahrnují i ztráty kvalitativní (např. ztrátu reputace), jejichž reálný dopad lze předpovědět a vyčíslit jen stěží.

Použitá literatura

[1] CLARK, T.: Designing Storage Area Networks: A Practical Reference for Implementing Fibre Channel and IP SANs. ADDISON-WESLEY PROFESSIONAL, London 2003.

[2] CLARK, T.: Storage Virtualization: Technologies for Simplifying Data Storage and Management. ADDISON-WESLEY PROFESSIONAL, London 2005

[3] IBM Redbooks.: Introduction to Storage Area Network. IBM, New York 1999

[4] TOBY J. VELTE, ANTHONY T. VELTE.: Síťové technologie Cisco. COMPUTER PRESS, Brno 2003

[5] JIROVSKÝ,V.: Vademecum správce sítě. GRADA, Praha 2001

[6] OSIF,M.: Windows Server 2003. GRADA, Praha 2003

[7] Bunn, F.: Nejlepší kombinace zálohovacích metod, dostupné z http://www.cw.cz/cwarchiv.nsf/clanky/13395553D0535901C1256C360041DE0C

[8] Rudišar, K.: SAN realizované prostřednictvím protokolu iSCSI, dostupné z http://archiv.computerworld.cz/cwarchiv.nsf/clanky/D0CD0BB87C8CE106C125733A005C665C

[9] Matlis, J.: Virtualizace ukládání dat, dostupné z http://archiv.computerworld.cz/cwarchiv.nsf/clanky/ADD082B0A3D4A2CFC1256AB10055DB08

[10] Veselý, J.: Vysoká dostupnost databází a jejich obnova po havárii, dostupné z http://archiv.computerworld.cz/cwarchiv.nsf/clanky/C05EED1C98513BF6C1256E28003CE066

[11] www.computerworld.cz .: Jak na zálohování dat, dostupné z http://archiv.computerworld.cz/cwarchiv.nsf/clanky/1DA6C3612167959BC1256AB100561CFD?OpenDocument

[12] www.computerworld.cz.: Virtualizace a ukládání dat v síti, dostupné z http://archiv.computerworld.cz/cwarchiv.nsf/clanky/7FB41B03454ED133C12570C8004DF232

[13] Olbright G.: Technologie pro přenosy velkých objemů dat, dostupné z http://archiv.computerworld.cz/cwarchiv.nsf/clanky/C461B45416FAEFB1C12569B000545260

[14] Rudišar, K.: Ochrana dat, zálohování a disaster recovery, dostupné z http://archiv.computerworld.cz/cwarchiv.nsf/clanky/EA907676B8C1D340C125733A005C66DB

[15] Nolte, T.: Gridy pro inteligentní ukládání dat, dostupné z http://archiv.computerworld.cz/cwarchiv.nsf/print/757DDA3AC1D3D24BC1256F5500491163?

[16] Gruman, G.: Virtualizujte si ukládání dat, dostupné z http://archiv.computerworld.cz/cwarchiv.nsf/clanky/4E2F8AE4ED4EEF4BC12571AA004712BE

[17] Stonawski, I.: Virtualizace v datových centrech, dostupné z http://archiv.computerworld.cz/cwarchiv.nsf/clanky/3FABFC7CE0F0BCF0C125733A005C0F55

[18] Dryml, J.: Profi ochrana a záloha dat od Microsoftu, dostupné z http://www.zive.cz/Titulni-strana/Profi-ochrana-a-zaloha-dat-od-Microsoftu/sc-21-sr-1-a-140735/default.aspx

[19] EasyVirtualStoage (EVS) - made by FalconStor, dostupné z http://www.coma.cz/PrintClanek.aspx?kod=AKTUALITY&subjekt=2536

[20] www.storyflex.cz /: Rejstřík (storage) pojmů, dostupné z http://www.storyflex.cz/216-rejstrik-storage-pojmu.html

[21] www.storyflex.cz/: Virtualizace, dostupné z http://www.storyflex.cz/157-virtualizace.html

[22] Softwarové řešení pro konsolidaci a virtualizaci server, dostupné z http://www.mediumsoft.cz/cs/Systemova-reseni/VMware/46.aspx?js=4

[23] Palkovský, J.: Business Continuity, dostupné z http://www.dsm.tate.cz/print.php?typ=DAA&showid=289&id=71033

