Řízení výrobní linky čipových karet

Smart-Card Assembly-line Control

Bc. Martin Hoke

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

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

Jméno a příjmení:	**Bc. Martin HOKE**
Osobní číslo:	**A09758**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Řízení výrobní linky čipových karet**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na téma bladových řešení a jejich vztahu k vizualizaci.**
2. **Navrhněte potřebné prvky infrastruktury pro řešení systému.**
3. **Vypracujte konfiguraci bladového systému pro daný úkol.**
4. **Vypracujte vhodný koncept pro sledování, ukládání a zálohování dat.**
5. **Pro autentizaci do domény vypracujte systém přihlašování za pomocí čipových karet a certifikační autority domény.**
6. **Analyzujte přínosy navrženého řešení a vyhodnoťte přínosy a nedostatky návrhu.**
7. **Nastiňte možný další rozvoj systému.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **RUSSEL, Charlie. Microsoft Windows Server 2008: velký průvodce administrátora. Vyd. 1. Brno: Computer Press, 2009, 1271 s. ISBN 978-802-5121-153.**
2. **DOSTÁLEK, Libor a Marta VOHNOUTOVÁ. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. vyd. 1. Brno: Computer Press, 2006, 534 s. ISBN 80-251-0828-7.**
3. **ŠETKA, Petr. Mistrovství v Microsoft Windows Server 2003. Vyd. 1. Brno: Computer Press, 2003, 680 s. ISBN 80-251-0036-7.**
4. **LONEY, Kevin. Mistrovství v ORACLE. Vyd. 1. Praha: Computer Press, 2002, 860 s. ISBN 80-722-6635-7.**
5. **GOLDWORM, Barb a Anne SKAMAROCK. Blade servers and virtualization: transforming enterprise computing while cutting costs. Indianapolis, IN: Wiley Pub., c2007, 384 s. ISBN 04-717-8395-1.**
6. **LARSON, Robert a Janique CARBONE. Windows server 2008 hyper-V resource kit. Redmond, Wash.: Microsoft Press, c2009, 761 s. ISBN 978-0672330230.**
7. **MEYLER, Kerrie, Byron HOLT a Greg RAMSEY. System center configuration manager 2007 unleashed. Indianapolis, Ind.: Sams Pub., c2010, 1190 s. ISBN 06-723-3023-7.**

Vedoucí diplomové práce: **Ing. Radek Šilhavý, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **21. května 2012**

Ve Zlíně dne 24. února 2012

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Hlavním cílem diplomové práce je popsat proces implementace bladového řešení do produkční výrobní linky na čipové karty. Práce je rozdělena na dvě hlavní části. Teoretická část je výsledkem studia dostupných informačních zdrojů, které se vztahují k problematice bladů a jejich vztahu k virtualizaci. Praktická část, která navazuje na teoretická východiska objasňuje proces implementace navrženého bladového systému přímo v konkrétním podniku. Na úplný závěr diplomové práce byla problematika podrobena ekonomické analýze a je nastíněn další možný postup rozvoj nového systému

Klíčová slova: blade, virtualizace, implementace, server, switch

ABSTRACT

The main objective of this thesis was implementation process blade solutions into production Smart card assembly line.. The work is divided into two main parts. The theoretical part is the result of the study of accessible information sources related to the issue of blades and their relationship to virtualization. The practical part that refers to the theoretical one briefly describes blade proposed system in bussiness company. n conclusion there is a economical analysis and to show another possible development of new system.

Keywords: blade, virtualization, implementation, server, switch

Na tomto místě bych rád poděkoval Ing. Radkovi Šilhavému, Ph.D. za vedení diplomové práce a také za jeho věcné připomínky, při jejím zpracování.

Rovněž patří můj dík rodině, zvláště mé manželce za podporu při studiu a tvorbu potřebného zázemí.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Ve své diplomové práci jsem se rozhodl blíže se zaměřit na problematiku, která se v posledních letech stává velice aktuálním tématem mezi IT profesionály a firmami využívající moderní výpočetní technologie. Tímto tématem je využití a nasazení bladových řešení v rámci malých datových center.

Nápad zabývat se ve své diplomové práci právě touto problematikou, jsem dostal při realizaci státní zakázky, na kterou naše firma vyhrála výběrové řízení. Toto téma se mi zdá právě v době dnešního rychlého rozvoje v nasazování bladových řešení velice atraktivní.

Podle principů Moorových zákonů se dá očekávat, že rozvoj bladových systémů nabere velkou rychlost a využitelnost těchto systémů bude rok od roku vyšší. Ano, vždy se budou provozovat systémy, u kterých nebude využití bladu vhodné. Také odpůrců bladu se vždy několik najde. Nicméně při dobrém naplánování se ukáže, že i malé firmy si mohou pořízení bladových systémů dovolit a své výrobní procesy tak zefektivnit.

Cílem diplomové práce je seznámit čtenáře s moderními technologiemi, které se používají ve výrobních podnicích 21. století. Z práce by mělo být zřejmé, jak je proces modernizace výrobních systémů náročný na přípravu, projektování, ověření daných konfigurací a jak je nakonec obtížné celý systém implementovat do zaběhnutého produkčního prostředí s ohledem na stávající výrobní procesy.

I. TEORETICKÁ ČÁST

1 MOŽNOSTI MODERNIZACE DATOVÉHO CENTRA

Datové centrum je srdcem podnikové infrastruktury. Je tomu tak díky stále silnější orientaci na konsolidaci dat a fyzických prostředků. Výkonný hardware, stabilní a koncepční virtualizační technologie a inovativní a spolehlivé aplikace pro management zálohování jsou dnes nezbytným standardem.

Budování či modernizace datového centra se většinou zakládá ze zodpovězení tří základních otázek: jak velké má být datové centrum, jak má být spolehlivé a jak dosáhnout požadovaných vlastností s minimálními náklady. V dnešní době je kladen velký tlak především na zvyšování účinnosti, pozornost je kladena na virtualizaci, implementaci nových technologií, přičemž úspora energie je na prvním místě.

Srdcem každého datového centra je pak serverovna, v níž jsou uloženy servery – výpočetní výkon, data a sítě. Trendem v modernizaci datových center je využívání Blade serverů.

1.1 Co je Blade

Na začátek je dobré vysvětlit si co to vlastně blady jsou. Blade servery jsou ultratenké servery, u kterých se klade důraz na rozšiřitelnost a výkon, efektivní management a nízký objem kabeláže. Blady zabírají nesrovnatelně méně prostoru oproti klasickým serverům. V moderních firmách proto již poměrně dlouhou dobu nacházejí stále větší uplatnění. Tyto firmy kladou velký důraz na obsazený prostor v rackových skříních a celkovou ekonomiku provozu serverovny/datového centra. [1]

S tím, jak se neustále zvyšuje koncentrace serverů a výpočetní výkon na co nejmenších plochách se upírá hlavní pozornost na napájení a chlazení. Množství energie a vyzářeného tepla na jednotku prostoru dostává k hodnotám, na které nejsou dříve budovaná datová centra připravena. Nové technologie se naštěstí dostávají do dostupnějších cenových hladin a díky tomu se blade řešení stávají také velmi zajímavým krokem ve středních a menších organizacích. Díky snadné údržbě, instalaci nových serverů a unifikované správě přináší časovou a finanční úsporu na obsluhu IT. [1]

Obr.1 Blade v provedení 7U a 14U [1, 2]

1.2 Blade servery – výkonné počítače na jedné desce

Blade nebo-li žiletka je server, který je maximálně zmenšen. Jeho vnitřní design je tvořen tak, aby byl kvůli své integrovanosti co nejkompaktnější tzv.“cable-less” (bez kabelu). Jakékoliv kabelové vedení by mohlo být pouze překážkou v proudění vzduchu. Není žádoucí, aby obsahoval nějaké pohyblivé části (kromě HDD, pokud má). Veškerá I/O konektivita je vyřešena multi konektorem do Blade Chassis. [2]

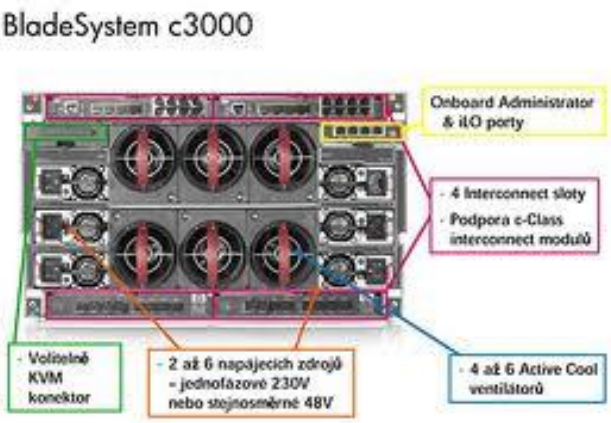
1.2.1 Z čeho je bladový systém složen?

Blade systém se samozřejmě neskládá pouze ze serverů, ty jsou v podstatě jen jakýmisi stavebními kameny. Jednotlivým prvků Blade systému jsou věnovány následující podkapitoly.

1.2.1.1 Blade Chassis

Blade server je zásuvný modul, který se zasunuje do Blade Chassis, což je jakýsi RACK v RACKu. Do chassis se zasouvá více serverů a poskytuje jim elektrické zdroje, výkon ventilátorů, vnitřní konektivitu a prostředky ostatních zásuvných modulů pro komunikaci s okolním světem. Vnitřní komunikace je zajištěna šterlinky samotné chassis. Chassis umožňuje konsolidaci KVM (Keyboard Video Mouse) je jeho součástí a tím také šetří zákazníkovi pořizovací náklady. [2]

Obr. 2 Detailní pohled na chassis bladu a na vysunuté servery [21]



Obr. 3 Schéma zadní strany bladu [1]

1.2.1.2 Blade Server – „Žiletka"

Blade server se až na svou velikost nijak neliší od klasického serveru. Lze jej konfigurovat dle vlastních požadavků a potřeb plánovaného datacentra. Samotná žiletka obsahuje pouze základní HW součásti nutné pro poskytnutí maximálního operačního výkonu. Součástí žiletky je tedy pouze:

- Základní deska
- Procesory
- Operační paměť
- Pevný disk pro instalaci OS

Obr. 4 Pohled na blade server v provedení se dvěma harddisky [22]

1.2.1.3 Zásuvné moduly

Kvůli modularitě a komplexnosti blade serveru je zadní strana vyhrazená pro napájecí zdroje, výkonné ventilátory a v neposlední řadě sloty pro I/O moduly. Např. interconnect moduly, On Board Administrator s iLO a KVM switche.

Je evidentní, že sestava blade je konfigurovaná dle přání zákazníka. Klient by měl z analýzy a návrhu nového datacentra vědět, jaké bude mít v budoucnu požadavky na funkcionalitu modulu. Zásuvné moduly totiž díky malým rozměrům a vysoké kvalitě nejsou levnou záležitostí. I zde je nutné mít na paměti, že blade řešení má mít kromě výkonu především i ekonomický přínos do budoucna.

1.2.1.4 I/O konektivita

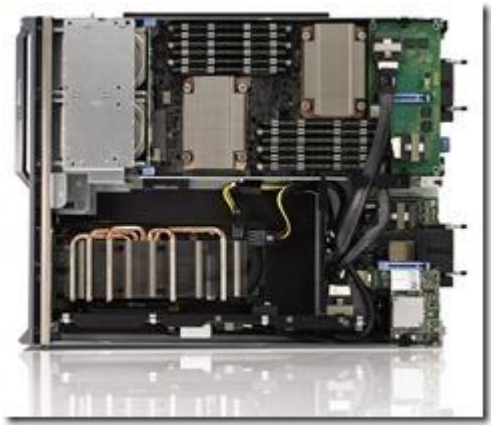
I/O konektivita je tvořena externí konektivitou a interní konektivitou. **Externí konektivita** je konektivita s okolním světem mimo blade chassis. I **interní konektivita** je konektivita I/O modulů oproti serverům a je to důvod, kdy je nevýhodné provozovat nezaplněné chassis. I/O Moduly totiž mají stejný počet portů do vnitřní konektivity, jako je počet portů k serverům (v některých případech i 2 na server). Nesmí tedy nastat situace, kdy si koupíme např. switch PowerConnect M6220 který má v sobě 4x konektivitu na vnější porty a 16x vnitřní konektivitu uvnitř chassis. To proto, že pokud využijeme jen 2 nebo 4 blade servery, zbude nám poměrně hodně nevyužitých portů, které máme zaplaceny. Ty totiž bohužel nemůžeme využít, protože nemáme zaplněné celé chassis. [2]

Takový problém s menším počtem serverů se dá samozřejmě také řešit tzv. Pass-thru moduly. To jsou v podstatě patch panely, které inteligentně vlastně propojují 1:1 interlinky s externími konektory. U takového řešení je ale nutné mít ještě externí switch, který zabírá další U v RACKu. V takovém případě se ale projeví nevýhody, protože propojení je nutné realizovat kabely, které ve stísněném prostoru slouží jako značná překážka v proudění vzduchu. Tím vlastně ztrácíme benefit v podobě jednotného managementu blade serveru , switche a jednoduchost přidání nového serveru. Následně musí být řešeno i zapojování kabelů zezadu a nestačí již jen zastrčit žiletku a vše ostatní udělat vzdáleně. [2]

1.2.1.5 PCI-E

Z předchozího popisu blade je patrné, že s omezenou velikostí serveru se musel udělat kompromis na straně rozšiřitelnosti. Do Blade se zkrátka nevleze PSI-E karta a nedá se tedy použít pro některé účely. Jejich rozšiřitelnost je provedena za pomocí tzv. mezzanin

karet. Klasickou PCI-E kartu je sice možné nechat do serveru přidat na zakázku, znamenalo by to všem velký zásah do designu serveru.

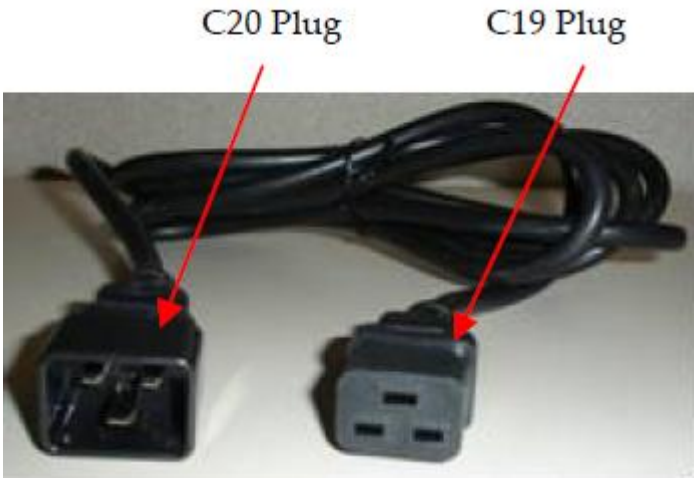


Obr. 5 Speciální úprava serveru s přidanou kartou [2]

1.2.1.6 Napájení

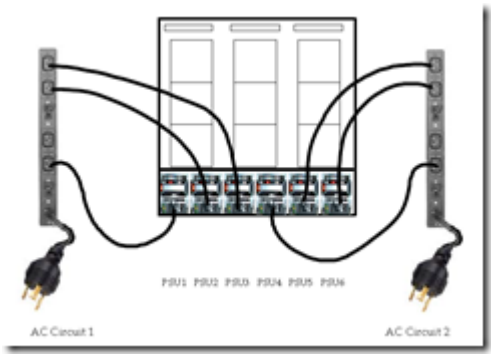
Blade jsou vyráběny tak, aby měly minimální spotřebu el. E

energie, ale celé chassis jako takové musí být dimenzováno na maximální osazení. Také kabely jsou kvůli splnění norem a elektrických vyhlášek dimenzovány tak, aby zvládly maximální osazení. Z tohoto důvodu musejí mít blade servery větší konektory přívodního napájení C20/C19, který je na 32A což rozhodně není standardní 16A konektor, jak jej známe z RACK/TOWER serverů a osobních počítačů,který se zasouvá do standardní 220V zásuvky. [2]



Obr. 6 Napájecí kabel s UPS konektory [23]

Realizace tedy probíhá v praxi přes tzv. PDU (Power Distribution Unit). Zde je ukázka realizace redundantního zapojení dvou single fáze 2x30A obvody ! (zástrčka na obr. je pro USA). [2]



Obr. 7 Schéma rackového zapojení k ups [23]

Z těchto informací se dá říci, že při plánování implementace bladu musí být implementační prostory řádně připraveny tak, aby byl zajištěn vždy dostatek elektrických rozvodů. V takových prostorách se můžeme setkat i s tím, že někde může být implementace neproveditelná díky nedostatku přívodních el. rozvodů (tedy velikosti jističů a průřezu přívodních drátů). To je další důkaz toho, že je nejvhodnější mít chassis zaplněné co nejvíce, aby investice do nových kabeláží nebyla do jisté míry zbytečná. [2]

1.3 Bez diskových polí se neobejde..

Data jsou pro společnosti velice důležitá, někdy dokonce kriticky důležitá. Rozhodujícími parametry jsou při výběru vhodného diskového pole rychlost přístupu k uloženým informacím a především jejich zabezpečení při případné havárii samotného pole či nepředvídatelné události. Pečlivě se zvažují všechny možnosti a vybírá se takové řešení, které vyhovuje zadaným podmínkám co nejvíce.

Blade servery, díky jejich velikosti, jsou omezeny co do počtu disků. Jak bylo zmíněno již výše, blady jsou designovány, aby pracovaly s diskovým polem.

Využít disková pole je důležité z několika důvodů. To proto, že zajišťují rychlejší přístup k datům, ale hlavně zabraňují při náhlém incidentu či havárii některého z disků, ztrátě dat. Disky jsou totiž podle předem definovaných pravidel spojovány do fyzických i logických celků s odlišnou vnitřní strukturou i funkcionalitou. Každé nastavení diskových polí je použitelné pro odlišné způsoby použití. Proto také finální nastavení podléhá analýze konkrétních požadavků na dostupnost či bezpečnost. [3]

Pokud se pro použití diskových polí, která jsou dávno nedílnou součástí serverových pracovišť, rozhodneme, musíme počítat s tím, že kapacita pro zásuvné disky je omezena počtem volných pozic v serverové skříni. Externí disková pole disponují vetší škálovatelností a dokonalejším zabezpečením přístupu k datům. Jejich výhoda je v tom, že z našeho pohledu nemají omezenou kapacitu. Provádí se v řešení jako skříně se zdvojenými zdroji ventilátory a řadiči. Externí disková pole se připojují k serverům přímo pomocí rozhraním SAS (Serial Attached SCSI) nebo tvoří samostatnou síť (SAN – Storage Area Network), která je určena pro ukládání dat s využitím technologie FC (Fibre Channel) nebo iSCSI. [3]

Obr. 8 Čelní strana diskového pole s horizontálním uložením zásuvných disků [24]

1.3.1 Zálohování dat

Disková pole jsou tedy z pohledu bezpečnosti uchování dat relativně spolehlivá a při ztrátě některé z mechanik data ochrání. Co ale dělat, když se stane havárie většího rozsahu, třeba živelné katastrofy nebo větší výpadek disků? Lidským chybám také nelze zabránit. V takových případech je důležité mít vypracovaný systém zálohování. Proto by se zálohovací mechanika (knihovna) měla stát automatickým doplňkem každého systému na ukládání dat. [3] Příkladem může být externí a interní pásková mechanika, která je zobrazena na obr. 9.

Obr. 9 Shora externí a interní páskové mechaniky [25]

1.4 Záložní zdroje

V dobře provedeném návrhu systému serverů a diskových polí je nezbytné myslet na záložní zdroje elektrického napětí (UPS). UPS-ky zaručují kontinuální provoz při výkyvech a výpadcích napětí a jinými negativními jevy v napájecí soustavě. Takové mohou způsobit nezvratné škody na IT vybavení. [3]

Záložní zdroj by se měl volit takový, aby splnil požadavky na dobu výdrže při plném výkonu napájených zařízení. Tedy na dobu nezbytně nutnou k provedení definovaných úkonů při náhlém výpadku proudu či havárii.

1.5 Správa

Správa bladových systémů je řešena přes webové rozhranní, které je provozováno na management modulu. Přes toto rozhranní lze hlídat stavy blade a ovládat a konfigurovat všechny napájecí zdroje, switche i samotné blade servery. K dispozici máme monitoring teplot, otáček větráků, aktuální spotřeby jednotlivých komponent atd. [4]

Nastavit a přizpůsobit se zde dá velké množství parametrů. Zmiňme alespoň možnost nastavení priority serverů. Toto nastavení má zvláštní význam při výpadku několika napájecích zdrojů, které nejsou v daný okamžik schopné napájet všechny servery. Tyto priority také ovlivní automatické vypínání jednotlivých serverů, do té doby, dokud systém nedosáhne stabilního stavu. V momentě, kdy se napájení obnoví na původní hodnoty, vypnuté servery začnou opět automaticky nabíhat. To je ovšem pouze jedna z mnoha chytrých funkcí, které lze pře management řešit. Samozřejmostí je zasílání informativních, varovných a chybových hlášek e-mailem. [4]

1.5.1 Administrátorské rozhranní – KVM

KVM Switch (zkratka KVM je odvozena z anglického keyboard, video, mouse pro **klávesnici**, **video** – neboli monitor, **myš**) je hardwarové přepínací zařízení, umožňující ovládat uživatelem více počítačů z jedné klávesnice, monitoru a myši. V jeden okamžik jde samozřejmě ovládat pouze jeden počítač, na který je zrovna alokován aktivní port. Připojeno jich ale může být tolik, kolik je portů na KVM zařízení. Novější KVM switche dokáží publikovat i jiné periferní porty, např. USB zařízení, reproduktory atd.. Některé KVM switche mohou také fungovat v opačném směru – tedy jeden počítač lze připojit na více monitorů, klávesnic a myší. I když tato možnost není tak častá, i tato konfigurace je užitečná, když chce uživatel získat přístup k jednomu počítači ze dvou nebo více (obvykle blízkých) míst. [5]

1.6 Chlazení

Chlazení je důležitou součástí každé serverovny a jako takové není přímo součástí blade. Proto je při návrhu nutné uvědomit si, zda bude nové nebo stávající chlazení dostatečně odvádět teplo od skříní racků. Dopředu si také musíme dobře rozmyslet,, zda potřebujeme chladící jednotku pro velké sály či pro malou serverovnu o velikosti kanceláře.

Jaké požadavky má klimatizační zařízení splňovat [6]?

- Chladící výkon klimatizačního zařízení musí odpovídat celkové tepelné zátěži serverovny.
- Operační rozsah venkovních teplot musí umožnit celoroční provoz v režimu chlazení tj. minimálně -15°C až + 40°C.
- Musí být zvolen správný typ jednotky s ohledem na cirkulaci vzduchu v serverově, rozhodující je i její umístění.
- Instalační možnosti zařízení – např. maximální délky potrubí a převýšení mezi vnitřní a venkovní jednotkou (kondenzátorem) a hlukové parametry musí splňovat podmínky konkrétní instalace.
- Výhodou je možnost dálkového dohledu, minimálně je nutná signalizace poruchy klimatizace nebo teplotního alarmu beznapěťovým kontaktem.

Obr. 10 Skříňové ventilační systémy určené pro chlazení serveroven [26]

2 PLÁNOVÁNÍ BLADOVÉHO ŘEŠENÍ

Tlak na snížení nákladů na IT se týká i moderních datových center. Důvodem jsou stoupající ceny energií a pronájem za místo. Trend zvyšování cen energií vede k vyrovnání investičních nákladů za hardware a poplatků za energie v roce 2011.

V dnešní době se na trhu objevuje nesčetné množství výhodných nabídek na Blade řešení. Často se také stává, že dodavatelé hardwaru tlačí na pořízení Blade řešení do firemních infrastruktur. Blade řešení může vyžadovat značnou investici v řádu miliónů až desítek miliónů korun. Proto je obzvláště důležité, aby vedení podniku a IT oddělení bylo přesvědčeno o provozních a ekonomických výhodách nasazení Blade v jejich prostředí. Efektivní návrh infrastruktury je další prostor k úsporám.

2.1 Kdy se rozhodnout pro blade?

Množství spotřebované enrgie na serverových zařízeních a serverovnách se pohybuje okolo 30–40 %. Proto jsou vedeny jako jedny z nevyšších priorit právě úspory za energie a zavádění efektivních energeticky úsporných opatření. Běžná serverová zařízení v typických serverovnách nebo datových sálech zahrnují standardní servery, které se montují do IT rozvaděčů, ale také stojanové servery a více-uzlové servery (multi-node). [7]

Energetické úspory mají ohromný potenciál a v závislosti na typu IT systému a aplikovaných opatřeních mohou energetické úspory dosahovat 20–60 % nebo ještě více oproti stávajícím řešením. Nejdůležitějším krokem pro zlepšení energetické účinnosti, jsou přístupy k těmto řešením. Výběr by měl zahrnovat energeticky efektivní hardware a návrh systému správy napájení na všech úrovních od hardwarových komponent až po celý systém. V neposlední řadě je nutné myslet také na konsolidaci hardwaru a virtualizaci. [7]

2.2 Virtualizace serverů

Nejen z pohledu úspory energie se nabízí velký potenciál ve využití virtualizace. Technologie virtualizace, která umožňuje konsolidovat provozní zátěže nižšího počtu hardwarových zařízení, silně snižuje požadavky na chlazení a napájení. Využití virtualizace nám s efektivním návrhem IT systémů serverových a datových centrech nabízí řadu výhod. [7]

2.3 Efektivní návrh infrastruktury

Již byl několikrát zmíněn fakt, že datová centra se neobejdou bez tzv. efektivního návrhu infrastruktury. Takový návrh potom udává prostor k dalším úsporám. Pokud si vezmeme např. Ethernet, mluvíme zde o Agregační vrstvě a Access vrstvě. Pro FC síť se definuje Core a Edge vrstva. Dostatečnou přenosovou kapacitu by měly poskytnout obě z nich a také nabídnout rozumnou oversubscripci v poměru 4:1 až 12:1. Oversubscripce je přirozená vlastnost libovolné sítě. Navrhovat oversubscripci menší 4:1 je neefektivní, může být vyžadovaná pouze pro specifické aplikace. Oversubsripce za hranicí 12:1 může způsobovat výkonnostní potíže. [8]

Architektury dnešních datových center ovšem počítají se třemi oddělenými infrastrukturami pro Ethernet provoz a pro SAN. Takový koncept vyžaduje připojení do obou sítí jak blade serverů, tak i rack serverů redundantně. Také se musí počítat s tím, že se zvyšujícím se počtem chassis roste lineárně počet portů a kabelů. Správci na začátku implementace často neznají počty a požadavky na rozhranní a propustnost, a proto se během celé implementace jejich požadavky mění. Pozdější zásah totiž bývá v pozdějších fázích značně problematický. [8] Příklad efektivního návrhu infrastruktury zachyceného v grafickém prostředí znázorňuje obr. 11.

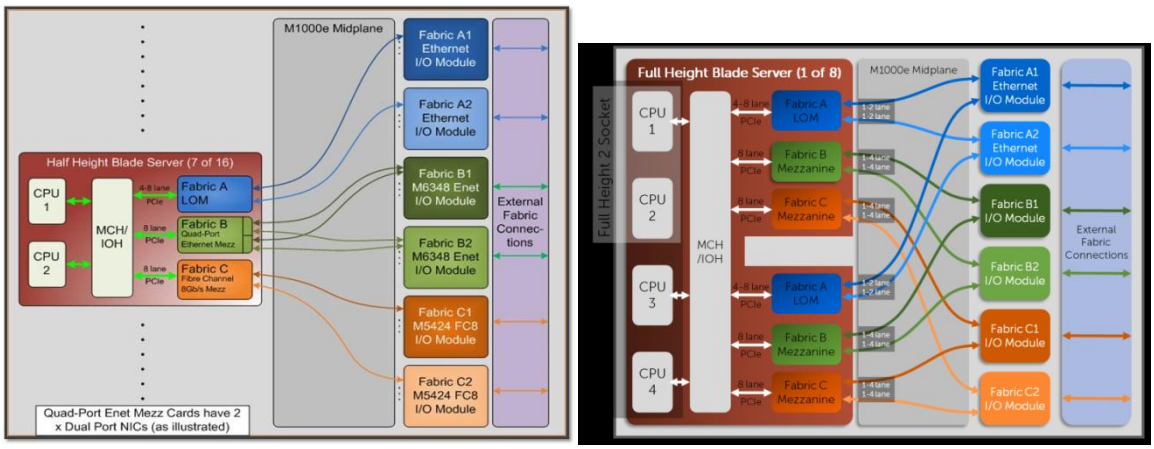
Obr. 11 Příklad efektivního návrhu infrastruktury zachyceného v grafickém prostředí [27]

2.4 Výhody

Důvodů, proč se rozhodnout pro Bladové řešení je samozřejmě hodně. Podle požadavků zákazníka lze přijít na nové a nové důvody, proč Blady nasadit. Zmíníme alespoň ty hlavní:

Jednoduchá implementace – za pomocí speciálních kolejniček se dá server snadno zasunout do chassis bez použití dalších nástrojů. Pokud tedy chce klient přidat další blade server, a pokud má nastaveny všechny prvky prostředí, jako jsou třeba switche pro budoucí žiletky, celý úkon nezabere víc než několik minut [2]

Plně osazené chassis je např. na tomto obrázku i se schématem zapojení vnitřního InterConnect.



Obr. 12 Schéma vnitřního zapojení šterlinků bladu [2]

Jednoduchý management – jak bylo zmíněno již výše, celý management balde serverů je na úrovni chassis, tím získáme jednoduchost a v celém systému není problém se vyznat. Za použití KVM navíc získáme praktický a jednoduchý přístup k managementu. KVM je levnější pořizovat již integrovaný než jej kupovat odděleně. Navíc se blade chassis dají propojit mezi sebou.

Úspora místa - Díky konsolidaci ventilátorů, napájecích zdrojů, síťových adaptérů, KVM a SAN switchů jsme schopni ušetřit nemalé prostory.

Úspora energie - Díky již zmíněné konsolidaci jsme schopni uspořit také dosti významně spotřebu elektrické energie.

Flexibilita – Blade servery jsou navrženy tak, aby bylo v rámci několika minut možné přesunout server z jednoho chassis do druhého bez toho, aniž bychom museli něco konfigurovat. [2]

Disk Less - Blade servery jsou navrženy tak, že ideální kombinace je s diskovým polem SAN. Dá se u nich nakonfigurovat funkce Boot From SAN, a protože až 30% spotřeby serveru můžou tvořit HDD, je prakticky ideální využít dnešní možnosti virtualizace jako je VMWARE ESXi nebo Microsoft Hyper-V, Hypervisor bootuje z SD Karty. Virtuální servery jsou pak umístěny většinou na diskovém poli SAN. [2]

Dostupnost - Je také možné vytvoření hot-spare blade pro účely výpadku jiné žiletky.

2.5 Nevýhody bladových řešení

Žádný systém není dokonalý a i bladové systémy mají své nevýhody. Nutné je ale říci, že i když by se nevýhod dalo najít hodně, tak výhody většinou přebijí všechny nevýhody. Hlavním problémem, který často řeší centra s malými prostory je velká produkce tepla. Pokud je bladových systémů v serverovně více, vyvstává zde důležitá otázka týkající se chlazení takového prostoru. Do serveroven totiž není vhodné instalovat běžné kancelářské klimatizace, ale speciálně řízené klimatizační jednotky. To s sebou ovšem nese další zvýšení nákladů. S tímto je nutné při plánování již počítat.

S tím souvisí i situace, kdy zákazníci nechávají některé racky volné a efektivita využití drahého prostoru se rapidně snižuje.

Další nevýhodou je bezesporu to, že každý výrobce používá proprietární chassis. Servery a moduly prostě není možné koupit od různých výrobců, což může způsobovat pomalý nárůst ve využití bladových systémů. Zákazník je pak donucen využívat pouze moduly jediné firmy i do budoucna a spoléhat na podporu starého chassis u produkce nových modulů.

3 VIRTUALIZACE NA BLADE

Při snižování nákladů je kladen velký důraz na úsporu místa, šetření elektrické energie při nižší potřebě chlazení a napájení virtualizovaných serverů. Tím, že se snažíme integrovat více virtuálních serverů na jeden fyzický, zvyšujeme průměrnou zátěž procesorů z původních 15% na 40-60% a tím efektivitu využití výpočetní kapacity. K úspoře místa přispívá také použitý form factor blade serverů. [8]

3.1 Virtualizační architektury

Pro přehlednost je nutné na začátku objasnit typy architektur a metod, které se pro virtualizaci x86 serverů používají. Na počátku virtualizace pracovaly virtualizační produkty přímo nad obecnými operačními systémy. Ovšem obecný operační systém bude mít oproti tenkému jednoúčelovému operačnímu systému, který je vyladěný pro virtuaizaci, vždy vyšší režie. Tenký operační systém je ve virtualizaci tzv. hypervisor. Hypervisor je zodpovědný za management paměti a management I/O prostředků a operací a také rozděluje celkový výpočetní výkon. Vlastní virtualizaci obstarává pro každý virtuální server samostatná komponenta VMM – Virtual Machine Monitor, která zajišťuje komunikaci mezi virtuálním serverem a hypervisorem. Hypervisor pracuje přímo nad fyzickým hardwarem. V principu se v rámci VMM mluvit o třech typech vitualizačních metod [9]:

- **Softwarová emulace hardwaru** (Full Virtualization-Binary Translation) – Výhodou softwarové emulace je absolutní nezávislost na hardwaru a to umožňuje provozovat ve virtuálních serverech nezměněné operační systémy. Nevýhodou jsou vysoké nároky na režie.
- **Virtualizace s hardwarovou asistencí** (Hardware Assisted Virtualization) – Kvůli rychle se měnícím a rostoucím požadavkům jsou výrobci hardwarových komponent nuceni zaměřit se na hardwarovou podporu virtualizace na úrovni procesorů chipsetů, paměti, síťových karet a host bus adaptérů. Díky přenechání některých činností hardwarovým komponentám je možné minimalizovat virtualizační režii hypervisorů.
- **Paravirtualizace** – Je to metoda virtualizace, která vyžaduje zásah do jádra operačního systému, který je provozován ve virtuálním prostředí. Jádro paravirtualizovaného operačního systému obsahuje speciální procedury, které

dokáží přesměrovat určité instrukce, které by jinak byly vykonány hardwarem do hypervisoru přes tzv. root partition (často nazývanou Domain0 nebo kontrolní doménou). S užitím paravirtualizace je obecně známá nižší výkonnostní režie, na rozdíl od plné softwarové emulace

Každá z výše uvedených metod má své výhody i nevýhody a většina porovnávaných platforem používá více virtualizačních metod.

3.2 Aktuální trend ve virtualizaci

Virtualizačních platforem pro PC servery je celá řada. Stačí si pročíst výsledky hledání na Google.com, kde je jich nespočet. Při důkladnějším prostudování je možné zjistit, že za hlavní proud lze považovat produkty dvou tradičních a na trhu virtualizace největších firem, VMware a Microsoft.

Nová éra virtualizačních platforem začala v roce 2008. To přišly firmy s novými verzemi virtualizačních platforem hypervizorů. U VMwaru to byly VMware s ESX Server 3.5i a u Microsoftu to byl Windows 2008 Hyper-V. U obou produktů se již veřejnost konečně dočkala využití nových virtualizačních funkcí moderních x86/x64 procesorů (technologií Intel VT a AMD-V), podporující i jejich 64bitovou architekturu. Zajímavé je sledovat na trhu souboj těchto virtualizačních gigantů, jehož výsledkem je jednak technologický rozvoj, především však zlevňování a zpřístupňování virtualizačních technologií širokému spektru „běžných“ zákazníků. Oba produkty jak VMware ESXServer 3.5i a i zbrusu nový Microsoft Hyper-V Server 2008 jsou ke stažení zcela zdarma. Platí se pouze za profesionální licence. Co nejširší paletu virtualizačních prostředků od serverů až po pracovní stanice či jednotlivé aplikace se snaží pokrýt obě firmy, ale je zde patrná hlavně snaha vytvořit jednu integrovanou virtualizační infrastrukturu. I proto si mohou obě firmy dovolit nabídnou základní komponenty své virtualizační platformy zdarma. Jejich byznys je totiž postaven na nástavbových funkcích nezbytných pro profesionální provoz virtualizovaných prostředí v prostředí podniků. [10]

Firma VMware se může pochlubit delší historií v oblasti virtualizace PC a dokáže svých zkušeností plně využít. Dá se proto říci, že je momentálním lídrem trhu na poli virtualizace, jak z pohledu technologického, tak i z hlediska podílu na trhu.

Windows Server Hype-V se dal spolu s rodinou System Centerdo vážně míněného konkurenčního boje a v budoucích letech bude více než zajímavé tento souboj sledovat,

zda vůbec a případně v jakém časovém horizontu náskok VMware dožene. Stačí vzpomenout na dřívější „neotřesitelnou“ pozici Novell NetWare oproti Windows NT v oblasti síťových operačních systémů. [10]

3.3 Jak si vybrat virtualizační platformu

Bez Virtalizace se dnes v podstatě neobejde žádný moderní systém a dalo by se říci, že je opravdu i nutností. Ale když už reorganizace rozhodnou pro virtualizaci, tak jaký systém zvolit VMware nebo Hyper-V? Při pořizování serverové virtualizace je nutné promyslet jaký tzv. Hypervizor zvolit - ten je vlastně tím nejdůležitějším v rámci využití virtuálních strojů. Nicméně víme-li, co od virtualizace chceme a co virtualizace přináší (jako je konsolidace serverů, menší nároky na napájení, rychlejší nasazení nových serverů) pak musíme myslet na to, že celou virtualizační platformu je nutné také spravovat, podporovat atd. [11]

Je nutné si před samotným technickým porovnáním alespoň v krátkosti představit ty hlavní posuzované platformy tak, aby byl zřejmý celý širší kontext. Hypervisor je jednou z důležitých komponent virtualizační platformy, ale bez softwaru pro centrální správu infrastruktury by vlastně nebyl použitelný. [9]

3.3.1 Přínosy virtualizace platforem

Od virtualizace platforem jsou očekávány následující přínosy [12]:

- **konsolidace serverů v rozsáhlém IS** – co největší integrace virtuálních serverů na co nejmenší počet fyzických serverů, to se rozumí konsolidací serverů. Tím se uspoří potřebná elektrická energie, prostory a náklady na hardwarovou podporu vzhledem k menšímu počtu fyzických serverů;
- **minimalizace vzájemného ovlivňování provozovaných systémů** - virtualizace také umožňuje ještě více rozvinout trend specializace jednotlivých serverů, instalovaný software má tak vlastní provozní prostředí a není negativně ovlivňován jiným instalovaným softwarem v rámci stejného systému;
- **zvýšení dostupnosti a provozní spolehlivosti služeb ICT** - jednoznačně rychlejší a pružnější obnova po výpadku - virtuální stroje právě běžící na havarovaném fyzickém serveru lze velmi rychle a během okamžiku opět spustit na jiném fyzickém serveru, a to i třeba ve zcela jiné lokalitě. U nových virtualizačních

softwarů dokonce zcela automaticky. Dále umožňuje snazší a efektivnější zálohování celých virtuálních serverů;

- **sjednocení testovacího a provozního prostředí** – díky virtualizaci může být testovací prostředí takřka identické s tím produkčním. Kdykoliv jej můžete obnovit do původního bodu, či vytvořit jeho klon;
- **snazší doplňování a obnova HW vybavení** – implementace je značně zjednodušená, protože v případě virtualizace stačí na nový fyzický server instalovat jen virtualizační prostředí. Virtuální stroje, které chceme v provozu se pak na nový server jednoduše přenesou. Tím lze dosáhnout značné úspory práce a času v řádu dnů až týdnů.

3.3.2 Nároky a nevýhody virtualizace platforem

Každá technologie s sebou přináší určité výhody, ale také řadu nevýhod a nároků na jednotlivé segmenty odvětví. Hlavní nevýhody jsou shrnuty v následujících bodech [10]:

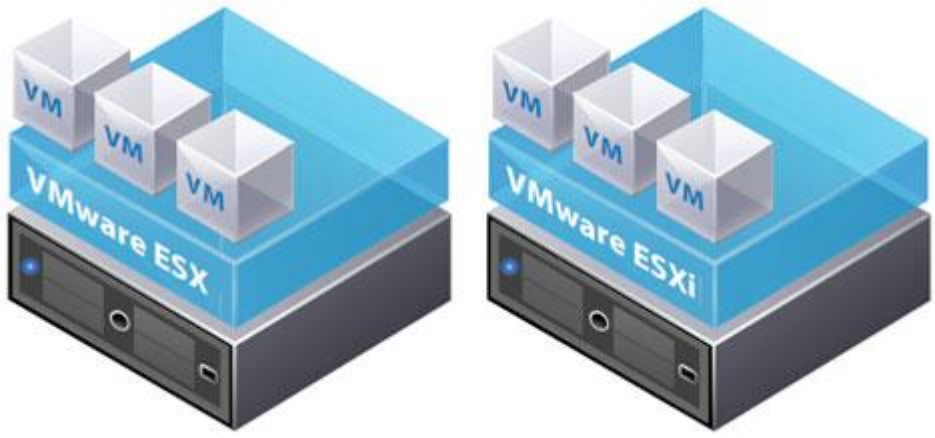
- **potřeba přenesení stávajících fyzických prostředí do virtuálních strojů** - tento jednorázový proces lze podpořit použitím specializovaného P2V - physical to virtual software - pro přenesení „obsahu“ fyzického serveru do virtuálního;
- **vyšší HW nároky a jistý výkonový propad** – samozřejmě, že virtualizace a virtualizační SW mají také nároky na režie. Reálný pokles výkonu způsobený virtualizací prostředí se však může lišit dle zátěže a způsobu využití jednotlivých virtualizovaných systémů;
- **exploze virtuálních serverů** – výhodnost virtualizace s jednoduchostí při vytváření nových virtuálních stanic vede k ohromnému nárůstu jejich počtu. Ideálním místem jsou různá testovací prostředí, která využívají možnosti vytváření klonů a je tak vždy zaručeno homogenní prostředí pro testy;
- **správa, údržba a záplatování virtuálních OS** – virtuální servery je ale také nutné udržovat, stejně jako fyzické servery. Je proto ideální využít automatizovaných funkcí a nástrojů virtualizátorů a maximálně zefektivnit jejich údržbu. Aktualizace a záplaty lze bezpečně distribuovat v rámci virtuálního prostředí bez vnějších vstupů;
- **zvýšené licenční nároky a složitost** – licenční politiky k provozování virtuálních serverů se značně liší dle potřeby a využití zákazníky. Sice mohou být stejná jako v případě fyzických serverů nicméně snahou výrobce je získat od zákazníka co

nejvíce peněz, a proto jsou v licenčních politikách zaneseny podmínky, které mohou nákup jak prodražit, tak zlevnit.

3.4 VMware ESX a ESXi

Produktovou řadu firmy VMWare tvoří základ v podobě VMware ESX a VMware ESXi Ty jsou určeny pro výstavbu spolehlivé a dynamické infrastruktury informačních technologií. Tyto v produkčním nasazení ověřené hypervizory mají rozhodující podíl na trhu, abstrahují prostředky paměti, úložišť, procesorů a sítě do podoby virtuálních strojů, Bez nutnosti jakýchkoliv úprav v nich lze provozovat jakýkoliv operační systém a nejrůznější aplikace. Jak z výše uvedených faktů plyne, VMware ESX a ESXi jsou nejčastěji nasazovanými hypervizory. Do podniků jakékoliv velikosti přinášejí spolehlivost a výkon na nejvyšší úrovni.