[24] VMware VMFS, dostupné z http://www.soft-tronik.cz/web/katalog.nsf/0/9f14aafacd124a6dc12573b6005055f1/$FILE/VMware_VMFS.pdf

[25] Novák, J.: 100% Dostupnost dat ??, dostupné z http://www.storage.cz/index.php?option=com_content&task=view&id=33&Itemid=39

[26] Novák, J. Definice a rotace záloh, dostupné z http://www.storage.cz/index.php?option=com_content&task=view&id=47&Itemid=39

[27] Mrnka, L.: Storage Area Networks, dostupné z http://www.kiv.zcu.cz/~simekm/vyuka/pd/zapocty-2004/san-mrnka/

[28] Krejčů, V.: Virtuální SAN sítě s nevirtuálními úsporami, dostupné z http://www.datavpeci.cz/index.php?c=cl&id=16

[29] Beran, R.: Virtualizace operačních system, dostupné z http://www.beranr.webzdarma.cz/virtualizace.html

[30] www.fibrechannel.org/: Executive Summary, Fibre Channel Industry Association, 2004, dostupné z http://www.fibrechannel.org/OVERVIEW/index.html

[31] Wikipedie: Otevřená encyklopedie:Storage Area Network, dostupné z http://cs.wikipedia.org/wiki/Storage_Area_Network

[32] Sádovský A., Drahovzal M.: Fibre Channel , Česká zemědělská univerzita v Praze, katedra Informační inženýrství, 2006, dostupné z http://adrin.ic.cz/Data/Works/

[33] Pužmanová R.: DAS, SAN, NAS:Varianty řešení ukládání a zálohování dat, dostupné z http://www.systemonline.cz/clanky/das-san-nas.htm

[34] Hájek, J.: Virtualizace - mýtus, kouzlo, hype nebo realita?. dostupné z http://interval.cz/clanky/virtualizace-mytus-kouzlo-hype-nebo-realita/

[35] Čečelský D.: Na iSCSI s NetWarem, dostupné z http://www.anect.com/cs/info/tiskove-centrum/clanky/na-iscsi-s-netwarem.html

[36] Matoušek, J.: Virtualizace dat, dostupné z http://www.systemonline.cz/sprava-it/virtualizace-dat.htm

[37] Gottvadl, D. : Zálohování dat a disaster recovery, dostupné z http://www.gapp.cz/download/prezentace-konference/GAPP2008/3%20Zalohovani%20dat%20a%20disaster%20recovery.pdf

[38] Dvořák, P. : Zálohování dat a Disaster Recovery v prostredí VMware, dostupné z http://www.gapp.cz/download/prezentace-konference/DSW2007/backupDRvmware.pdf

[39] Dvořák, P. : Nerozbitná úložiště dat, dostupné z http://www.gapp.cz/download/prezentace-konference/GAPP2008/2%20Nerozbitna%20uloziste%20dat.pdf

[40] VMware ESX Server, dostupné z http://www.soft-tronik.cz/web/katalog.nsf/0/9f14aafacd124a6dc12573b6005055f1/$FILE/VMware_ESX%20Server.pdf

[41]] Lugsch, Z.: Datová centra, dostupné z http://www.autocont.cz/sluzby-ebs-infrastruktura-datovacentra.cml

[42] www.systemonline.cz/: Páskové knihovny a ochrana investic, dostupné z http://www.systemonline.cz/clanky/paskove-knihovny-a-ochrana-investic.htm

Seznam zkratek a symbolů:

IT	Information Technology
IBM	International Business Machines Corporation
SCSI	Small Computer System Interface
LAN	Local Area Network
SQL	Structured Query Language
SATA	Serial Advanced Technology Attachment
DAS	Dirrect Attached Storage
NAS	Network Attached Storage
SAN	Storage area network
VMI	VMware Infrastructure
RAID	Redundant Array of Independent Disks
TCP/IP	Transmission Control Protocol / Internet Protocol
FCP	Fibre Channel Protocol
FCIP	Fibre Channel over IP
LUN	Logical Unit Number
NTFS	New Technology File System
CDP	Continuous Data Protection
FDDI	Fiber distributed data interface
RTO	Recovery Time
RPO	Recovery Point

SEZNAM PŘÍLOH:

Příloha A: obr Záložní centrum