Nejnovějším řešením hypervizorů VMware je VMware ESXi. Nezávislost tenké architektury na obecném operačním systému i tak nabízí stejný výkon i funkce jako systém VMware ESX. VMware ESXi dále zvyšuje laťku bezpečnosti a spolehlivosti, neboť menší velikost jeho kódu omezuje prostor k útoku i potřebu oprav. Malá velikost a spolehlivost na úrovni hardwaru umožňují systému VMware ESXi integraci do standardních serverů na platformě x86 od předních výrobců, jako jsou Dell, IBM, HP a Fujitsu-Siemens. Při jeho návrhu byl především kladen důraz na jednoduchost a zároveň spolehlivost. Spuštěním pomocí nabídek a automatické konfigurace je možné přesvědčit se o nejsnazším způsobu, jak začít s virtualizací na prostředí VMWare. [13]



Obr. 13 Grafické schéma vrstev vmwaru znázorněna společností Vmware [13]

3.4.1 Jak systémy VMware ESX a VMware ESXi fungují?

Virtualizační systémy VMware ESX a VMware ESXi vkládají robustní virtualizační vrstvu mezi operační systém a hardware, instalují se tak přímo na hardware serveru. VMware ESX a ESXi dělí fyzický server na řadu přenositelných a bezpečných strojů. Takové pak mohou běžet na jednom fyzickém serveru současně. Každý nainstalovaný virtuální stroj představuje kompletní systém s pamětí, procesory, úložištěm, připojením k síti a systémem BIOS. Softwarové aplikace i samotný operační systém tak můžeme na virtuálním stroji instalovat i provozovat bez jakýchkoliv úprav a běžný uživatel si ničeho nevšimne. Virtuální stroje jsou také od sebe absolutně odděleny mohutnou virtualizační vrstvou. Pád jednoho stroje nebo některé aplikace tak nemá sebemenší vliv na chod jiných virtuálních strojů. Tím, že jsou fyzické prostředky efektivně sdíleny mezi všechny virtuální stroje dle konfigurace jednotlivých virtuálních strojů, se zvyšuje využití hardwaru a výrazně se omezují investice. Provoz přímo nad hardwarem dává systémům VMware ESX a ESXi plnou kontrolu nad prostředky serveru přidělenými jednotlivým virtuálním strojům a umožňuje výkon virtuálních strojů blízký fyzickým strojům a škálovatelnost podnikové úrovně. Systémy VMware ESX a ESXi poskytují virtuálním strojům vestavěné funkce pro vysokou dostupnost, bezpečnost a správu prostředků, s nimiž dokáží softwarovým aplikacím poskytovat vyšší úrovně služeb než statická fyzická prostředí. [13]

3.4.2 Klíčové vlastnosti

O vmwaru se dlouhodobě mluví jako o lídru na trhu. To je samozřejmě otázka diskuzí a záleží na úhlech pohledu. Nicméně zde je několik důvodů, proč by to tak mohlo být [13]:

- VMware udává, že disponuje rekordním výkonem až 8 900 databázových transakcí za sekundu, 200 000 vstupně-výstupních operací za sekundu a 16 000 poštovních schránek serveru Exchange na jednom fyzickém hostiteli.
- Až osm virtuálních procesorů (symetrický multiprocesing), což umožňuje virtualizaci zátěže využívající více procesorů.
- Přidělování paměti „na dluh“ a odstraňování duplikace paměti umožňují vyšší poměry konsolidace.
- Vestavěná podpora pro vysokou dostupnost díky spojování síťových karet a vícenásobným cestám pro adaptéry HBA chrání před selháním hardwarových komponent.

- Až 64 logických procesorových jader, 256 virtuálních procesorů a 1 TB paměti RAM na hostitele umožňují dosáhnout vyšších poměrů konsolidace.

3.4.3 Možnosti správy

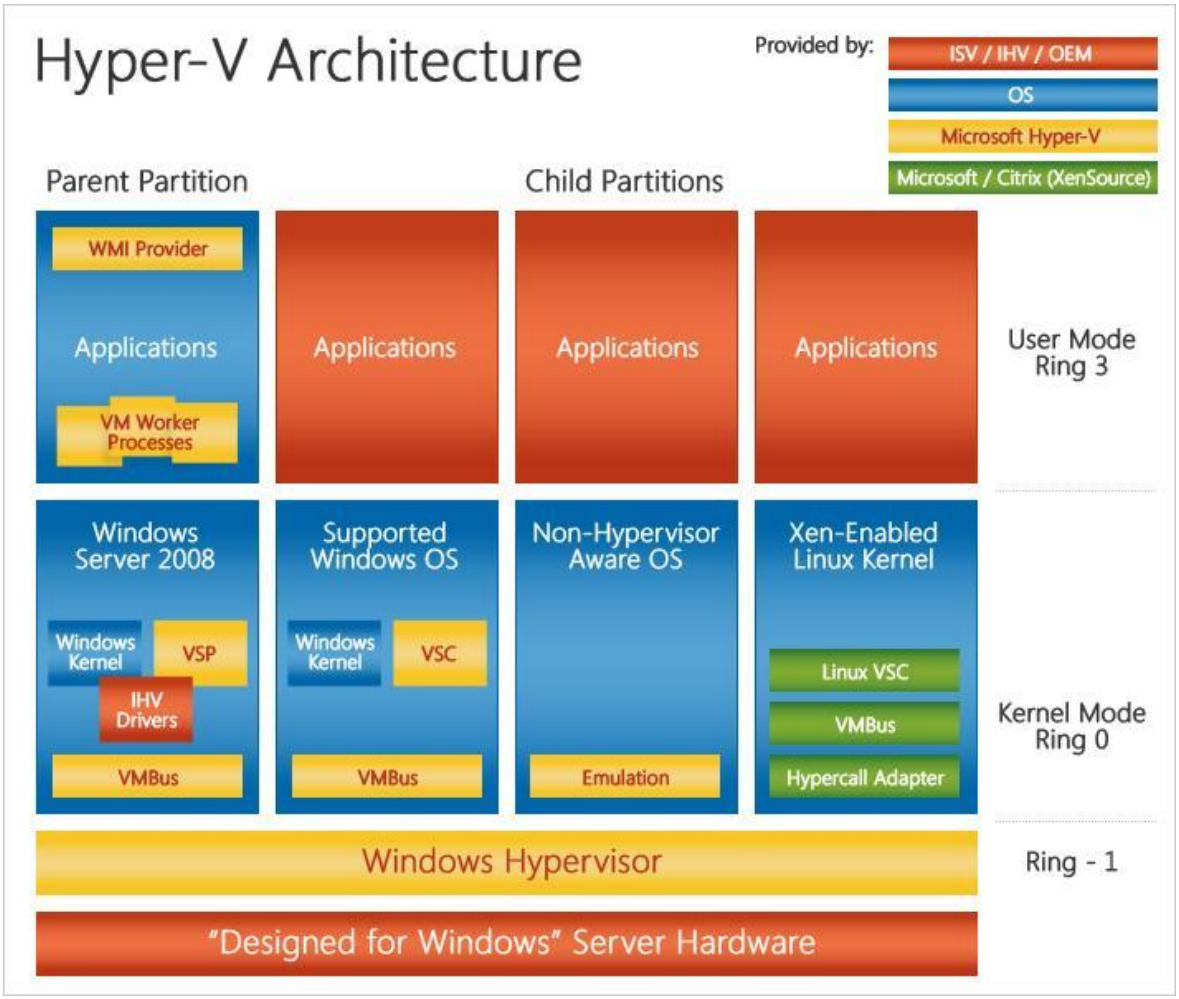
Pro efektivnější prostředí se systémy VMware ESX a ESXi je k dispozici několik rozhraní pro správu. Hlavními rozhraními, která správci systémů VMware ESX a ESXi používají, jsou [13]:

- **VMware vSphere™ Client.** Společnou správu systémů VMware ESX a ESXi, umožňuje uživatelské rozhraní nástroje VMware vSphere Client. VMware vSphere Client ale umožňuje i správu virtuálních strojů a (volitelně) systémů VMware vCenter Server. Nástroj vSphere Client lze bezplatně stáhnout. Nabízí připojení k hostiteli VMware ESX či ESXi a správu jednoho hostitele nebo připojení k systému vCenter™ Server a správu více hostitelů.
- **VMware vCenter Server.** Poskytuje uživatelům centralizovanou správu hostitelů VMware ESX a ESXi a jejich virtuálních strojů. Pro správu hostitele VMware ESX nebo ESXi pomocí nástroje VMware vCenter Server je zapotřebí licence k nástroji VMware vCenter Agent, která je součástí všech edic platformy VMware vSphere™. Platforma VMware vSphere nabízí mnoho dalších možností správy, které zlepšují kontinuitu podnikání a maximalizují efektivitu provozu. Takovými funkcemi jsou migrace v reálném čase, automatické vyvažování zátěže, ochrana před selháním hardwaru a možnosti zálohování a obnovy virtuálních strojů.

3.5 Microsoft Hyper-V

V 21. století snad neexistuje počítačový uživatel, který by neznal společnost Microsoft. Její krok, pustit se na trh virtualizačních technologií, byl jakýmsi logickým vyústěním jejich produktového portfolia. Microsoft totiž hraje významnou roli v serverových a desktopových operačních systémech a logicky se nechce dělit o zásluhy na využití jejich operačních systémů na virtuálních strojích. Microsoft s virtualizací začal tak, že koupil v únoru 2003 společnost Connectix, která od roku 1997 vyvíjela produkt Virtual PC pro počítače Apple Macintosh a v roce 2001 přišla i s verzí pro Windows. Ale již během akvizice společnosti Microsoftem se usilovně pracovalo na serverové verzi a první verze produktu Virtual Server byla uvolněna rovněž v roce 2003. [9]

Jak je zřejmé z předchozího textu, Hyper-V označuje virtualizační technologii od Microsoftu, která přichází spolu se serverovým operačním systémem Windows Server 2008. Aby byla distribuce virtualizačního systému co nejrychlejší, zvolil Microsoft svou oblíbenou fintu. Microsoft se tentokrát rozhodl implementovat tuto funkci do svého nového systému rovnou jako jednu ze serverových rolí. Na rozdíl od předešlých verzí virtualizace se ta současná liší hlavně tím, že jde o čistě hardwarovou virtualizaci. Hyper-V používá hypervisor v podobě tzv. **mikrojádra**, které obsahuje opravdu jen ty nejnutnější funkce pro virtualizaci a na rozdíl od přístupu tzv. monolitického hypervisoru neobsahuje ovladače zařízení. Toje rozhodně správný nově zvolený přístup, jelikož nutnost instalace ovladačů třetích stran přímo do hypervisoru by představovala riziko pro stabilitu i bezpečnost celého systému. To si Microsoft rozhodně nemohl dovolit. Jelikož se jedná o plně hardwarovou virtualizaci, je k provozu serveru s technologií Hyper-V třeba i speciální hardware. Hyper-V je potřeba zajistit hardwarovou podporu pro virtualizaci (AMD-V nebo Intel VT) a také Data Execution Prevention (DEP = AMD (NX no execute bit), nebo Intel (XD execute disable)). Podmínka x64bit systému v tomto případě platí pouze pro hostitelský server. Servery virtualizované na této platformě mohou být jak 64bitové, tak i 32bitové. [14]



Obr. 14 Zachycení architektury Hyper-V od Microsoftu [28]

3.5.1 Proč Hyper-V používat?

Hyper-V poskytuje dynamickou, spolehlivou a dostupnou virtualizační platformu spojenou s integrovanými nástroji pro správu fyzických i virtuálních zdrojů, která umožňuje vytvořit dynamické datové centrum. Takže proč se může Hyper-V rovnat s vmwarem? Důvody jsou jasné [15]:

- **Zajištění kontinuity provozu a disaster recovery** jako jsou neočekávané výpadky proudu, vykonáváním rutinních úkolů, stejně tak správa a zálohování. Pokročilé funkce pro zajištění kontinuity provozu jsou součástí Hyper-V, další, jako je zálohování za běhu či rychlá migrace, a umožňuje tak splňovat přísné požadavky na rychlou reakci a znovuobnovení chodu systému.

- **Disaster recovery** zajišťuje klíčovou součást procesu zajišťující kontinuitu provozu. Pro administrátora tak není problém při přírodních pohromách, zákeřných útocích, či při problémech konfigurací obnovit zálohovaná data.
- **Rychlá migrace** je velice užitečná funkcionalita, které umožňuje rychle zmigrovat běžící virtuální počítač z jednoho fyzického hostujícího systému na jiný s minimální dobou odstávky. Rozšiřují se tak známé funkce pro vysokou dostupnost v systémech Windows Server a System Center.
- **Network Load Balancing (softwarové rozkládání zátěže)** Hyper-V nyní nově obsahuje nové, lepší možnosti práce s virtuálním switchem. Virtuální počítače mohou být jednoduše konfigurovány pro běh se službou Network Load Balancing k rozkladu zátěže zatížení napříč virtuálními počítači na různých serverech.
- **Podpora SMP (Symmetric Multiprocessors)** Náročné aplikace také využijí schopnost Hyper-V podporovat až čtyři procesory v prostředí virtuálního stroje a poskytnout tak všechny výhody vícevláknových aplikací.

3.5.2 Možnosti správy

Hyper-v je součástí nástroje Server Manager a jeho prostřednictvím lze nyní Hyper-V nainstalovat jako roli serveru.

Po instalaci role Hyper-V již veškerá práce, nastavení a cokoliv dalšího s Hyper-V probíhá v konzoli Hyper-V Manager. Hyper-V Manager lze spustit dvěma způsoby a to jak na samotném serveru, tak také jako součást balíku administrátorských nástrojů pro vzdálenou správu RSAT (Remote Server Administration Tools). Díky tomu můžeme Hyper-V Server plnohodnotně administrovat i vzdáleně, například z Windows Vista nebo Windows 7. [16]

Obrovskou výhodou, kterou se může Hyper-V chlubit je použití mocného skriptovacího nástroje PowerShell. Díky tomu si může správce systému naskriptovat úlohy, které zjednoduší správu celého systému. Když k tomu přidáme velkou časovou úsporu, může být např. migrace virtuálních serverů podle využití prostředků plně automatizovanou záležitostí.

3.6 Použití profesionálních produktu SYSTEM CENTER

Systém Center je rodina produktů, která obsahuje ucelenou sadu neocenitelných konfiguračních nástrojů a prostředků pro správu fyzického a virtuálního prostředí a jejich monitoring. Nejnovější sada nástrojů System Center 2012 ovšem správu a monitoring pozvedává na jinou úroveň a umožňuje monitoring a správu soukromých cloudů, veřejných cloudů i jejich kombinaci. [17]

S produkty System Center Microsoft dává jasný signál k tomu, že chce hrát klíčovou roli v dlouhodobé vizi společností a také, jakchce IT organizacím pomoci se samospravujícími dynamickými systémy. Řešení System Center vyhledávají a shromažďují informace o infrastruktuře, zásadách, procesech a ověřených postupech, aby IT specialisté mohli optimalizovat IT struktury s cílem snížit náklady, zvýšit dostupnost aplikací a zlepšit poskytované služby. [18]

Není účelem této práce seznámit se podrobně s celou rodinou produktů System Center, blíže si proto popíšeme pouze System Center Virtual Machine Manager.

Nejdříve je nutná rekapitulacet Microsoftu a virtualizace. Před třemi lety se na trhu objevila firma Microsoft s novou Windows Server 2008 Hyper-V rolí, kterou nejprve představila jako samostatnou platformu pro virtualizaci, náhradu zastaralé technologie Microsoft Virtual Server 2005. Rázem se tak stala přímou konkurencí projiž zaběhnutou a dominující platformu VMware. V té době byl již na trhu System Center Virtual Machine Manager 2007, který byl určený ke správě prostředí Microsoft Virtual Serveru 2005. S příchodem Hyper-V byl nahrazen verzí System Center Virtual Machine Manager 2008 umožňující nyní i správu Hyper-V prostředí, ale také platformy VMware 3.5, což produktům Microsoft začalo značně hrát do noty. Novinkou byla i funkce Performance and Resource Optimization (PRO) nebo automatické umísťování virtuálních počítačů na host servery. Po dalším roce a půl byl dokončen Windows Server 2008 R2 a s ním i nová verze Hyper-V. Opět byla na trhu k dispozici nová verze produktu System Center Virtual Machine Manager 2008 (SCVMM), nyní však s označením R2. Hlavní novinky, které se v této nové verzi objevily byly např. podpora Live a Storage migrace, clustered shared volume (CSV), síťová optimalizace nebo maintenance mode. [19]

System Center Virtual Machine Manager se může chlubit tím, že umožňuje zvýšenou fyzickou využitelnost serveru. Tohoto docílí tak, že umožňuje jednoduchou a rychlou konsolidaci ve virtuální infrastruktuře. To vše umí díky Physical-to-Virtual (P2V) migraci

a inteligentně rozložené zátěži, která je založená nauživatelských nastaveních a na výkonu dat. System Center Virtual Machine Manager rychle poskytuje nové virtuální stroje (dalších VPC apod.) skrze administrativu uživatelem využívající nástroj k tomu určený. Mimo jiné také umožňuje spravovat všechny podsystémy a virtualizovaná data centra díky vlastní konzoli. [20]

PRAKTICKÁ ČÁST

4 PLÁNOVÁNÍ MIGRACE NA BLADE ŘESENÍ

Pro zavedenou pražskou firmu, která se zabývá výrobou a personalizací čipových karet byl zadán úkol modernizovat stávající IT zařízení s cílem zefektivnit náklady na provoz výpočetního centra i na samotnou výrobu. Byla provedena analýza stávajícího řešení jak po hardwarové stránce, tak po softwarové.

Firma potřebovala zachovat stávající výrobní a personalizační linky od firmy Muehlbauer. Linek Muehlbauer firma vlastní celkem pět. Náklady na pořízení jedné takové linky by dnes vyšly na cca 20 mil. korun. Jeden z důvodů, proč nebyl důvod linky kupovat nové je to, že životnost a efektivita těchto linek se udává v řádech desítek let. Ty stávající mají stáří od 9 do 4 let.

S ohledem na finanční náročnost zavedení takové výroby, byla stávající IT infrastruktura vybudována ve dvou etapách, přičemž první již v roce 1998 a druhá v roce 2003. Kvůli povodni v roce 2002 v Praze byla pro uložení serverové části infrastruktury vybudována serverovna v druhém nadzemním patře a byla vybavena výkonnými automatickými klimatizačními jednotkami, záložními inteligentními vysokokapacitními UPS zdroji, napojenými na externí diesel-agregátor.

Kvůli vyššímu bezpečnostnímu provozu výroby bylo požadováno, aby autentizace do celého systému výroby byla zajištěna pomocí přihlašování čipovými kartami s využitím vlastní certifikační autority.

Podmínkou migrace byl i požadavek, aby plán přechodu co nejméně zasahoval do procesu výroby. Výroba totiž funguje v jednom až dvousměnném režimu, podle pracnosti zakázky. Jakékoliv zdržení výroby by mohlo ohrozit termíny dodávek. Proto byly jako termíny migrace zvoleny nepracovní víkendy, kdy byly k dispozici veškeré zařízení pro otestování funkčnosti implementace.

Cílem praktické části diplomové práce je tedy nastínit či charakterizovat implementaci…..

4.1 Stávající infrastruktura

Stávající infrastruktura, kterou bylo třeba nahradit novou, výkonnější variantou, byla tvořena ze serverové části a klientských a obslužných počítačů. Veškeré HW zařízení bylo řešeno fyzicky, z důvodu, že virtualizace nebyla před 10 lety v době plánování zavedení provozu na takové úrovni, aby byl zabezpečen provoz i v případě havárie.

Součástí serverové části bylo 12 produkčních fyzických serverů, které zajišťovaly jednotlivé role výrobního prostředí a 2 testovací servery, které se využívaly pro testování nestandardních událostí. Dále pak diskové pole pro ukládání personalizačních dat do databáze a síťové prvky pro síťové rozvody po celém objektu.

Jednotlivých rolí serverů je celkem 6 a jsou řešeny aplikačně, kromě doménového řadiče. Aplikace jsou součástí dodávky externí firmou. Doména byla vytvořena na platformě Windows Server 2003. Kvůli požadavku na vysokou dostupnost domény byla řešena clusterem. Ten se musel při výpadku nebo poruše jednoho uzlů přepínat ručně.

Kvůli bezpečnostnímu režimu byla data šifrována lokálními HSM moduly. Data tak byla zabezpečena proti zneužití. Pro dešifrování se využívala externí certifikovaná certifikační autorita I.CA.

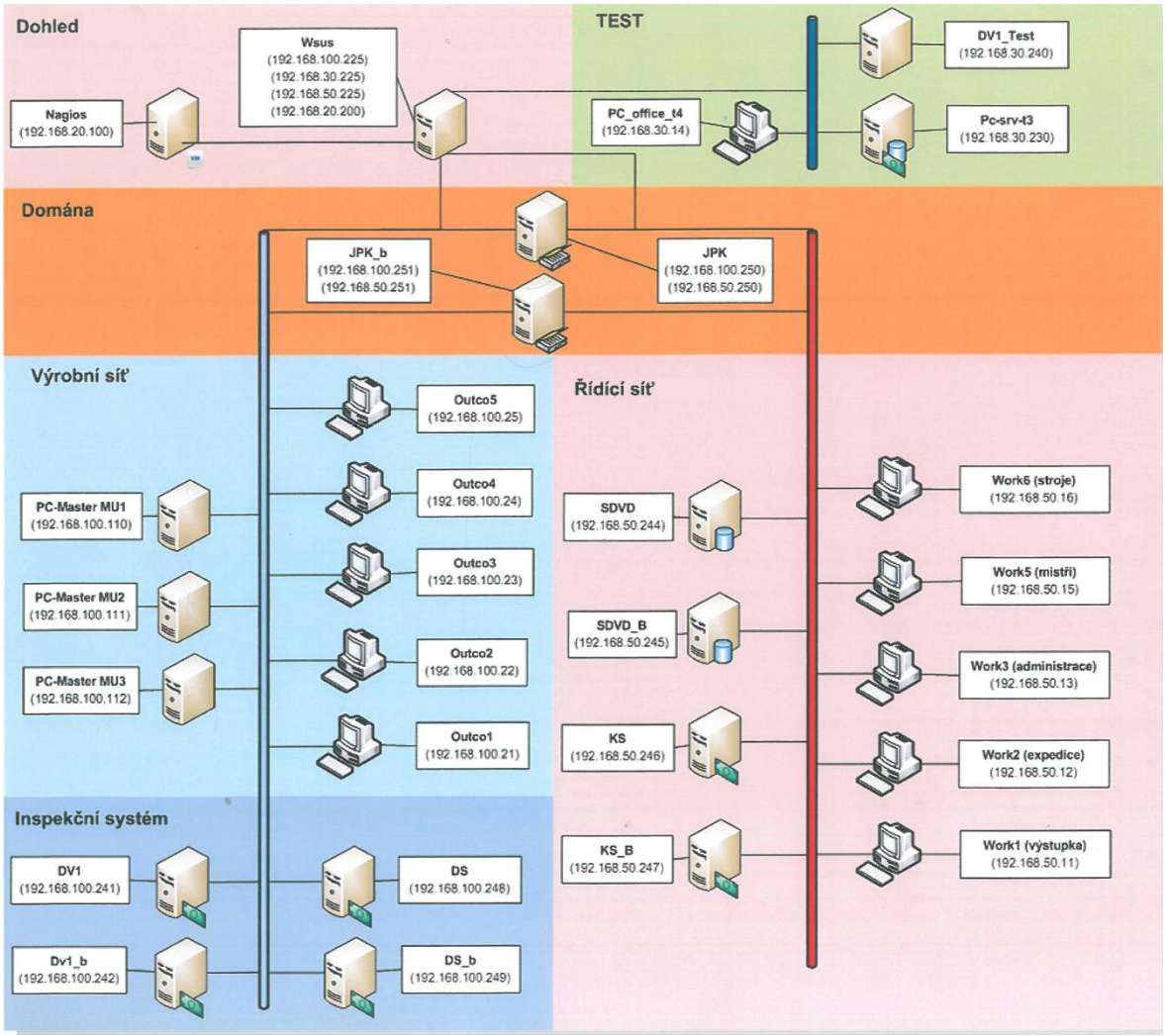
Jedna z rolí je a po migraci zůstane, vybudována na platformě Linux RedHat 5.5 Enterprise a je součástí externí certifikační autority, ověřující platnost vyrobených čipových karet. Tvoří ji dva servery v databázově řízeném clusteru a dva HSM moduly pro šifrování dat.

4.1.1 Stávající vybavení serverové části infrastruktury

V následujících bodech je popsáno stávající vybavení.

- 2 fyzické servery HP DL360 a 1 pásková jednotka - zajišťující služby domény, zálohování, certifikační služby a provoz personalizačních služeb
- 2 fyzické servery HP DL380 - připojené pomocí optických kabelů k diskovému poli. Na těchto serverech běží databáze Oracle v clusteru
- 2 fyzické servery HP DL320 - obsahující kryptokartu, sloužící ke kryptografické podpoře při příjmu a výdeji médií s daty
- 4 fyzické servery HP DL320 - obsahující kryptokartu, sloužící ke kryptografické podpoře při výrobě čipových karet
- 2 fyzické servery HP DL320 – obsahující kryptokartu, sloužící k ověření platnosti vyrobených čipových karet
- 1 fyzický server a 1 virtuální server, zajišťující dohled prostředí
- Testovací prostředí je provozováno na jednom fyzickém serveru HP ML310, obsahujícím doménový řadič, databázi a kryptokartu. Server je ve všech personalizačních rolích. V testovacím prostředí jsou 2 stanice pro zpracování dávek.

Pro lepší názornost je schéma celé infrastruktury znázorněno na obr. 15.



Obr. 15 Stávající infrastruktura celého prostředí [vlastní zpracování]

4.2 Důvod migrace

O upgradu hardwaru firma uvažovala již delší dobu s ohledem na stále se vyvíjející technologie výroby karet. Hlavním podmětem však bylo přijetí nové zakázky na výrobu čipových karet, kde se denní produkce měla oproti stávající několikanásobně zvýšit. To vyžadovalo zvýšit výkonnost výrobních linek a zlepšit infrastrukturu výrobního a řídícího prostředí. Jako nejlepší varianta se ukázalo vybudovat novou infrastrukturu na bladovém hardwaru.

Nová zakázka vyžaduje lepší dostupnost domény a je také náročnější na datové přenosy uvnitř systému. Proto byl kladen důraz na virtualizaci, migraci nových serverů a dynamické přidělování volných prostředků v rámci bladů.

S využitím nových nástrojů System Center si firma slibuje efektivnější management záloh databáze a samotných serverů, kvalitní dohled nad celým systémem a jednodušší správu celého systému v rámci vlastního IT oddělení.

Kvůli rozšíření stávajícího řešení by značně vzrostly náklady na provoz takového systému. Úspora energií při využití virtualizace je zřejmá a úspora místa v serverovně nabízí v budoucnu možnost dalšího rozšíření.

Od nové konfigurace si vedení firmy slibuje značný nárůst výkonu celého systému a celý systém je dimenzovaný tak, aby pokryl neočekávaný výpadek některého ze serverů.

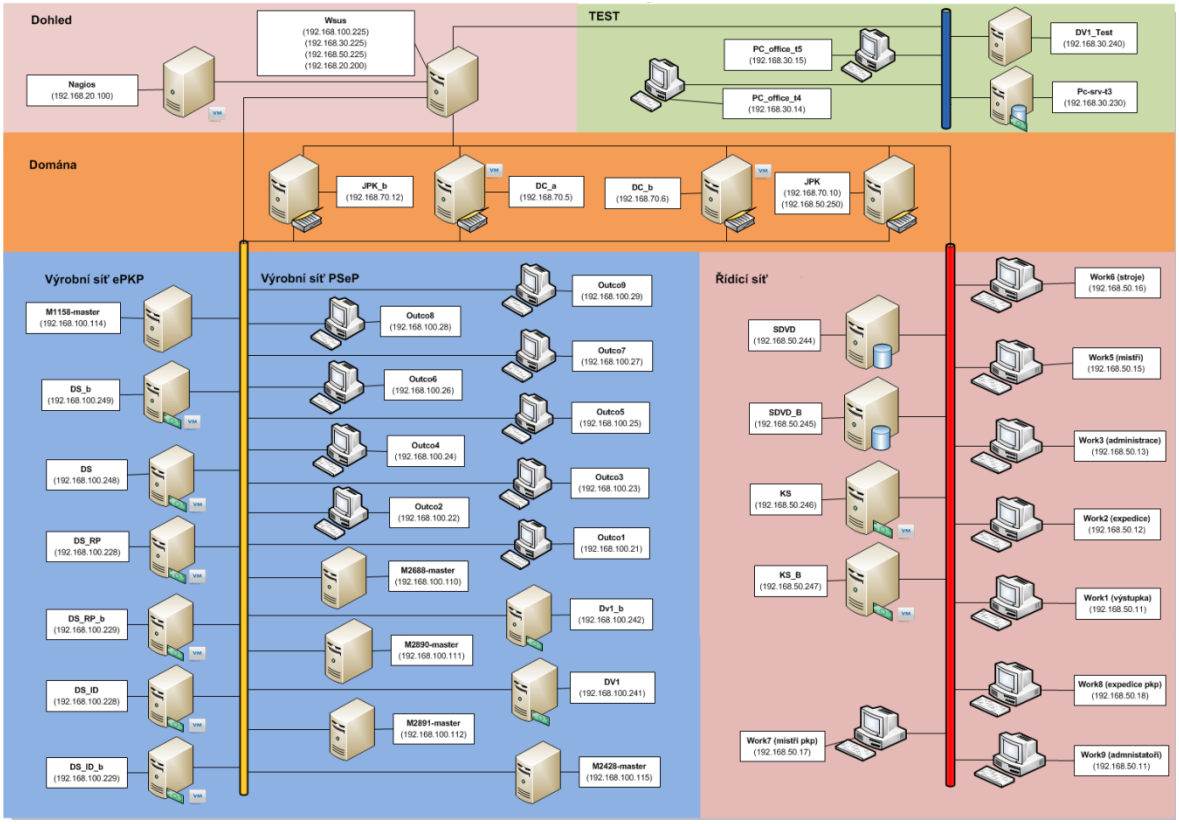
Stávající konfigurace také počítala s využitím HSM modulů ve variantě PCI-E. Při ceně jednoho HSM modulu v hodnotě cca 250 tis. Kč by se cena při pořízení fyzických serverů a dalších HSM modulů, vyšplhala na neakceptovatelnou úroveň. Nově byla navržena dvojce netHSM serverů, které zajistí potřebný šifrovací výpočetní výkon všem virtuálním serverům.

4.3 Návrh nové infrastruktury

Stávající infrastruktura byla rozšířena o dva domain conrollery (Virtuální servery) a Management server, které převezmou role doménových řadičů. Tím se uvolní prostředky doménových a řídících serverů, poskytující základní služby a aplikace výrobnímu prostředí. V minulosti se totiž stávalo, že byly tyto servery přetíženy. To je zásadní změna v novém návrhu, protože ovlivnila replikaci služeb aplikací třetích stran. Kvůli dvěma DC také vznikla chyba při synchronizaci času. To zásadním způsobem ovlivnilo automatické replikace dat, které se řídí časem domény. Tento problém byl nakonec vyřešen synchronizačním skriptem a úpravou DC.

Kvůli zapojení více fyzických zařízení a vzniku nových VLAN pro virtuální zařízení bylo nutné počítat s tím, že se musí pořídit výkonnější síťové prvky topologie. Nastavení VLAN a jejich propustnost je popsána v kapitole 5.3

Zůstal také systém aktualizací WSUS. Celý systém je totiž v Off-line režimu a vyžaduje aktualizace. Ty jsou distribuovány pomocí Offline WSUS serveru. Nová infrastruktura je opět znázorněna i schematicky, v obr. 16.



Obr. 16 Nový návrh infrastruktury [vlastní zpracování]

4.4 Výběrové řízení aneb firma věří komponentám HP

Firma má dlouhodobé zkušenosti s produkty od firmy Hewlett Packard a s ohledem na již zakoupené servisní balíky byla pro návrh nového řešení zvolena opět firma HP. Nejlepší nabídku na kompletní objednávku zaslala firma Alwil Trade, s.r.o. K zadanému hardwaru zdarma přidala i konzultace, školení a odbornou pomoc při konfigurování vnitřních rozhranní blade a dodaných Cisco Switchů ProCurve. Samozřejmostí k takové dodávce byl pak balíček podpory HP CarePack.

4.4.1 Výběr HW

BladeSystem c7000 - Vzhledem k možnému budoucímu rozvoji výrobní linky firmy se zvolilo chassis z větší kapacitou zásuvných modulů – „žiletek“ **HP BladeSystem c7000.** Toto chassis pojme až 16 serverových žiletek ve dvou řadách. V rámci naší migrace využijeme pouze 6 pozic pro přední zásuvné moduly (5 Serverů, 1 pásková mechanika).

Server ProLiant BL460c G7 – byl vybrán pro svou rozšiřitelnost a možnost budoucího upgradu. Je osazený procesorem Intel® Xeon® E5640 (4 jádra, 2,66 GHz, 12 MB mezipaměti L3, 80 W). Všech 5 serverů disponuje také dvojicí rychlých SAS disků v

RAID 1 (mirror), sloužící k instalaci operačního systému. Na databázových serverech bude navíc instalace SW od Oracle. Na management serveru budou nainstalovány produkty System Center. Celkem jsou tedy 4 servery s celkovou kapacitou 72 GB a jeden 146 GB.

- 1 Server je navržen jako Management server – řídící celou doménu.
- 2 Servery – virtualizační, budou poskytovat výpočetní výkon pro virtuální servery
- 2 Servery budou databázové a bude na nich provozován Oracle Cluster.

Dodatečné RAM kvůli virtualizaci. U virtualizačních serverů bude navýšena kapacita operační paměti na 48 GB. Jsou tak dimenzovány pro převzetí všech virtuálních serverů na jediný virtualizační server.

Switch - HP ProCurve_6120XG - blade je osazen dvěma redundantními ethernetovými přepínači (switche), redundantním napájením a administrátorskou konzolí.

HP StorageWorks TapeBlade – pásková mechanika pro bezztrátové a dlouhodobé zálohování databáze a virtuálních serverů. Jednotka je provedena v blade velikosti. Pro zálohy budou použity přepisovatelné pásky **HP LTO4 Ultrium 1,6TB RW.** Výrobce udává, že životnost archiválií na těchto páskách je minimálně 30 let.

Disková pole HP P2000 LFF Modular Smart Array – při implementaci byla použita dvě disková pole:

- Jedno pole je osazeno rychlými disky (15000 otáček za minutu, RAID 10) o celkové kapacitě 2,4TB pro uložení virtuálních serverů a pomalými disky (7200 otáček za minutu, RAID 5) o kapacitě 3TB pro zálohování. Pole je připojeno k chassis pomocí 10Gb iSCSI rozhraní.
- Druhé pole je osazeno rychlými disky (15000 otáček za minutu, RAID 10) o celkové kapacitě 1,2TB pro uložení výrobních databází.

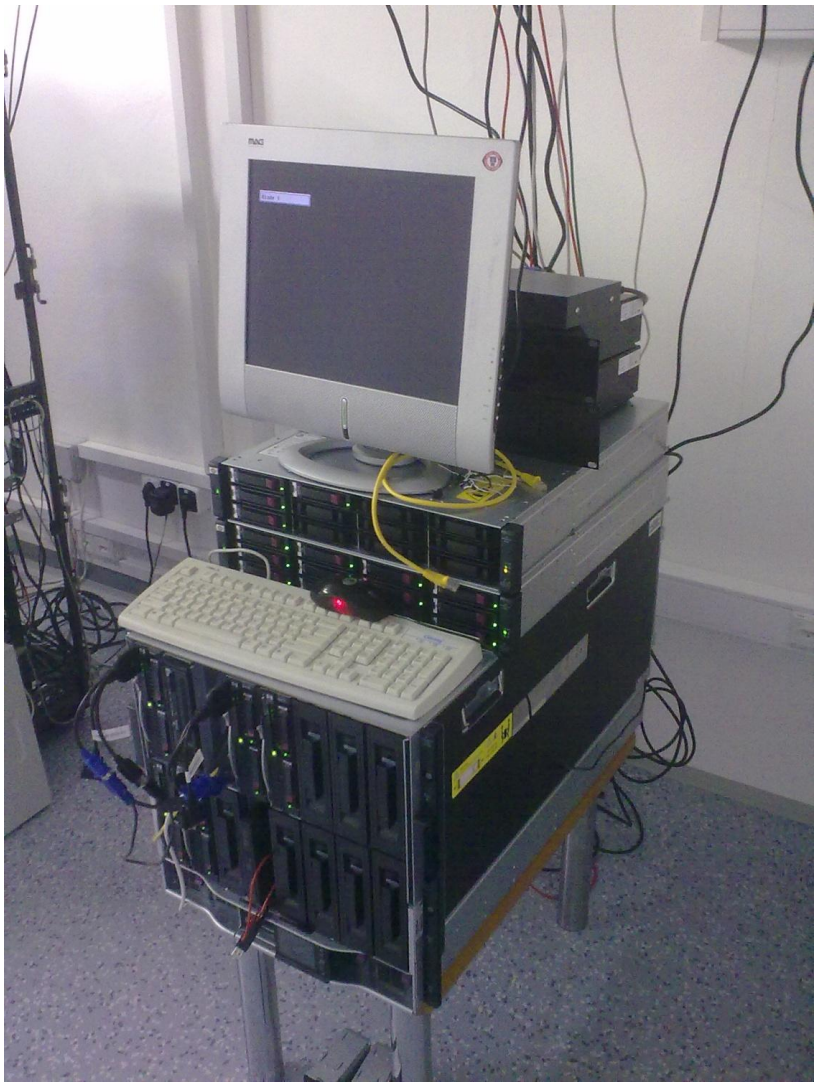
iSCSI kabely - Pole je připojeno k polici pomocí 10Gb iSCSI rozhraní

Síťové HSM – pro testovací a produkční provoz bylo třeba pořídit různé varianty:

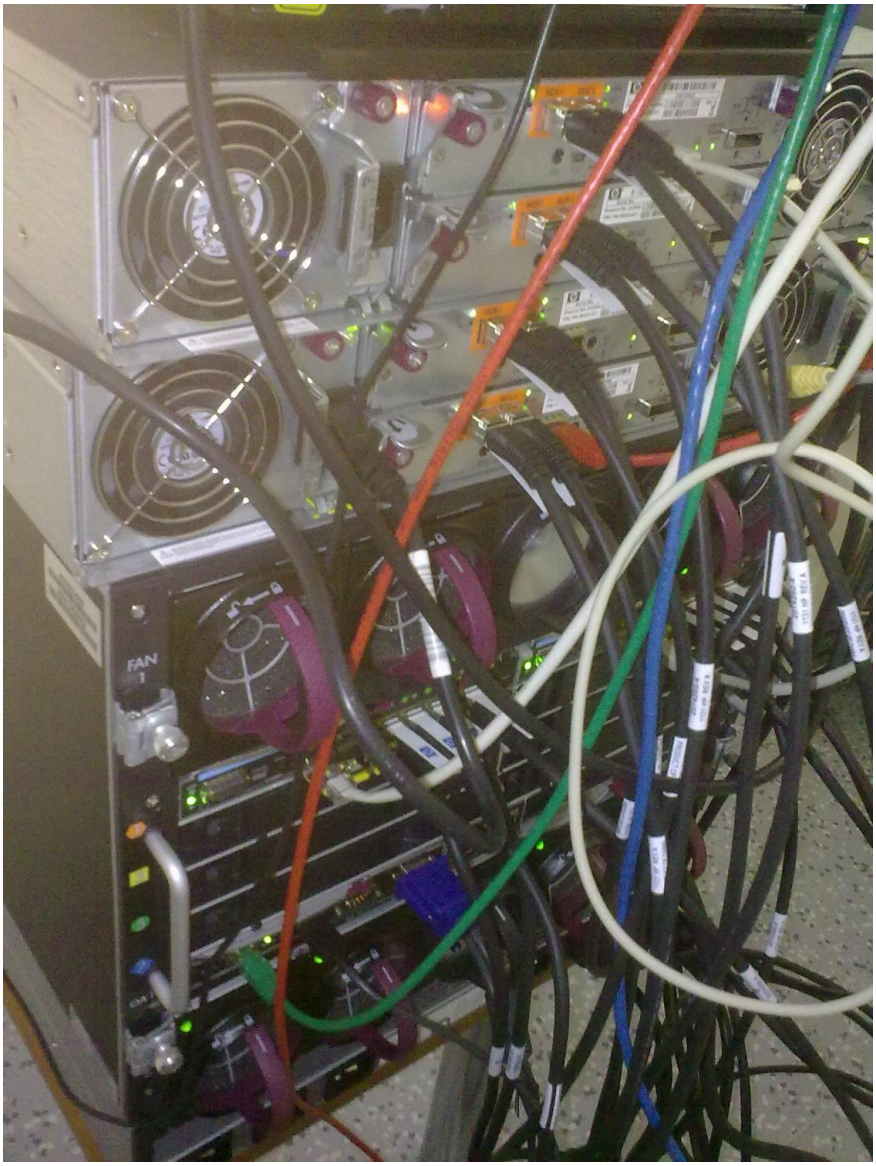
- **netHSM PL220** – vyhrazeno pro testovací systém
- **netHSM PL600** – pro produkci, obě HSM obsahují stejné tokeny, jsou vzájemně zastupitelné

Cisco switche C3560 – jsou součástí redundantního zapojení síťové infrastruktury

Pohled na zapojené komponenty v testovacím – vývojovém režimu zepředu i zezadu zobrazuje obr. 17 a 18 níže.



Obr. 17 Pohled na všechny dodávané komponenty [vlastní zpracování]



Obr. 18 Pohled na zadní stranu Chassis [vlastní zpracování]

4.4.2 Výběr serverového OS

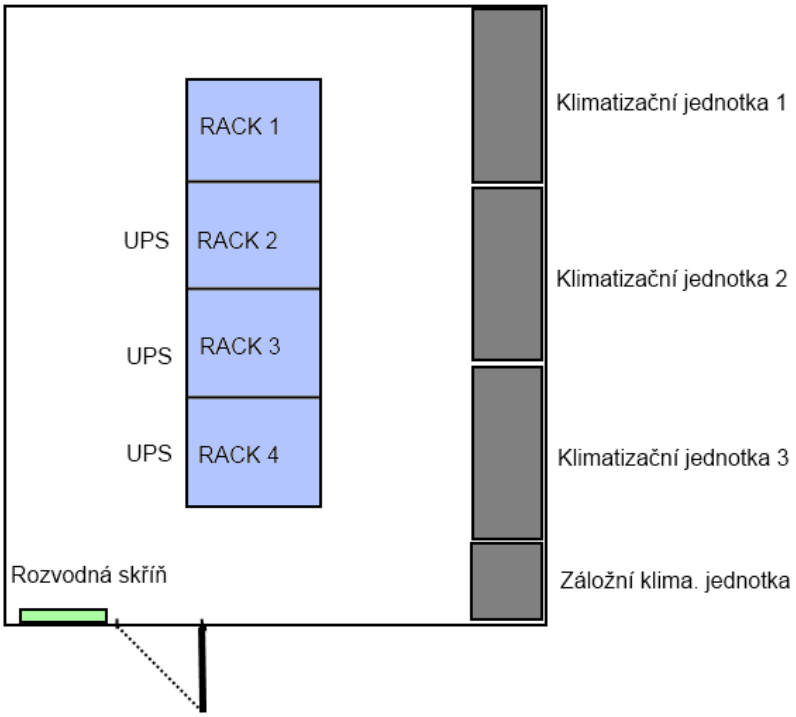
Vzhledem k požadavkům na virtualizaci bylo nezbytnéi zvolit vhodnou platformu, na které bude celý systém provozován. Muselo se počítat i s faktem, že stávající IT oddělení má zkušenosti hlavně OS Windows Server, že stávající doménové politiky budou muset být zachovány a že bude do systému zabudovaná certifikační autorita, která bude sloužit k identifikaci do systému. Vzhledem k těmto faktům byla zvolena platforma Windows Server 2008 R1 a Windows Server 2008 R2. Klientské stanice zůstávají u operačních systémů Windows XP SP3 a Windows 7.

5 KONFIGURACE A IMPLEMENTACE BLADE DO VÝROBNÍHO PROSTŘEDÍ

Z důvodu omezené dostupností místa implementace u zákazníka, byla příprava na migraci započata mimo místo implementace. To s sebou neslo rizika, že se nepodaří nakonfigurovat všechna nastavení, pro správný provoz blade. Hlavním důvodem obav bylo specifické prostředí a nemožnost otestování finálního nastavení.

Příprava na nasazení všech komponent trvala asi měsíc. Během této doby se podařily vyřešit hlavně problémy, se specifickým nastavením VLAN sítě a s přidáním nových domain controllerů do stávající domény.

Pro samotnou implementaci byly vybrány dva po sobě jdoucí víkendy, ve kterých byla omezena nebo odstavena produkční výroba. Jeden víkend byl vyhrazen na fyzické zapojení veškerého nového HW, přestěhování, opětovné zapojení a zajištění kontinuity výroby na stávající serverech. Druhý víkend byl vyčleněn na vnitřní konfiguraci management bladu, instalaci nového prostředí na blade, na otestování prostupnosti sítě a testování migrace virtuálních strojů mezi jednotlivými virtualizačními servery.



Obr. 19 Schematický plán serverovny [vlastní zpracování]

5.1 Uspořádání jednotlivých komponent v chassis

Blade servery se nacházejí v jedné polici, která obsahuje rozhraní pro interní switche. Tyto switche zajišťují komunikaci nejen mezi samotnými fyzickými servery, ale také mezi virtuálními servery běžícími na virtualizačních serverech. Servery byly do chassis uspořádány tak, aby logické členění odpovídalo povaze serverů. Na první pozici byl tedy logicky umístěn Management server, vedle kterého je na pozici 2 napojená pásková jednotka podporující páskové kazety Ultrium 4. Připojena je interním linkem k management serveru, která řídí zálohování.Třetí pozice je volná. Na pozici 4 a 5 jsou umístěny virtualizační servery. Pozice 6-8 jsou opět volné. Na začátku druhé řady na pozicích 9 a 10 jsou umístěny databázové servery.

Servery navzájem komunikují po integrovaném interním linkem, podporující rychlost 10Gb. Toto rozhraní je řízeno připojenými interními přepínači, na kterých se definují VLANy, prostupy mezi nimi a komunikace mezi interními servery, fyzickými pracovními stanicemi a virtuálními servery.

Na zadní straně jsou zasunuty do pozic A1 a A2 Ethernetové switche HP ProCurve.

5.2 Konfigurace fyzických serverů

Konfigurace fyzických serverů byla navržena tak, aby byl návrh co nejvíce efektivní z pohledu dostupných prostředků k ekonomické stránce návrhu. V jednom z nových návrhů se přemýšlelo i o šestém serveru, který bude virtualizovat virtuální domain controllery, při hlubší analýze se ale tato varianta ukázala jako zbytečná, protože výpočetní výkon a teoretická dostupnost zajišťující výrobu na serverech VIRT_A a VIRT_B se ukázala jako pně dostačující. Uvedená tabulka popisuje fyzické servery a jejich technické parametry.

Tabulka 1 Technická specifikace fyzických serverů [vlastní zpracování]

	Blade	CPU		paměť	disk	Operační systém	
		počet	typ	GB		verze	edice
1	MGMT	1x4	Xeon E5503 2GHz	8	146	Windows Server 2008 R2 x64	Enterprise
2	VirtA	2x6	Xeon X5650 2,6GHz	48	72	Windows Server 2008 R2 x64	Datacenter
3	VirtB	2x6	Xeon X5650 2,6GHz	48	72	Windows Server 2008 R2 x64	Datacenter
4	SDVD_C	1x4	Xeon E5503 2GHz	12	72	Windows Server 2008 R2 x64	Standard
5	SDVD_D	1x4	Xeon E5503 2GHz	12	72	Windows Server 2008 R2 x64	Standard

5.2.1 MGMT Blade

Blade slouží k obsluze virtualizace a správě prostředí. K blade je připojena pásková jednotka pro zálohování fyzických systémů, virtuálních systémů a databáze. Vše se bude zálohovat systémem Disk-to-Disk-to-Tape.

K blade je namapován disk z pole o kapacitě 3TB, který slouží k uchování právě zálohovaných systémů, před přesunem na pásku. Toto úložiště bude zpřístupněno pomocí technologie DFS.

Management blade je plánován jako jediný fyzický řadič domény, který bude čas synchronizovat s HW zařízením, poskytující čas. Doménové služby od něj budou přebírat virtuální doménové řadiče. Blade není součástí clusteru, pouze tento cluster řídí. Na blade není instalována žádná komponenta aplikací třetích stran. Blade bude nakonfigurován tak, aby jeho krátkodobé vypnutí nemělo vliv na funkci systému.

5.2.2 Virtualizační blade

Dvě virtualizační blade v clusteru slouží k provozu virtualizovaných serverů. Výkon každé blade je designován tak, aby v případě výpadku jedné z blade byla druhá schopna převzít veškeré běžící virtuální servery. Blade budou nakonfigurovány tak, aby po přemigrování virtuálních serverů z jedné z nich, mohla být tato blade bezpečně vypnuta bez dopadu na systém.

K blade je namapováno diskové pole, připojené přes iSCSI rozhraní, které slouží k uložení dat virtuálních serverů. Tyto prostředky jsou sdíleny mezi blade, aby byla možná migrace mezi nimi.

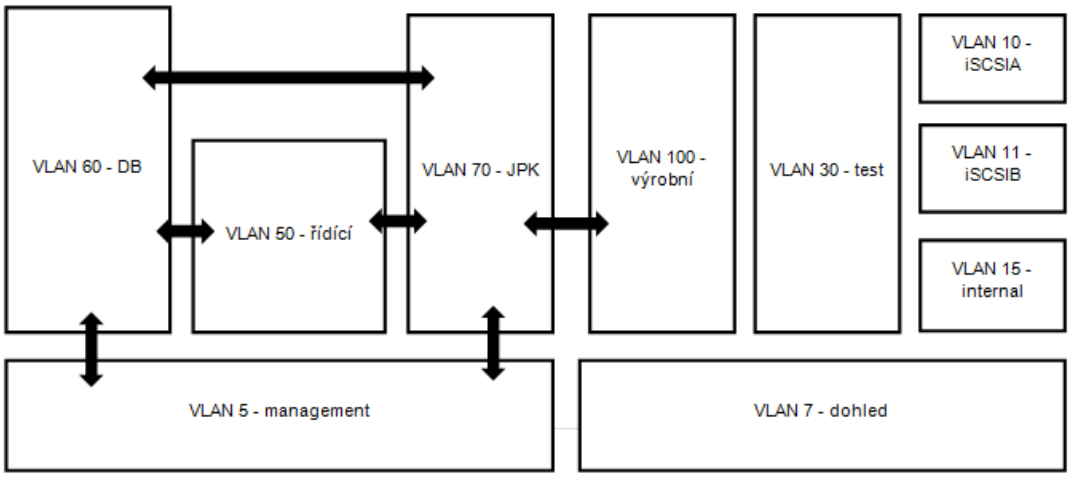
5.2.3 Databázové blade

Dva blade servery vyhrazené pro běh Oracle databáze fungují v databázovém clusteru. K bladu je namapováno diskové pole, připojené přes iSCSI rozhraní. Databáze se zálohuje na diskový prostor vyhrazený na serveru MGMT, odkud budou zálohy pravidelně zapisovány na páskovou jednotku. Při obnově z páskové jednotky budou data zapisována opět do tohoto umístění, odkud si je databáze načte.

5.3 Definování síťových prostupů

Síťové prostředí bylo tvořeno dvěma switchi, které zajišťovaly konektivitu v daném segmentu sítě. Switche neměly děleny porty mezi sítě. Vzájemná zastupitelnost síťového prostředí neexistovala.

Jak už byl zmíněno výše, celá infrastruktura má přísná pravidla do jednotlivých sítí – VLAN. Aby bylo zajištěno dostatečné oddělení těchto sítí, bylo potřeba definovat VLANy pro jednotlivé servery a definovat prostupy či zákazy prostupů mezi nimi. Prostupy jednotlivých VLAN jsou zachyceny na obr. 20 níže:

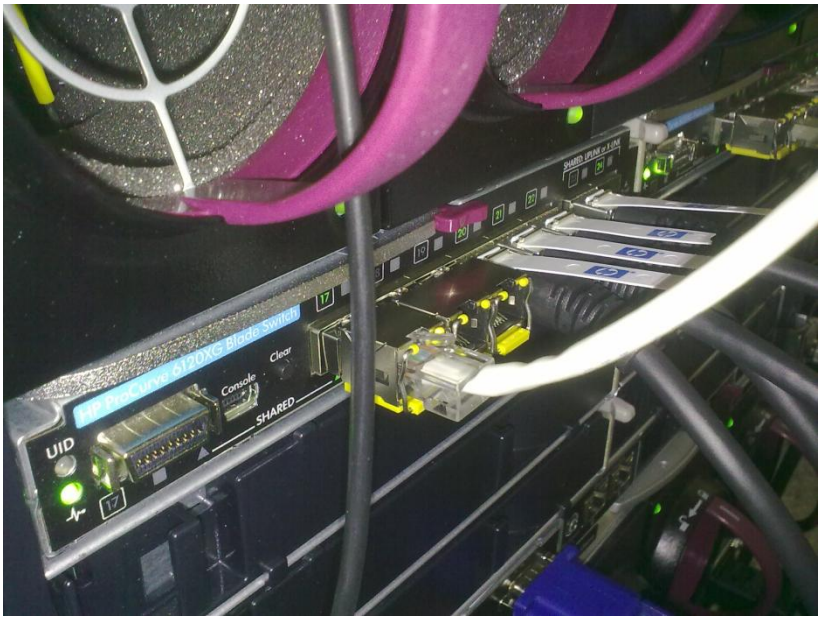


Obr. 20 Schéma zapojení VLAN [vlastní zpracování]

VLANy, které nemají šipku do jiné VLANy, nemají povolen přístup do žádné VLANy. Mají pouze výstup na switchi. Prostup funguje jen přes jednu šipku – např. VLAN Výrobní má přístup jen do VLAN JPK.

Popis VLAN a přiřazení jednotlivých serverů zobrazuje tabulka v příloze PI Konfigurace síťových prostupů.

Pohled na propojení Switchu HP ProCurve pomocí SCSI kabelů je vyobrazen na obr. 21.



Obr. 21 Pohled na propojení Switchu HP ProCurve pomocí SCSI kabelů [vlastní zpracování]

Fyzické propojení switchů a alokace portů je zachyceno v následujících dvou tabulkách:

Tabulka 2 Propojení switchů a alokace fyzických portů [vlastní zpracování]

Propojení switchů (10Gb linka)			
Zdroj		Cíl	
Switch	Port	Switch	Port
CR1	E1	HP1	18
CR2	E1	HP2	18
CR1	E2	CR2	E2
HP1	23	HP2	23
HP2	24	HP1	24
CR1	1	CC	1
CR2	1	CC	2
CR1	5	CV	1
CR2	5	CV	2

Alokace portů			
CR1		CR2	
Port	VLAN	Port	VLAN
1	50	1	50
2	50	2	50
3	50	3	50
4	50	4	50
5	100	5	100
6	100	6	100
7	100	7	100
8	100	8	100
9	30	9	30

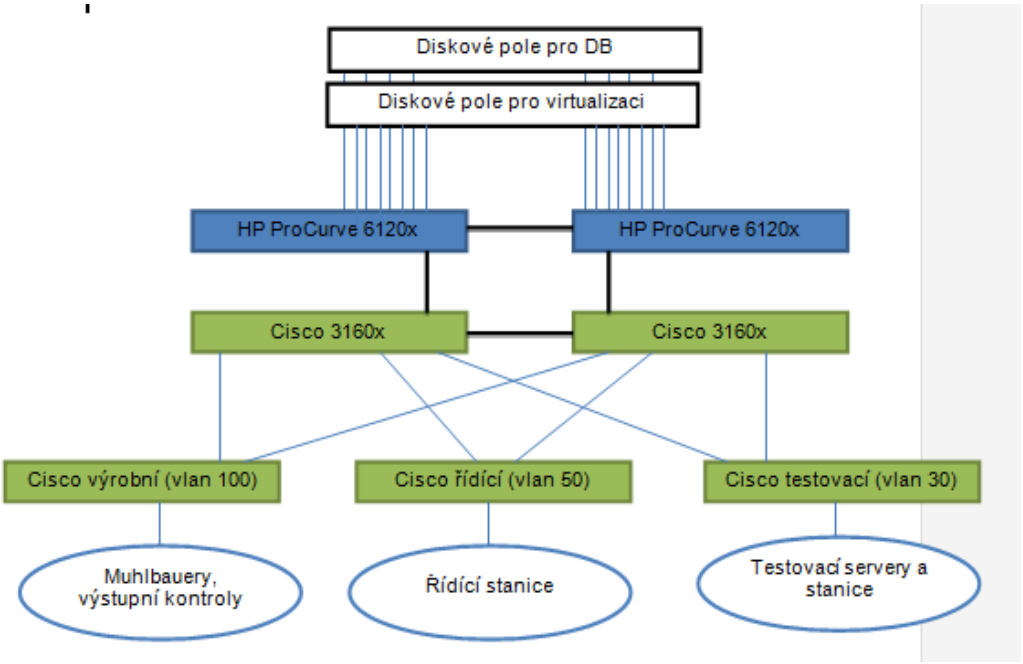
CR1	6	CV2	1
CR2	6	CV2	2
CR1	9	CT	1
CR2	9	CT	2
CR1	10	CT2	1
CR2	10	CT2	2
CR1	13	netHSM	1
CR2	13	netHSM	2

10	30	10	30
11	30	11	30
12	30	12	30
13	70	13	70
14	70	14	70
15	7	15	7
16	7	16	7
17	7	17	7
18	7	18	7
19	7	19	7
20	7	20	7
21	7	21	7
22	7	22	7
23	7	23	7
24	7	24	7

Legenda k tabulce 2

		Obsazeno	Celkem
CR1	Cisco Router 1	17	24
CR2	Cisco Router 2	17	24
HP1	HP ProCurve 6120xg 1	7	8
HP2	HP ProCurve 6120xg 2	7	8
CT	Cisco Test	13	24
CC	Cisco Řídící	13	24
CV	Cisco Výrobní	18	24

Finální zapojení již nesmělo být zaznamenáno, ale na následujícím obrázku č. 22 je uvedeno redundantní zapojení switchů.



Obr. 22 Redundantní zapojení switchů [vlastní zpracování]

5.4 Co se současnými servery?

Díky migraci na nové HW vybavení se nabízí otázka, jak naložit se starými rackovými servery. Některé ze serverů toho pamatují již hodně, mají velkou spotřebu elektrické energie, jejich komponenty produkují hodně tepla, a proto by nebylo vhodné tyto servery ještě nějak využít.

Vedení společnosti se tedy rozhodlo pro ty nejstarší komponenty zřídit malé muzeum a umístit je tam. To bude sloužit hlavně pro ukázku historických prací při prezentacích firmy. Výroba čipových karet je totiž velice zajímavý a v České Republice málo vídaný projekt.

Na druhou stranu by nebylo vhodné relativně nové servery (stáří 2-5 let) úplně odstavit a nechat je nevyužité. Také se zde muselo myslet na to, že disky obsahují citlivá data, která se nesmí dostat do cizích rukou. Servery se sice mohly prodat bez pevných disků, ale otázkou je, zda by někdo koupil v dnešní době staré servery bez pevných disků, které jdou dnes sehnat pouze v servisních rezervních skladech firmy Hewlett Packard. Rozhodlo se tedy, že část těchto serverů bude uložena v trezoru jako HW bod záchrany při selhání blade systému.

6 KONFIGURACE A IMPLEMENTACE SW PROSTŘEDÍ BLADE

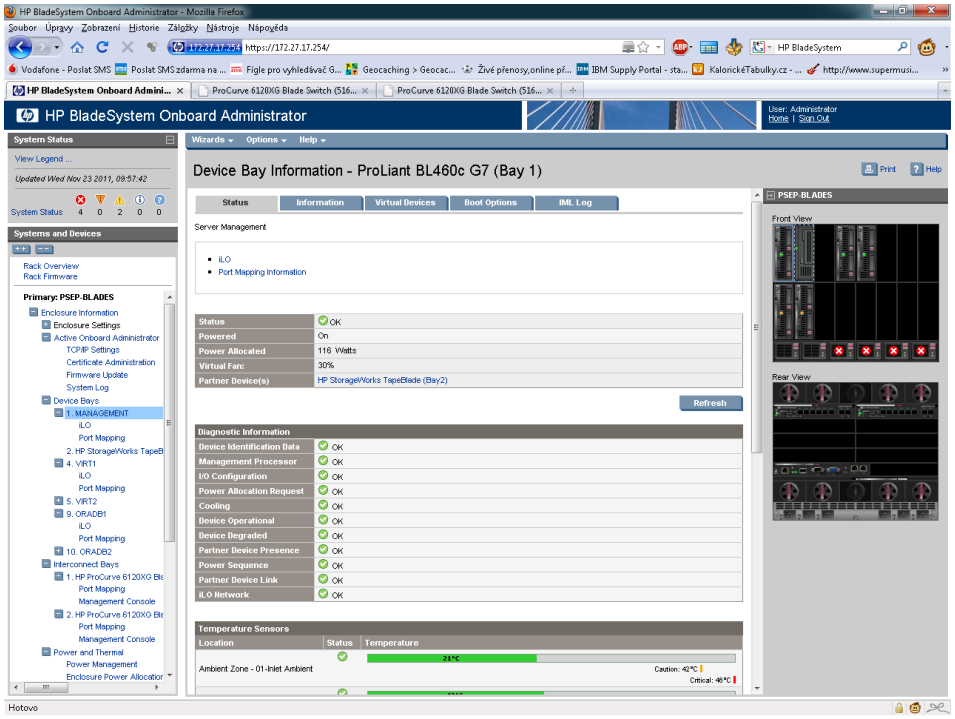
Blade má implementováno vlastní managementovou konzoli dostupnou přes KVM switch a http protokol pomocí nastavené IP adresy. Přes tuto konzoli se hlídají události bladu, definují se uživatelé a správci blade. Konfigurace bladu na úrovni managementu HW prostředků umožnila nastavit chování všech připojených zásuvných komponent.

V první řadě bylo třeba nastavit sekvenci spouštění jednotlivých fyzických serverů a switchů. Protože jednotlivé servery nabíhají různě dlouhý čas, bylo třeba tomu přizpůsobit i zapnutí síťových prvků včetně Cisco Switchů. Časy byly nastaveny tak, aby nejdříve kompletně naběhly síťové prostředky (Hp ProCurve a Cisco) a teprve potom se začnou spouštět fyzické servery v pořadí:

1. Management server s páskovou mechanikou v čase t=270s
2. Virt_A a Virt_B v čase t=600s
3. SDVDC a SDVDD v čase t=810s

Kompletní naběhnutí systému bez virtuálních stanic bylo změřeno na 16 minut.

Další konfigurovanou položkou pro jednotlivé fyzické servery byly ILO spojení a mapování portů pro separátní uživatelské rozhranní. U těchto položek byla ponechána defaultní hodnota, tj. správa těchto serverů i nadále pomocí globálního managementu.



Obr. 23 Management konzole Onboard administrator Blade [vlastní zpracování]

6.1 Instalace OS

Na virtualizačních serverech byla zvolena datacenter edice z licenčních důvodů – umožňuje v rámci jedné licence legálně vytvořit libovolný počet virtuálních systémů. Enterprise edice umožňuje vytvoření pouze 4 virtuálních systémů. Z toho plyne, že všechny virtuální systémy budou datacenter edice.

6.2 Instalace a konfigurace virtuálního prostředí

Ve virtuálním prostředí běží servery zajišťující komunikaci s kryptokartami a doménové řadiče pro VLANy, které nemají dostupnost na server MGMT.

Seznam instalovaných virtuálních serverů a jejich konfigurace fyzických prostředků je v následující tabulce č. 3:

Tabulka 3 Technická specifikace virtuálních serverů [vlastní zpracování]

ID	VM	CPU		paměť	disk	Operační systém	
		počet	typ	GB		verze	edice
1	DS	1	2GHz Xeon	2	40	Windows Server 2008 R2 x64	standard
2	DS_B	1	2GHz Xeon	2	40	Windows Server 2008 R2 x64	standard
3	DS_RP	1	2GHz Xeon	2	40	Windows Server 2008 R2 x64	standard
4	DS_RP_B	1	2GHz Xeon	2	40	Windows Server 2008 R2 x64	standard
5	DS_IS	1	2GHz Xeon	2	40	Windows Server 2008 R2 x64	standard
6	DS_IS_B	1	2GHz Xeon	2	40	Windows Server 2008 R2 x64	standard
7	KS	1	2GHz Xeon	2	40	Windows Server 2008 x32	standard
8	KS_B	1	2GHz Xeon	2	40	Windows Server 2008 x32	standard
9	DC_A	1	2GHz Xeon	2	80	Windows Server 2008 R2 x64	Enterprise
10	DC_B	1	2GHz Xeon	2	80	Windows Server 2008 R2 x64	Enterprise
11	JPK_C	2	2,67GHz Xeon DC	8	200	Windows Server 2008 x32	Enterprise
12	JPK_D	2	2,67GHz Xeon DC	8	200	Windows Server 2008 x32	Enterprise
13	Nagios	1	2GHz Xeon	1	40	Centos	
14	PC-SRV-T1	1	2GHz Xeon	2	40	Windows Server 2008 R2 x64	Enterprise
15	PC-SRV-T2	1	2GHz Xeon	4	100	Windows Server 2008 R2 x64	standard
16	PC-SRV-T3	1	2GHz Xeon	4	100	Windows Server 2008 x32	Enterprise

6.2.1 Správa virtuálního a fyzického prostředí

Celé prostředí bude spravováno z prvního blade serveru. Na serveru budou instalovány produkty z rodiny System Center, které jsou určeny pro správu datacenter.

- System center operation manager (SCOM) – dohled celého řešení (blade, virtuální servery, pracovní stanice, výrobní linky), základ řešení systém center. SCOM může zobrazovat aktuální zdraví sledovaných serverů.

- System center virtual machine manager (SCVMM) – správa virtualizace postavené nad Hyper V, zajišťuje spouštění virtuálních serverů, optimalizace vytížení fyzických blade a přidělování prostředků
- System center data protector manager (SCDPM) – zálohování fyzických bladů, zálohování virtuálních serverů a zálohování databáze.

Řešení System Centeru je postaveno nad databází MSSQL 2008, aktuálně ve verzi SP3. Každý z produktů System Center vyžaduje přístup k vlastní databázi na platformě MS SQL Server 2008 R2. Instalace SQL Serveru se žádným způsobem nedotkla produkčního prostředí a kromě SQL management konzole není nijak přístupná z jiných aplikací než jsou produkty System Center. Databáze běží na tom samém serveru, jako produkty System Centeru. Databáze se používá ve verzi Standard a je licencí vyhrazena pouze pro tento účel.

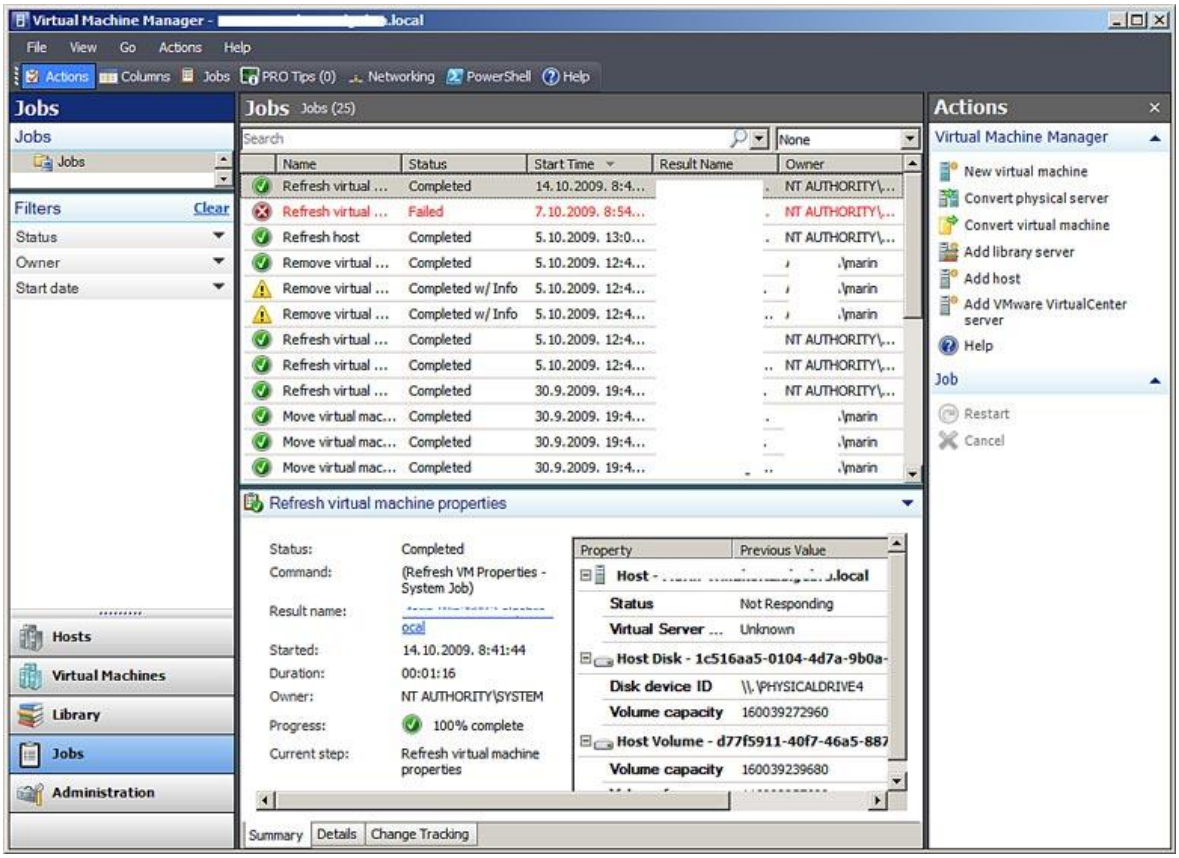
Prostředí System Centeru je možné dále rozšiřovat, například o System Center Configuration Manager (SCCM). Tato komponenta by umožňovala snazší distribuci softwarových balíčků po doméně. Komponenta není pro správu prostředí nezbytná.

Pro virtualizaci systémů se používá technologie Hyper-V R2, která podporuje clusterování, live migraci mezi fyzickými servery, quick migraci, live zálohování, dynamické přidělování paměti, snapshoty virtuálních serverů. Snapshoty se však nedoporučují v produkčním prostředí.

Celé virtuální prostředí může být spravováno z cluster manageru, Hyper-V manageru, nebo SCVMM. Celá pokročilá správa virtuálního prostředí je založena na SCVMM. To však neznamená, že bez tohoto nástroje by nebylo možné virtualizaci provozovat. Pokud nebude z nějakého důvodu tento nástroj dostupný, virtuální servery poběží dále. Správa by však nebyla centralizovaná. Virtuální servery mohou být migrovány ručním zásahem přímo na jednom z fyzických serverů.

Pro správu virtualizačních serverů a provozovaného virtuálního prostředí byl využit System Center Virtual Machine Manager. SCVMM zajišťuje podle předem definovaných pravidel automatické migrace jednotlivých virtuálních serverů mezi fyzickými virtualizačními servery. To opět značně ulehčilo správu celého systému.

Pomocí SCVMM byla nastavena jsme nastavili migrace tak, aby se v noci, při nízkých nárocích na výpočetní výkon uspávaly záložní (Custerové) servery a aktivní uzly se přesouvaly kvůli co nejnižším nárokům na dodávku elektrické energie.



Obr. 24 Konzole pro správu SCVMM [vlastní zpracování]

Na obr. 24 výše, je znázorněna ukázka konzola pro správu SCVMM.

Produkty System Center mají značné nároky na software. Podmínkou pro instalaci těchto produktů je, aby na serveru byly nainstalovány tyto součásti OS:

- .NET Framework 3.5 with Service Pack 1 (SP1) or later
- Microsoft Visual C++ 2008 Redistributable
- Windows PowerShell 2.0
- Windows Installer 4.5 or later
- Windows Single Instance Store (SIS)
- Microsoft Application Error Reporting
- SQL Server 2008 SP1 Enterprise nebo Standard edition nebo vyšší

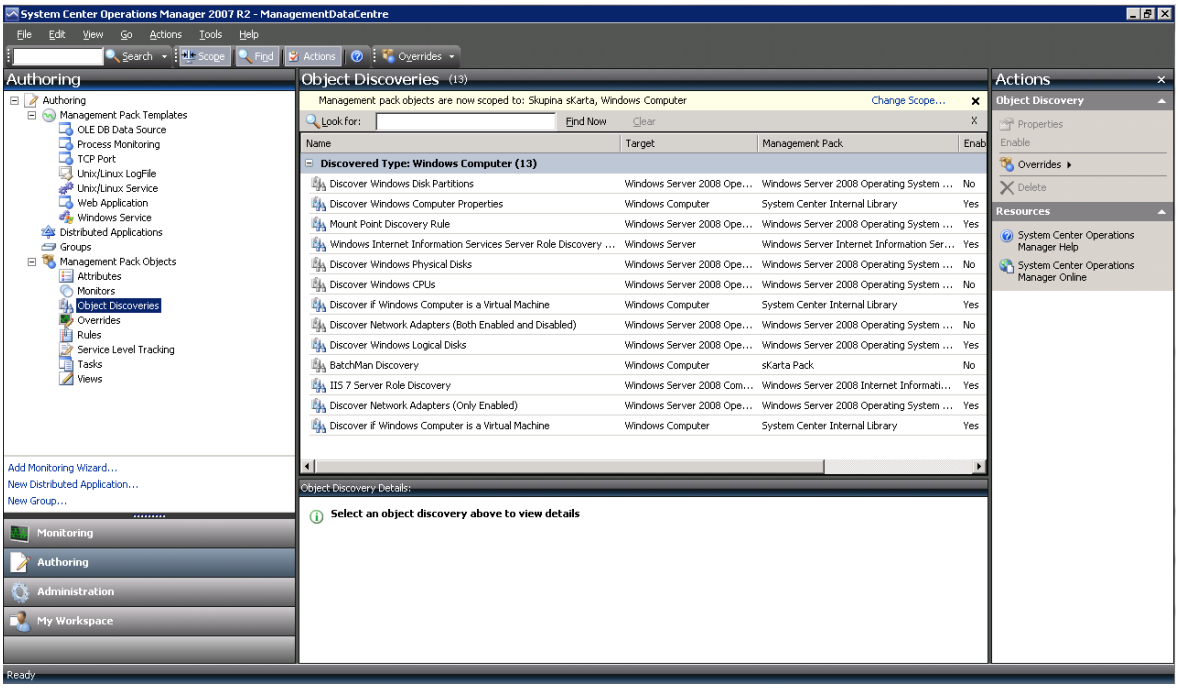
6.3 Sledování systému

Sledování celého systému je zajištěno nástrojem System Center Operation Manager 2007 R2. Tento sofistikovaný nástroj dokáže spolehlivě uhlídat celé výrobní prostředí. SCOM nabídl také nástroje pro sledování dvou Linuxových systémů.

Sledování je zajištěno nadefinovanými úlohami a monitory.

- V první řadě bylo potřeba hlídat dostupnost všech fyzických a virtuálních serverů vytvořením tzv. Tasku, který neustále posílá příkaz ping s parametrem -t
- Dostupnost domény a všech služeb, které doména poskytuje celému prostředí. Tuto službu zajišťuje klient v podobě běžící služby, na všech strojích v doméně. Ten komunikuje s domain controllerem a hlídá všechny důležité funkce komunikace.
- Kontrola domény a aplikací je zajištěna také monitorem událostí v EventLogu. Pokud tedy nastane nestandardní nebo nežádoucí stav, obsluha je ihned upozorněna.
- Pro výrobní činnost bylo důležité nastavit monitoring pro jednotlivé služby aplikací třetích stran a na monitoring logů těchto aplikací. Zde se vytvořil tzv. monitor, který je přímo navázaný na jednotlivé stroje, kde daná služba běží. Monitor hlídá dostupnost služby přes status v „services.msc“. Pokud služba neodpovídá, monitor vystaví varovné hlášení.
- Pro virtuální prostředí je nastaveno monitorování sítě a její aktuální propustnost. Tento monitor je pro výrobu důležitý, proto, že při tvorbě a přenášení dávek vznikají díky fotografiím značné nároky na datovou propustnost. Obsluha tak může naplánovat sestavy dávek podle vytížení sítě.

Ukázka konzole pro správu SCOM je znázorněna na obr. 25.



Obr. 25 Konzole pro správu SCOM [vlastní zpracování]

System Center Operation Manager uchovává a reportuje všechny nestandardní stavy a pro administrátory systému je pak jednodušší lokalizovat chybu v systému nebo při výrobě.

Podružnou roli ve sledování systému bude mít již zavedený monitorovací systém Nagios.

6.4 Definování zálohovacích procesů

Pro zálohování celého produkčního i testovacího prostředí bylo nutné upravit stávající havarijní plán. Ten nepočítal se zálohováním takového prostředí, jako je blade s využitím virtualizace. Nyní bylo třeba nadefinovat zálohy na úrovni serverovny, racku, fyzických serverů a blade a na úrovní virtualizačních prostředků. Všechny procesy záloh výpočetního střediska jsou popsány a definovány v dokumentu „Havarijní plán 2012“

Zálohou na úrovni serverovny se rozumí zajištění tzv. „blackoutu“. To je zajištění provozuschopnosti i při delším výpadku proudu. Dodávku elektřiny zajišťuje Dieselagregát schopný nepřetržitého provozu.

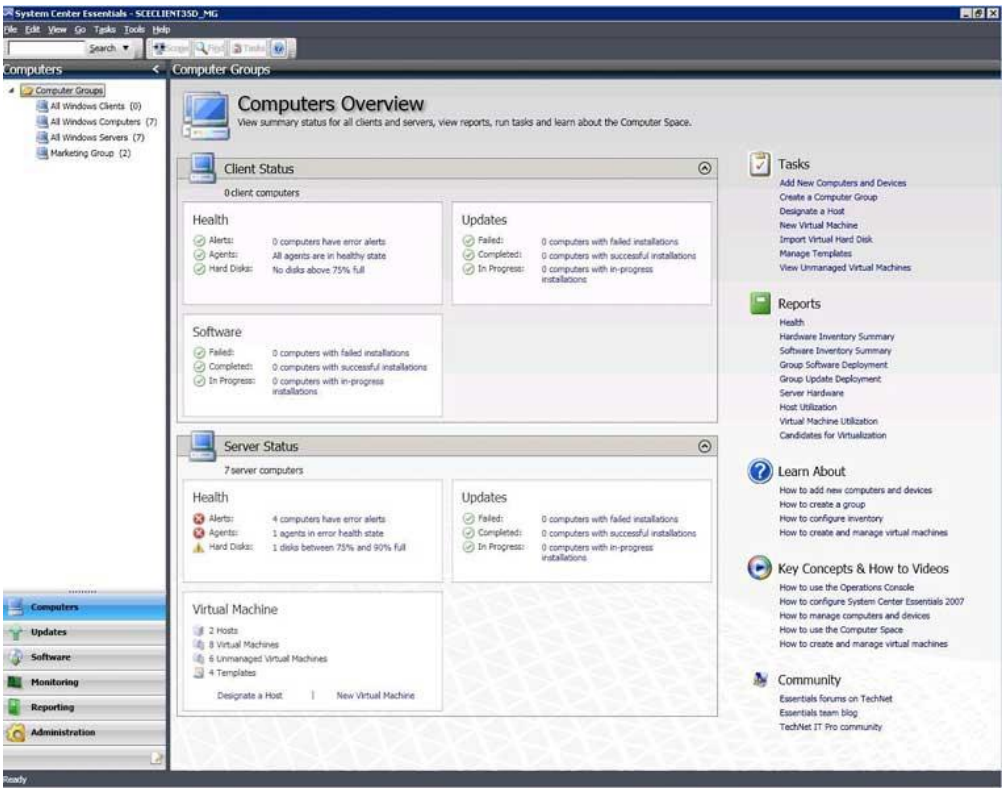
V každém racku 2,3 a 4 je zapojená vysokokapacitní automatická UPS. Ta je nastavena tak, aby v případě poklesu napětí pod kritickou úroveň vyslala příkaz na Management server, který pomocí skriptu ukončí všechny procesy v doméně a vypne nebo „pausne“ všechny servery. Klientských stanic a výrobních linek se toto opatření netýká.

Před samotným vypnutím fyzických serverů se virtuální servery automaticky uvedou do režimu spánku tak, aby mohly být kdykoliv uvedeny do původního stavu. Všechny virtuální servery se ukládají v podobě image každou noc na diskové pole.

Jednou týdně jsou zálohy virtuálních strojů a databáze zálohovány na páskové média. Vše se zálohuje systémem Disk-to-Disk-to-Tape. Tento proces je časově značně náročný, proto jej obsluha spouští v pátek na konci směny.

Všechny virtuální servery jsou vytvořené v clusteru. Je tak zajištěno, že se výroba nezastaví ani v případě havárie některého ze serverů.

Všechny operace zálohování na úrovni OS řídí produkt System Center Data Protector Manager (SCDPM). SCDPM (obr. 26) má přesně definovány časy a způsoby zálohování. Protože součástí záloh jsou citlivá data, včetně fotek, je každá záloha vyhodnocena z hlediska komprese a způsobu zašifrování zálohy. Kryptografickou podporu zajišťují opět síťové kryptokarty.



Obr. 26 Konzole pro správu SCDPM [vlastní zpracování]

7 VYTVOŘENÍ AUTENTIZAČNÍ A CERTIFIKAČNÍ POLITIKY

Dle požadavku zadávající firmy bylo součástí implementace řešení přihlašování čipovou kartou. Technologie autentizace čipovou kartou byla vyhodnocena jako dostatečně bezpečná pro užití ve výrobě s bezpečnostním režimem práce. Primárně byla tato technologie zvolena proto, že nabízí vysokou bezpečnost s využitím nejnovějších PKI technologií elektronického podpisu. Výhoda použití čipových karet je také v tom, že se auditní události v systému zaznamenávají přímo pod přihlášeným uživatelem a při bezpečnostním incidentu nebo chybě operátora je jasně patrné, kdo měl zrovna úsek na starost.

7.1 Výběr HW komponent

Pro dodávku autentizačního systému bylo nutné zvolit vhodnou technologii. Zda bude výhodnější vybudovat kontaktní nebo bezkontaktní přihlašovací systém. Zde byla jednoduchá volba. I když jsou dnes bezkontaktní Smart Card technologie zcela bezpečné a moderní, pořízení nových bezkontaktních čteček ke každému serveru, klientskému PC a k výrobní lince by značně prodražilo celou zakázku. Nejen, že kontaktní čtečky jsou řádově 2x levnější variantou, ale kvůli používané komerční certifikační autoritě již u většiny klientských PC jsou kontaktní čtečky k dispozici. Navíc při použití bezkontaktní karty na pracovišti není možné ověřit, zda je to stále ten samý zaměstnanec. U použití kontaktní karty musí být tato po celou dobu zasunuta ve čtečce. Princip si popíšeme níže.

7.2 Budování certifikační autority

Podmínkou využití autentizace čipovou kartou je provoz v rámci domény a vybudování certifikační autority na doménové úrovni. Pro instalaci bylo tedy nejvhodnější využít Management server, který je provozován na nejnovější verzi Windows Serveru 2008 R2, a na kterém je i doménový řadič.

Důležité je také uvědomit si, že chceme vybudovat kořenovou certifikační autoritu s novým privátním klíčem. Tím definujeme klíč s certifikátem, oproti kterému se budou jednotliví uživatelé ověřovat. Pro klíč se musí zvolit vhodný zprostředkovatel kryptografických služeb, jeho délka a hash algoritmus. Klíč je uložen v systémovém úložišti serveru. Klíče ke klientským certifikátům budou uloženy na čipových kartách

7.2.1 Instalace

Certifikační autorita byla nainstalována pomocí nástroje Server Manager, kde byla certifikační autorita přidána jako nová role serveru.

Konfigurace certifikační autority musí být nainstalována a nakonfigurována dle požadavků zákazníka.

Jednotlivé kroky instalace jsou uvedeny v příloze PII Postup instalace certifikační autority

7.2.2 Nastavení politik

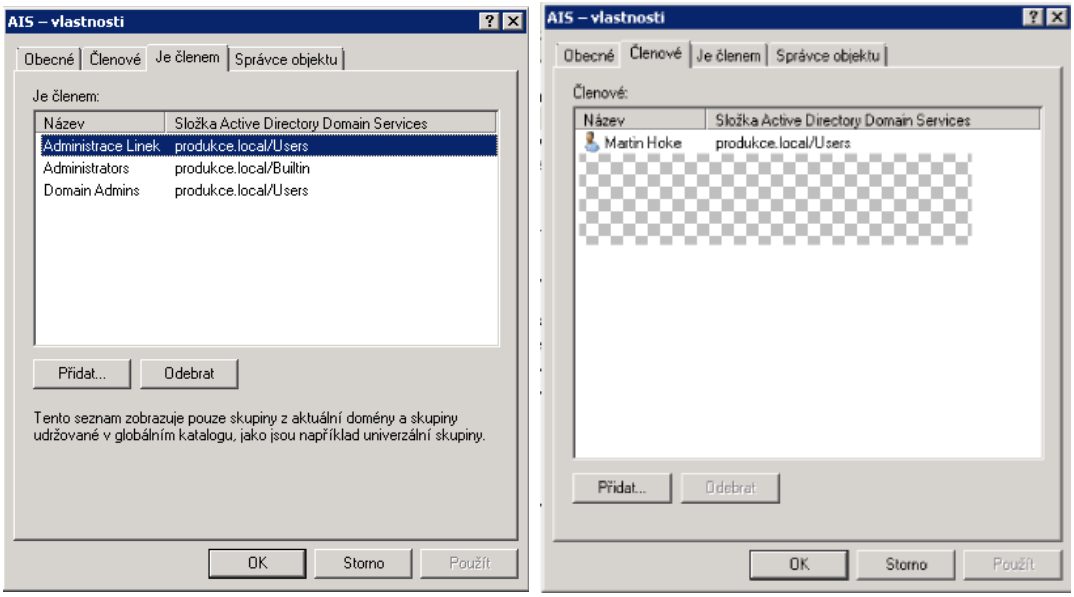
Autentizace do systému s využitím CA funguje na principech asymetrické kryptografie, tedy tak, že se vždy využívá páru šifrovacích klíčů, kdy jeden je soukromý a druhý veřejný. Nejznámějším asymetrickým algoritmem je RSA algoritmus.

Pro naši certifikační autoritu bylo nejdůležitější konfigurovat vhodné politiky tak, aby celá certifikační autorita byla dostatečně důvěryhodná a bezpečná vůči produkčnímu prostředí využívající externí certifikační autoritu I.CA.

Každý zaměstnanec musí mít na úrovni domény zřízen vlastní účet s definovaným umístěním v doménových skupinách. Skupiny mají na úrovni domény definovány přístupová práva pro vykonávání jednotlivých fází výroby. Skupiny jsou vytvořeny následně:

- AIS – Administrátor informačního systému, uživatelé mají neomezená práva na úrovni systémových komponent, údržby systému, nemohou se zapojit do výrobního procesu.
- OV - Operátor výroby, uživatelé mají právo sestavovat a zadávat dávky výroby do produkce, mohou obsluhovat výrobní linku i výstupní kontrolu.
- VL – Obsluha výrobní linky, může přijímat nové dávky na výrobní linku a ovládat výrobní linku.
- OVK – Operátor výstupní kontroly, může načíst vyrobenou kartu a oproti databázi zkontrolovat správnost výroby. OVK nese zodpovědnost za hotovou dávku.

Pro příklad uvádím snapshoty zařazení skupiny AIS do doménové struktury (obr. 27).

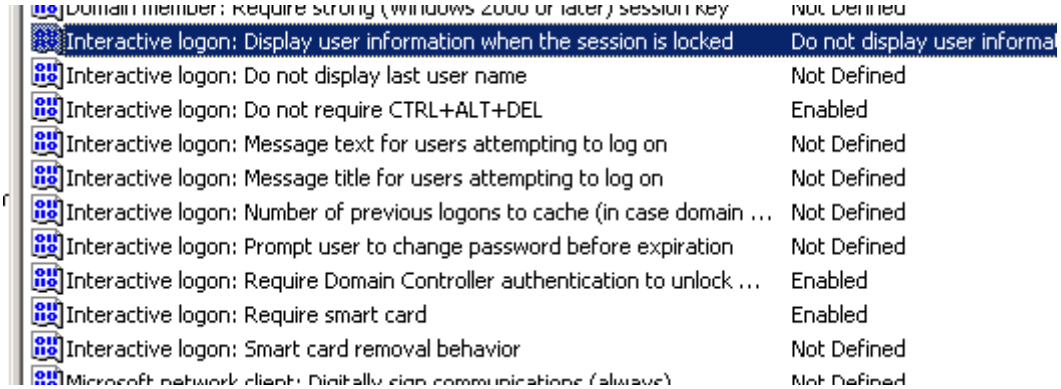


Obr. 27 Přiřazení uživatele AIS do skupin[vlastní zpracování]

Samotná karta je proti zneužití chráněna číslem PIN, kterou obdrží každý zaměstnanec v PINové obálce spolu s novou kartou. Při přihlášení do systému musí uživatel zadat tento PIN. Díky kontaktní verzi čipové karty je na úrovni domény nastaveno automatické odhlášení uživatele při vysunutí karty ze čtečky. Nemůže se tedy stát, že by někdo zneužil pracoviště bez přítomnosti přihlášeného.

Součástí certifikační autority je také vytvoření CRL, což je v podstatě seznam odvolaných, již neplatných certifikátů. Tento seznam zabraňuje zneužití ztracené, či ukradené karty s platným certifikátem a měl by být nedílnou součástí každé bezpečné CA.

Pro vynucení karty pro přihlášení a pro splnění klientových požadavků je nutné v zásadách domény nastavit pravidla viz obrázek č. 28:

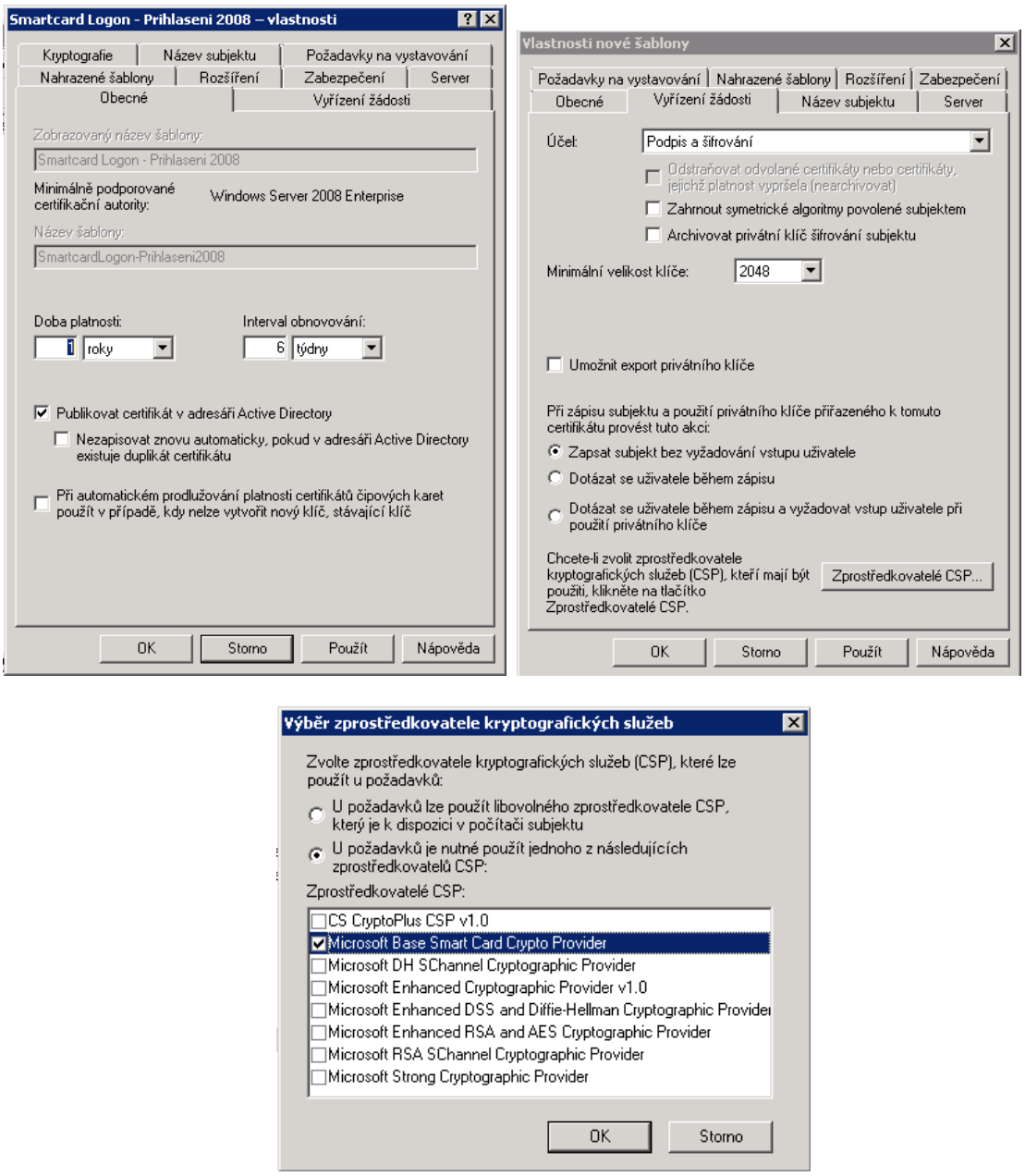


Obr. 28 Definování doménových pravidel pro Smart Card Logon [vlastní zpracování]

7.2.3 Vystavení osobního certifikátu

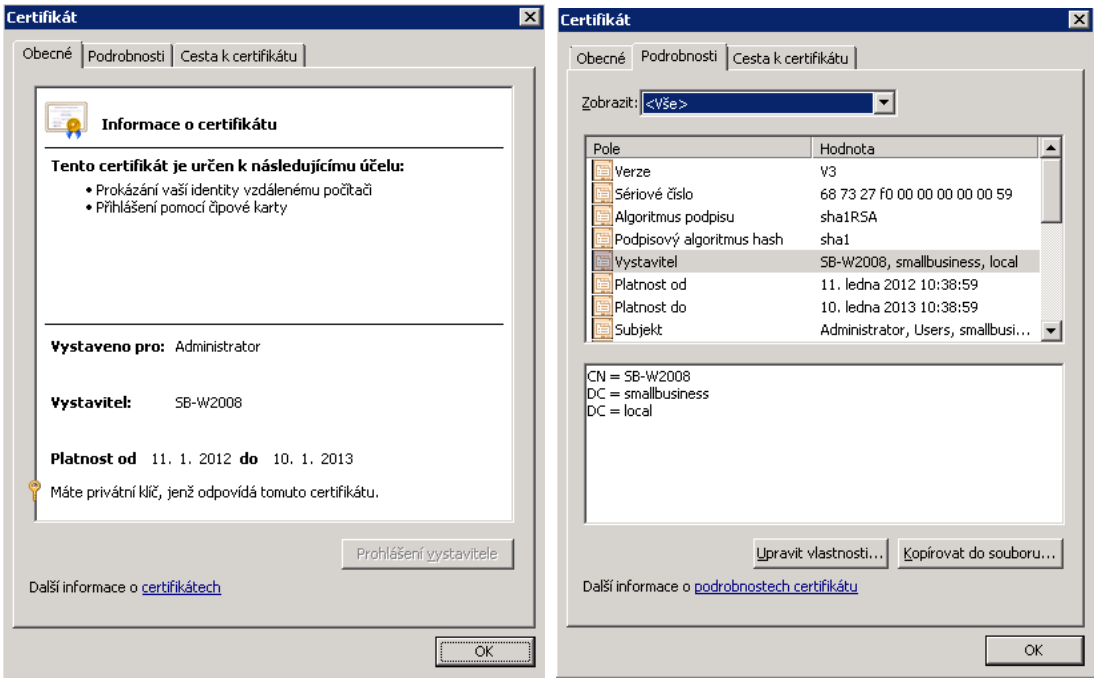
Každý zaměstnanec obdrží oproti podpisu čipovou kartu s jedinečným číslem (CLN) a na nově vzniklé certifikační autoritě si nechá u správce systému vygenerovat osobní kvalifikovaný certifikát s platností 1 rok .

Pro vydání certifikátu je nutné na certifikační autoritě definovat šablonu, podle které se budou certifikáty vystavovat a jaké CSP budou využívat. CSP certifikátu řekne, jakým způsobem má být vytvořen, kde má být uložen a jakým způsobem k němu budou aplikace přistupovat.



Obr. 29 Definování šablony pro vydávání přihlašovacích certifikátů [vlastní zpracování]

V certifikátu je jednoznačně uvedeno použití klíče, tedy pouze autentizace do systému. Obsahuje také osobní informace o držiteli karty, jako je jméno, pracovní pozice a skupina, do které patří.



Obr. 30 Certifikát pro přihlášení do domény [vlastní zpracování]

V certifikátu je také uveden platný odkaz na CRL. Takže při přihlášení se automaticky kontroluje platnost použitého certifikátu.

8 EKONOMICKÝ VÝHLED A ZHODNOCENÍ MIGRACE

Vzhledem k tomu, že projekt je již funkční a implementace byla dokončena, je potřeba podrobit daný projekt též ekonomickému zhodnocení a časové analýze, aby došlo ke zhodnocení celé akce.

8.1 Účel zpracování studie

Migrace na nový bladový systém byla vedením zadávající firmy zvolena za účelem zjednodušení a zefektivnění stávajícího výrobního systému. Cílem bylo začlenit novou zakázku do výroby a za pomocí nových HW technologií dosáhnout vyšších výkonů výrobní linky a zefektivnit tak náklady na vybavení IT technologií.

8.2 Stávající náklady na provoz stávajícího vybavení a výpočet návratnosti na pořízení nového vybavení

V době před implementací nového systému byly náklady na provoz ovlivněny provozem všech serverů na fyzických strojích. Tyto stroje měly velký podíl na spotřebě elektrické energie celé výroby. Bylo také velmi nákladné udržovat tyto stroje s pomocí externí servisní společnosti. Dále zde bylo riziko nedostupnosti náhradních komponent. Aspekt údržby fyzických strojů a nutnost implementace nových serverů byly vyhodnoceny jako největší míra pro pořízení nového vybavení.

Díky využití virtualizace se několikanásobně zlevnilo pořízení nového vybavení, hlavně díky využití multilicencí na operační systémy virtuálních strojů. Díky jednoduchosti implementace této technologie se mohou vnitrofiremní administrátoři více zapojit do údržby vlastního vybavení. Tím odpadnou značné náklady na údržbu a servis externí firmou. Ekonomickou návratnost investice do nového systému nelze v tuto chvíli jednoznačně spočítat, neboť vinou krátkého času na testování nového systému ve výrobě nelze určit, jak vysokou měrou zvýšený výkon přispěje do produkce výroby čipových karet. Nový systém je též považován za stabilnější a je zde nižší předpoklad neočekávané odstávky ve výrobě. Vzhledem k tomu, že náklady na HW činily 2358502,- Kč a SW 309924,- Kč + 15% marže dodavatele, předpokládá se, že návratnost celého projektu bude do 5 let. Tyto údaje byly zjištěny na základě výsledků zkoumání projekčního týmu. Konkrétní údaje zahrnující položky nového HW, výrobce, dodavatele i přesných cen,

zahrnuje tabulka č. 4 a 5. Tabulka odkazuje na pořizovací ceny pro subdodavatele, čili zde není zahrnuta marže ve výši 15%.

Tabulka 4 Seznam dodaných HW komponent a jejich nákupní cena [vlastní zpracování]

Pořízení nového HW					
Položka	**Typ**	**Výrobce**	**Dodavatel**	**Počet**	**Cena bez DPH**
Blade Chassis	HP BladeSystem c7000 Enclosure	hewlett packard	Alwil Trade s.r.o.	1	397785
Server	HP ProLiant BL460c	hewlett packard	Alwil Trade s.r.o.	5	233620
HDD Server	HP 72GB 15K 6G 2.5 SAS DP HDD	hewlett packard	Alwil Trade s.r.o.	10	56860
Switche	HP ProCurve 6120xg	hewlett packard	Alwil Trade s.r.o.	2	494426
Pásková mechanika	HP StorageWorks SB1760c Tape Blade	hewlett packard	Alwil Trade s.r.o.	1	79355
Pásky	HP LTO4 Ultrium 1,6TB RW	hewlett packard	Alwil Trade s.r.o.	4	2456
DVD vypalovačka	Externí DVD slim vypalovačka	hewlett packard	Alwil Trade s.r.o.	1	879
Diskové pole	HP P2000 LFF Modular Smart Array	hewlett packard	Alwil Trade s.r.o.	2	114214
HDD pole	HP HDD SAS 300GB 15k	hewlett packard	Alwil Trade s.r.o.	12	106788
HDD pole	HP HDD SAS 750GB 7,5k	hewlett packard	Alwil Trade s.r.o.	4	40928
Síťové HSM	netHSM PL220	SafeNet	DNS a.s.	1	171846
Síťové HSM	netHSM PL600	SafeNet	DNS a.s.	2	446798
iSCSI kabely	HP BLc SFP+ 1m 10GbE Copper Cable	hewlett packard	Alwil Trade s.r.o.	8	25848
KVM adaptéry	HP BladeSystem CAT5 KVM Intf Rmkt Adptr	hewlett packard	Alwil Trade s.r.o.	2	4794
Switche	Cisco C3560, 10G Network Module	Cisco	Alwil Trade s.r.o.	2	181500
Čtecky	GemPC USB TR	Gemalto	Gemalto	4	405
Celkem				57	2358502

Tabulka 5 Seznam dodaných SW komponent a jejich nákupní cena [vlastní zpracování]

Licence SW				
Sloupec1	**Sloupec2**	**Sloupec3**	**Sloupec4**	**Sloupec5**
typ	Produkt	Licence	počet	Cena bez DPH
OS Management	Windows Server 2008 R2 x64 Enterprise	Enterprise	1	44386
OS Virtualizace	Windows Server 2008 R2 x64 datacenter	Datacenter	2	147500
OS DB	Windows Server 2008 R2 x64 Enterprise	Enterprise	2	23758
Dohled	System Center Operation Manager	w SQL Tech	1	42270
Správa	System Center Virtual Machine Manager	w SQL Tech	1	42170
OS VIRT	Windows Server 2008 R1 x86 Enterprise	Virtual OEM	4	9840
Celkem				309924

Pro úplnost informací je zde potřeba dále zmínit i časovou hledisko. Časová náročnost celého projektu od zadání zakázky až po akceptaci implementace byla 8 měsíců. Nejnáročnější fází byla příprava na implementaci a navržení testovacích scénářů konfigurací operačních systémů a virtuálních strojů.

8.3 Přínosy navrženého řešení

Přínosy celého projektu lze definovat následovně:

- **Využití výkonnějšího zařízení** zvýšilo výkon celé výrobní linky a nyní se může vyrábět více čipových karet. Přechodem na virtualizaci se docílilo efektivnějšího využití finančních prostředků tak, že nebylo nutné dokupovat chybějící fyzické servery a hlavně kryptokarty, které jsou značnou položkou. Jejich pořízení do každého ze serverů by několikanásobně zvýšilo celý rozpočet.
- **Úspora elektrické energie**. Management bladu zajišťuje efektivní využití napájecích zdrojů a přiděluje příkon jednotlivým fyzickým serverům tak, jak aktuálně vyžadují. Oproti stávající sestavě je nově v provozu pouze 13 elektrických zdrojů.
- **Modernější a výkonnější technologie.** Zde je potřeba zmínit především virtualizaci serverů, která přinesla značné úspory při pořizování nových serverů a jejích následném provozu. Další velkou výhodou je možnost efektivnějšího zálohování a sledování celého systému. Celý systém může být zdvojen bez ohledu na provozní náklady a je tak zajištěna vysoká dostupnost jednotlivých komponent a aplikací.

- **Úspora finanční prostředků** vyčleněných na údržbu a servis stávajících strojů u outsourcingové firmy

8.4 Nedostatky

Vzhledem k tomu, že se jedná o relativně spolehlivé technologie, bylo velmi složité najít nedostatky. V tomto případě výhody převažují nevýhody, což je velmi pozitivní.

Při hlubším zamyšlení se jako hlavní nedostatek jeví např. fakt, že nebylo efektivně využito celé bladové chassis, když se do budoucna počítá s tím, že ke stávajícímu systému bude v budoucnu přiřazena i další výrobní linka, která bude vyžadovat vybudování dalšího systému.

Další nevýhodou je dle mého názoru návrh tří domain controllerů, které by se daly za určitých okolností integrovat do jediného. Systém tak musí zbytečně pracovat se třemi domain controllery, které mohou méně zkušenému administrátorovi způsobit komplikace při údržbě celého systému.

Za neovlivnitelný nedostatek považuji také to, že výrobní součást – okruh výrobní linky využívá zastaralé technologie, které neumožňují užití centralizované správy spolu s novým systémem.

8.5 Další možný rozvoj systému

Vzhledem k tomu, že implementace tohoto řešení představuje vrchol využití moderních technologií ve výpočetních centrech, není jednoduché alespoň nastínit možný budoucí vývoj takového systému. Přesto zde jisté rezervy určitě jsou a na následujících stránkách budou charakterizovány.

Jako další možný rozvoj systému je možné vidět hlavně v eliminování nastíněných nedostatků. Tudíž při dalším rozvoji by měl být kladen důraz na zaplnění chassis tak, aby byla lépe využita výhoda interlinků bladu. Z tohoto pohledu se do budoucna jistě najde důvod rozšířit stávající využití

Dalo by se také uvažovat o přesunu dvou linuxových serverů do bladového chassis a jejich napojení na nové netHSM moduly, které mají dostatečný výpočetní šifrovací výkon na to, aby pokryly potřeby všech šifrovacích operací. Pro takový přesun by ale musela být provedena hlubší analýza. Jak bylo totiž řečeno, tyto servery mají bezpečnostní funkci na

výrobu čipových karet. Dosud využívané PCI kryptomoduly by tak mohly být využity pro testování bezpečnostních operací.

Zcela jistě přijde také doba, kdy se budou muset revidovat a upgradovat stávající politiky doménových řadičů, ty byly v rámci časových úspor převzaty ze stávajícího systému a přinesly si tak s sebou léty zanesená, zbytečně omezující a nesmyslná pravidla.

Největší potenciál pro rozvoj lze též spatřit v ještě větší centralizaci správcovských komponent a hlubší využití produktů z rodiny System Center. Pokud by vedení firmy více investovalo do vzdělání svých administrátorů, mohlo by lépe využít potenciál nasazených produktů a ještě více zajistit bezpečnost svých investic.

ZÁVĚR

Diplomová práce se zabývá vysoce aktuální problematikou, týkající se využití a nasazení bladových řešení v rámci malých datových center. Firma, jež se zabývá výrobou čipových karet vypsala zakázku, která se zabývala zavedení výroby nového typu čipových karet. Společnost, ve které pracuji, tuto zakázku vyhrála a jsem velmi rád, že toto atraktivní téma mi mohlo být předlohou pro zpracování diplomové práce.

Cílem diplomové práce bylo navrhnout a implementovat potřebné prvky datového centra pro řešení nového výrobního systému, zabývajícího se, jak bylo uvedené výše, výrobou čipových karet.

V teoretické části jsem na základě studia odborné literatury analyzoval a následně vypracoval rešerši na téma bladových řešení a jejich vztahu k virtualizaci. Byly vysvětleny základy pojmy, jež je nezbytné osvojit si, pro pochopení celé problematiky. Z jednotlivých zdrojů jsem se snažil vybrat vždy nejsrozumitelnější zpracování.

V praktické části jsem se pak věnoval podrobnému popisu implementace bladového řešení, návrhu systému autentizace, ekonomickému dopadu implementace a vyhodnocení nového řešení.

Během příprav na finální implementaci jsme se s naším implementačním týmem setkali s mnoha problémy, se kterými jsme si museli poradit, dostali jsme se několikrát do časové tísně a bylo nutné na projektu pracovat i ve volném čase.

Cílem této práce nebylo poskytnutí detailního návodu, jak postupovat při modernizaci datového centra, ale seznámit se s problémy a nastínit základní předpoklady pro rozvoj komerční výrobní linky. Z práce by měla být patrná časová náročnost celého projektu.

Navrhnout systém autentizace pro mne nebyl těžký úkol. V rámci mého zaměstnání se kryptografickými a autentizačními technologiemi setkávám denně. Pro specifický zabezpečený provoz bylo ale potřeba pamatovat na všechny bezpečnostní aspekty a dle toho upravit stávající bezpečnostní politiky tak, aby neodporovali původnímu návrhu zabezpečení celého systému.

Diplomovou práci jsem navíc doplnil o fotografie zapojených komponent, na kterých je vidět složitost propojení celého výpočetního systému.

V poslední kapitole jsem vyhodnotil celou implementaci z ekonomického hlediska, pokusil jsem se shrnout přínosy a zápory tohoto řešení a nastínit další rozvoj systému.

ZÁVĚR V ANGLIČTINĚ

This thesis deals with highly topical issues concerning the use and deployment solutions blades in small data centers. The company, which deals with the production of smart cards, announced a state contract to deal with introduction of a new type of smart card Company in which I work, has won this contract and I am very pleased that this attractive theme I could be a model for my thesis.

The aim of my thesis is to propose and implement necessary components of the data center for the new production system solution.

In theoretical part I analyzed and subsequently worked out the research of blade solutions and their relations to virtualization on the basis of stated literature. I tried to find the most understandable arrangement from particular sources.

Practical part deals with the detailed description of blade solution implementation, the proposal of authentication system, the economical impact of implementation and evaluation of the new solution.

During the final implementation preparations our team faced many problems that we had to deal with. We were often pressed for time and we had to work on the project in our spare time.

The goal of this thesis was not to provide detailed instructions how to proceed when modernize the data center, but to make readers familiar with possible problems and to outline basic requirements for the commercial production line development. The thesis should point out how time demanding the whole project is.

The suggestion of authentication system was not difficult for me. Every day I deal with the cryptographic and authentication technologies in my work. For the specific secured operation it was necessary to remember all security aspects and according to this improve current security policies so as not to contradict with the original system security suggestion.

Furthermore I completed the thesis with the photos of connected components, where can be seen the complexity of computing system connection.

In the last chapter I evaluated the whole implementation from the economical point of view; I tried to sum up the contributions and negatives of this solution and to outline the system development.

SEZNAM POUŽITÉ LITERATURY

[1] Produktová řešení - Blade servery [online]. [cit. 2012-05-13]. Dostupné z: http://muj.autocont.cz/produktove-reseni-blade.aspx

[2] BAČINA, Ondřej. *Blade Servery – Pro koho jsou určeny ? Jaké mají výhody a nevýhody ?* [online]. [cit. 2012-05-13]. Dostupné z: http://www.optimalizovane-it.cz/servery/blade-servery-pro-koho-jsou-urceny-jake-maji-vyhody-a-nevyhody.html

[3] UNIS COMPUTERS. *Servery a diskové systémy - ukládání a záloha dat* [online]. [cit. 2012-05-13]. Dostupné z: http://www.uniscomp.cz/t/servery-a-diskove-systemy-ukladani-a-zaloha-dat/1103.?lang=cs

[4] WEDOS INTERNET, a.s. *Management blade serverů Fujitsu* [online]. 10.11.2010 [cit. 2012-05-13]. Dostupné z: http://datacentrum.wedos.com/a/122/management-blade-serveru-fujitsu.html

[5] *KVM Switch* [online]. 28. 10. 2011 [cit. 2012-05-13]. Dostupné z: http://cs.wikipedia.org/wiki/KVM_Switch

[6] LAKA CZ S.R.O. *Malé serverovny* [online]. [cit. 2012-05-13]. Dostupné z: http://www.laka.cz/poradna/male-serverovny

[7] PRIMEENERGYIT. *Energeticky efektivní IT a infrastruktura pro datová centra a serverovny* [online]. [cit. 2012-05-13]. Dostupné z: http://www.efficient-datacenter.eu/fileadmin/docs/dam/brochures/brochure_cz.pdf

[8] MICHAELI, Tomas. *Dalším prostorem k úsporám je efektivní návrh infrastruktury* [online]. [cit. 2012-05-13]. Dostupné z: http://www.netguru.cz/odborne-clanky/trendy-v-datovych-centrech-centralizace-virtualizace-power-management.html

[9] PAŠEK, David. DELL. *Tři z nejsilnějších - srovnání serverové virtualizace VMware vs. Citrix vs. Microsoft* [online]. [cit. 2012-05-13]. Dostupné z: http://www.vmwarenews.cz/vmw/vmwnews.nsf/0/53BB1B111BE5A818C12575E5005F83A6

[10] HRŮŠA, Petr. AQUASOFT. *Jak virtualizace platforem mění výpočetní centra?* [online]. 24. 11. 2011 [cit. 2012-05-13]. Dostupné z: http://www.aquasoft.eu/blog/nazor_odbornika.php?nazor=452

[11] VÝŠEK, Ondřej. MVP. *Hyper-V vs VMware* [online]. [cit. 2012-05-13]. Dostupné z: http://www.tchk.cz/kalendar-hyper-v-vs-vmware-ondrej-vysek-mvp-52.html

[12] HRŮŠA, Petr. AQUASOFT. *Výhody a nevýhody virtualizace platforem a aktuální nabídka* [online]. 24. 11. 2011 [cit. 2012-05-13]. Dostupné z: http://www.aquasoft.eu/blog/nazor_odbornika.php?nazor=450

[13] ALWIL. *VMware ESX a VMware ESXi* [online]. [cit. 2012-05-13]. Dostupné z: http://www.alwil.com/vmware-esx-a-vmware-esxi.html

[14] POMAZAL, Jiří. *Hyper-V: Virtualizační technologie vhodná pro větší firmy* [online]. 13.3.2009 [cit. 2012-05-13]. Dostupné z: http://www.itbiz.cz/hyperv-virtualizacni-technologie

[15] MICROSOFT. *Virtualizace s Hyper-V: Přehled* [online]. [cit. 2012-05-13]. Dostupné z: http://www.microsoft.com/cze/windowsserver2008/hyper-v/overview.aspx

[16] PAVLIS, Martin. *Instalace a nastavení virtualizovaného prostředí na platformě Hyper-V*: *Seriál: Virtualizace v praxi (2. díl)* [online]. [cit. 2012-05-13]. Dostupné z: http://www.systemonline.cz/virtualizace/instalace-a-nastaveni-virtualizovaneho-prostredi-na-platforme-hyper-v.htm

[17] ŘEPA, Pavel. MICROSOFT MVP. [online]. [cit. 2012-05-13]. Dostupné z: http://pavelrepa.wordpress.com/category/app-controller-scac/

[18] MICROSOFT. *Role produktů System Center v dynamickém IT* [online]. [cit. 2012-05-13]. Dostupné z: http://www.microsoft.com/cze/systemcenter/produkt/prehled.aspx

[19] ŘEPA, Pavel. MICROSOFT MPV. *Využití SCVMM vNext aneb představení vize správy datových center* [online]. [cit. 2012-05-13]. Dostupné z: http://pavelrepa.wordpress.com/2011/04/05/vyuzit-scvmm-vnext-aneb-predstaven-vize-sprvy-datovch-center/

[20] *System Center Virtual Machine Manager* [online]. [cit. 2012-05-13]. Dostupné z: http://cs.wikipedia.org/wiki/System_Center_Virtual_Machine_Manager

[21] HEWLETT PACKARD. *Kompletní blade řešení.* [online]. [cit. 2012-05-13]. Dostupné z: http://h10126.www1.hp.com/bladerunner/

[22] *Blade server* [online]. [cit. 2012-05-13]. Dostupné z: http://webobjects2.cdw.com/is/image/CDW/2320495?$product_230$

[23] *Napájecí kabel* [online]. [cit. 2012-05-13]. Dostupné z: http://www.optimalizovane-it.cz/images/stories/writer/image_a76f2a85ea7df66ab3d8e83bfd6e1782.png [24] http://www.64bit.cz/galerie/3876/ibm-diskove-pole-system-storage-exp3000-sas-sata-default.jpg

[25] *Pásková mechanika* [online]. [cit. 2012-05-13]. Dostupné z: http://www.it.cz/doc/img/atc/EH847A-ULT_HH.JPG

[26] *Sálové klimatizace* [online]. [cit. 2012-05-13]. Dostupné z: http://upspowersupply.manufacturer.supplierlist.com/productsimages/intelligentonlineupssystem_120176.jpg

[27] *Topologie* [online]. [cit. 2012-05-13]. Dostupné z: http://www.cathedral.cz/obrazky/infrastructure.jpg

[28] FS CODES. *Microsoft Hyper-V Architecture* [online]. [cit. 2012-05-13]. Dostupné z: http://www.fscodes.cz/index.php/produkty-a-sluzby/virtualizace-a-konsolidace/microsoft-hyper-v?showall=1

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PC (Personal Computer) – osobní počítač

IS (informatic systém) – informační systém

SW (Software) – programové vybavení počítače

HW (hardware) – fyzické vybavení počítače

RAM (Random Acces Memory) typ elektronické paměti

DC (Data Center) – Datové centrum

ICT (Information and Comunication Technologies) – Informační a komunikační technologie

OS (Operation Systém) – Operační systém

IT (informatik technology) – informační technologie

I/O (input/output) – vstupně/výstupní

KVM (Keyboard Video Mouse) – HW zařízení umožňující ovládání vzdáleného počítače

iLO (integrated Lights-Out) – ovládací rozhraní od firmy HP

PCI-E (Peripheral Component Interconnect-Express) – standard systémové sběrnice

PDU (Power Distribution Unit) – elektrická distribuční jednotka

SAS (Serial Attached SCSI) – sériová sběrnice, která nahrazuje paralelní sběrnici

SCSI/SCSI (Internet Small Computer Systém Interface)– rozhranní pro připojení pevných disků

SAN (Storage Area Network) – dedikovaná datová síť

FC (Fibre Channel) – Gigabitové komunikační rozhraní

UPS (*Uninterruptible Power Supply) - zařízení zajišťující nepřetržitou dodávku elektřiny*

USB (Universal Seriál Bus) – univerzální sériová sběrnice

SD (Secure Digital) – typ paměťové karty

BIOS (*Basic Input-Output System*) - implementuje základní vstupně–výstupní funkce pro počítače

DEP (Data Execution Prevention) bezpečnostní funkce na modemech v Operačním systému

SMP (Symmetric Multiprocessors) – multiprocesorový systém s centralizovanou sdílenou pamětí

RSAT (Remote Server Administration Tools) – Administrační nástroje pro vzdálenou správu

SCVMM (System Center Virtual Machine Manager) – Produkt z rodiny System Center

SCOM (System Center Operation Manager) – Produkt z rodiny System Center

SCDPM (System Center Data Protector Manager) – Produkt z rodiny System Center

SCCM (System Center Configuration Manager) – Produkt z rodiny System Center

P2V (Physical-to-Virtual) – přechod z fyzické vrstvy na virtuální

HSM (Hardware Security Module) – Hardwarové šifrovací zařízení

I.CA – První Certifikační autorita

VLAN (Virtual LAN) – logicky nezávislá síť v rámci jednoho nebo několika zařízení

WSUS (Windows Server Update Services) – Služba pro ruční instalaci bezpečnostních záplat

DFS (Distributed File Systém) – Distribuovaný diskový prostor

MGMT - Management

MSSQL – Microsoft SQL

SIS (Single Instance Store) – funkcionalita technologií Microsoft

PKI (Public Key Infrastructure) – označení pro správu a distribuci veřejných klíčů

CA (Certification Authority) – Certifikační autorita

PIN (*Personal Identification Number) – Osobní identifikační číslo pro autentizaci*

CSP (Cryptographic Service Provider) – Poskytovatel kryptografické vrstvy

CRL (Certificate Revocation List) – seznam zneplatněných certifikátů

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

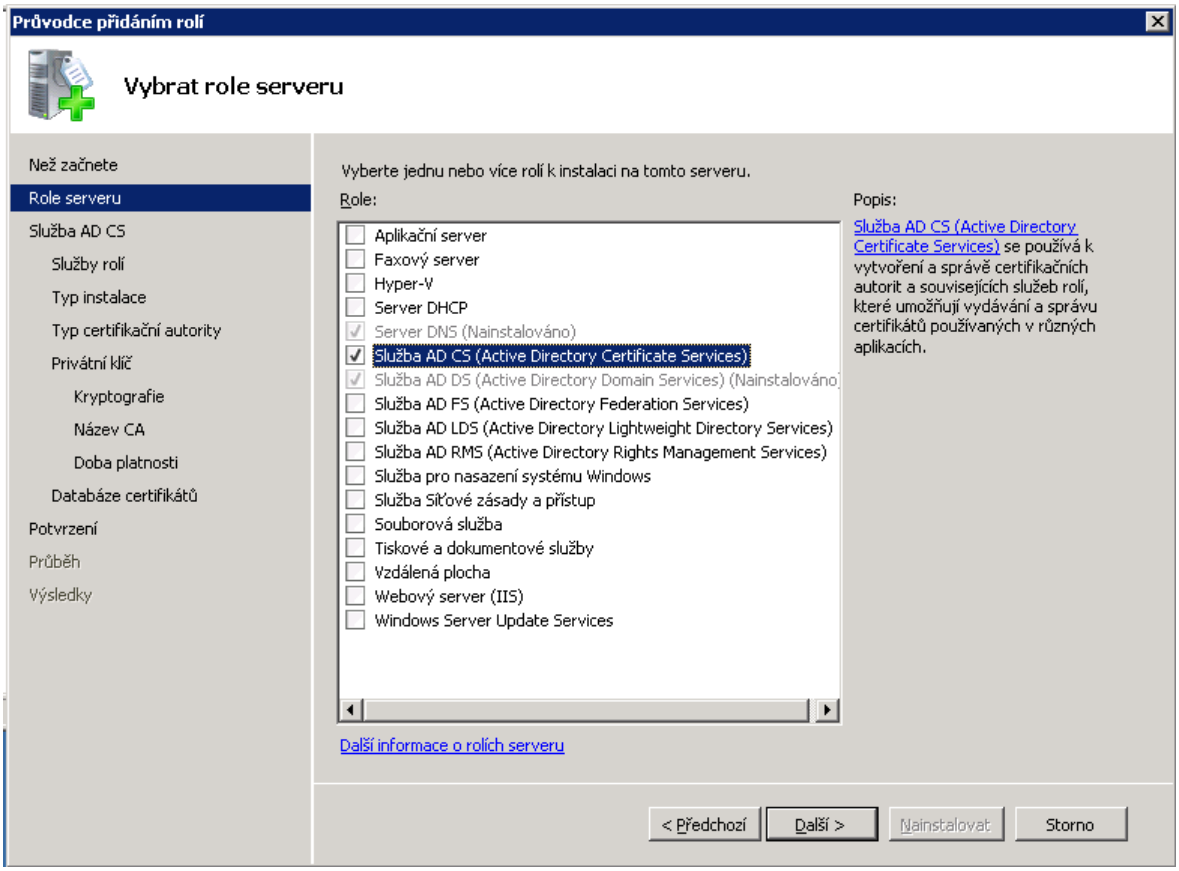
PŘÍLOHA P I: KONFIGURACE SÍŤOVÝCH PROSTUPŮ

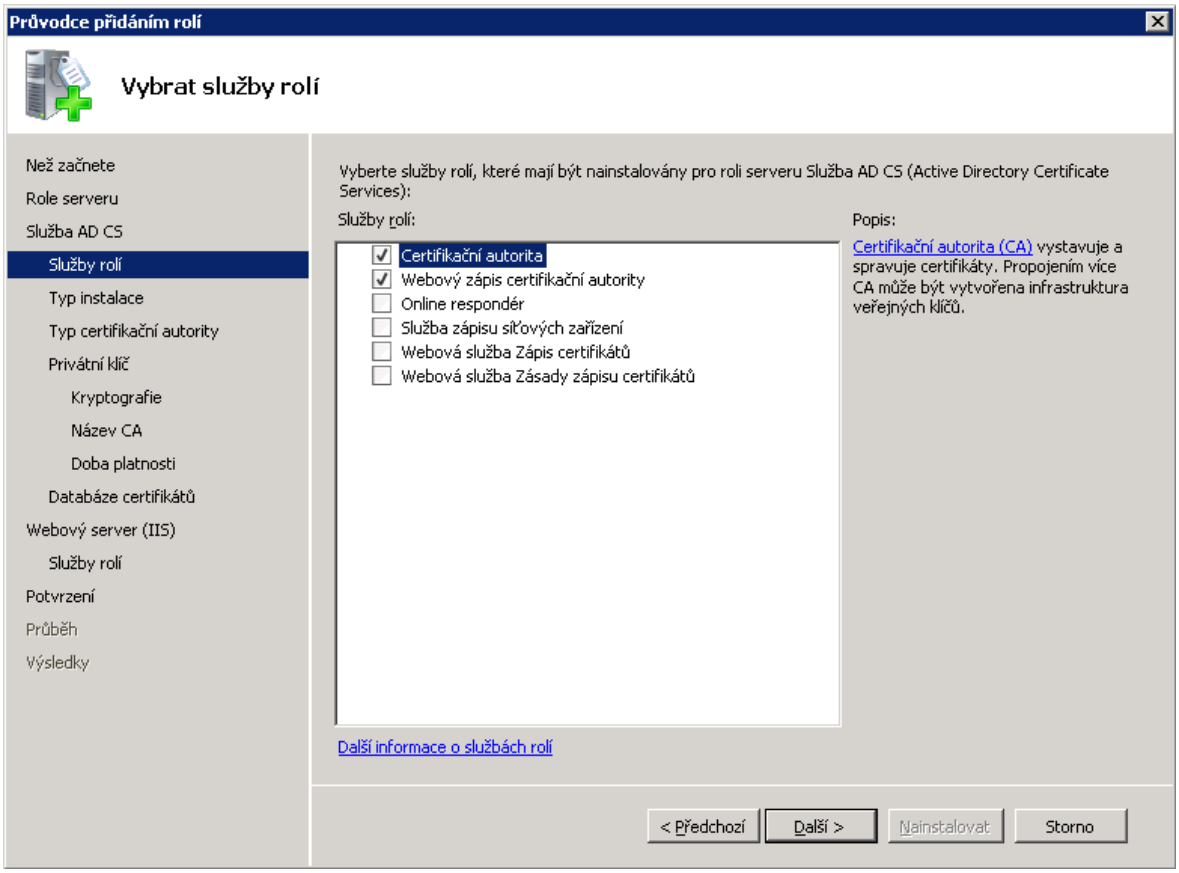
VLAN	Jméno	Prostup (VLAN, jeden směr)	IP bran (VRRP -default, CR1,CR2, HP1,HP2)	Interní servery		externí servery			
				jméno	IP	jméno	IP	Switch	Port
5	Management	50, 60, 70, 100	192.168.5.200	MGMT	192.168.5.10		192.168.5.20	HP1	17
			192.168.5.201	Virt1	192.168.5.11				
			192.168.5.202	Virt2	192.168.5.12				
			192.168.5.203						
			192.168.5.204						
7	Dohled	-	192.168.7.200			Pole Virt	192.168.7.1	CR1	11
			192.168.7.201				192.168.7.2	CR2	11
			192.168.7.202			Pole DB	192.168.7.3	CR1	12
			192.168.7.203				192.168.7.4	CR2	12
			192.168.7.204			ILo-ProCurve1	192.168.7.5	CR1	13
						ILo-ProCurve2	192.168.7.6	CR2	13
						ILo-Blade	192.168.7.7	CR1	14
						ILo-MGMT	192.168.7.10	CR2	14
						ILo-Virt1	192.168.7.11	CR1	15
						ILo-Virt2	192.168.7.12	CR6	15
						ILo-SDVDC	192.168.7.21	CR1	16
						ILo-SDVDD	192.168.7.22	CR2	16
10	iSCSI-A	-	-	Virt1	10.0.0.51	Pole Virt	10.0.0.41	HP1	18
				Virt2	10.0.0.53		10.0.0.43	HP1	20
				SDVDC	10.0.0.55	Pole DB	10.0.0.45	HP2	18
				SDVDD	10.0.0.57		10.0.0.47	HP2	20
				MGMT	10.0.0.59				
11	iSCSI-B	-	-	Virt1	10.0.1.54	Pole Virt	10.0.1.44	HP2	21
				Virt2	10.0.1.52		10.0.1.42	HP2	19
				SDVDC	10.0.1.58	Pole DB	10.0.1.48	HP1	21
				SDVDD	10.0.1.56		10.0.1.46	HP1	19

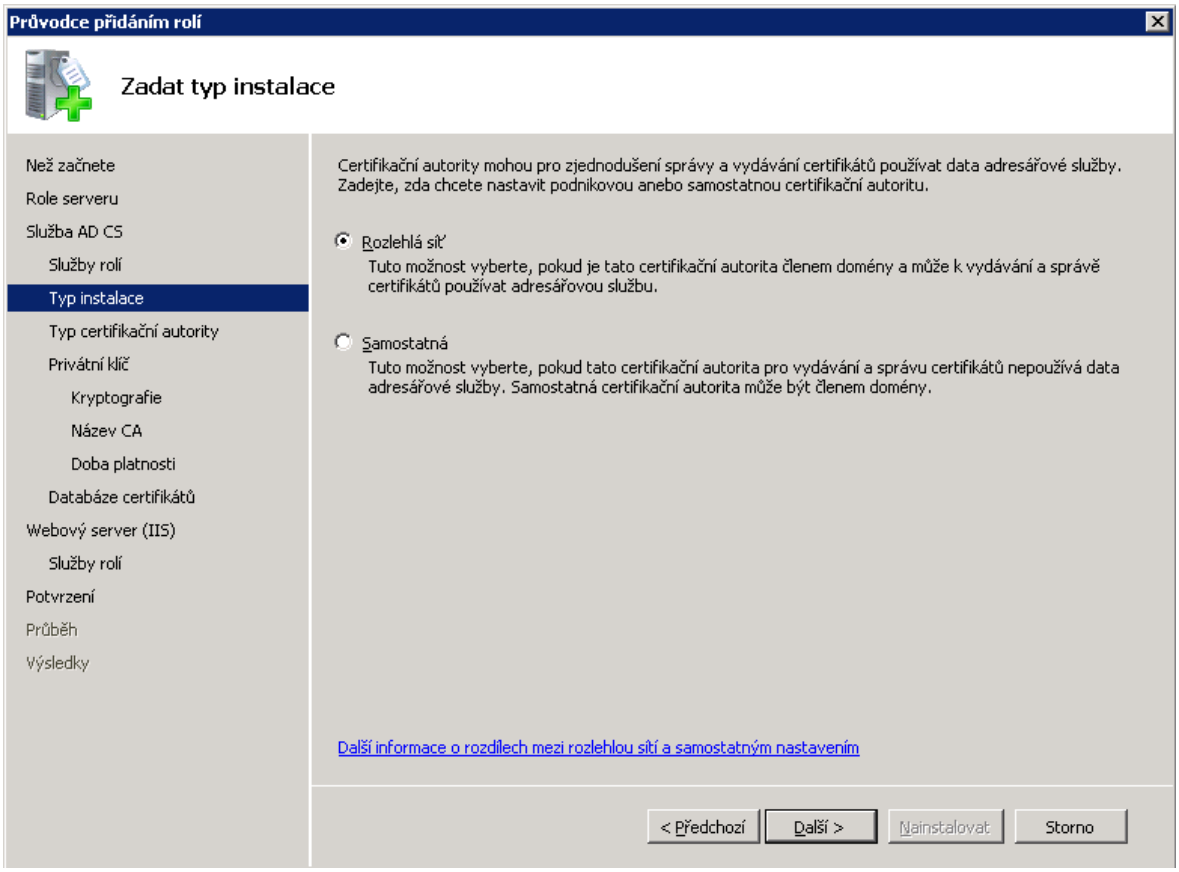
				MGMT	10.0.1.50				
15	Internal	-	-	Virt1	10.10.10.1				
				Virt2	10.10.10.2				
				SDVDC	10.10.10.11				
				SDVDD	10.10.10.12				
30	Test	-	192.168.30.200	PC-SRV-T3	192.168.30.230	PC_OFFICE_T4	192.168.30.14	CT	3
			192.168.30.201			PC_OFFICE_T5	192.168.30.15	CT	4
			192.168.30.202			Muhl1	192.168.30.110	CT	5
			192.168.30.203			Muhl2	192.168.30.111	CT	6
			192.168.30.204			Muhl3	192.168.30.112	CT	7
						MuhlVelký	192.168.30.114	CT	8
						MuhlMalý	192.168.30.115	CT	9
						MuhlDbMalý	192.168.30.116	CT	10
						Outco_eCD	192.168.30.22	CT	11
						Outco_ePKP/eID	192.168.30.27	CT	12
						Outco_eID	192.168.30.28	CT	13
						netHSM	192.168.30.229	CR1	7
								CR2	7
50	Řídící	60, 70	192.168.50.200	KS	192.168.50.246	work_1	192.168.50.11	CC	3
			192.168.50.201	KS_B	192.168.50.247	work_2	192.168.50.12	CC	4
			192.168.50.202			work_3	192.168.50.13	CC	5
			192.168.50.203			work_4	192.168.50.14	CC	6
			192.168.50.204			work_5	192.168.50.15	CC	7
						work_6	192.168.50.16	CC	8
						work_7	192.168.50.17	CC	9
						work_8	192.168.50.18	CC	10
						work_9	192.168.50.19	CC	11
60	DB	5, 50, 70	192.168.60.200	SDVDC	192.168.60.21				
			192.168.60.201	SDVDD	192.168.60.22				
			192.168.60.202						

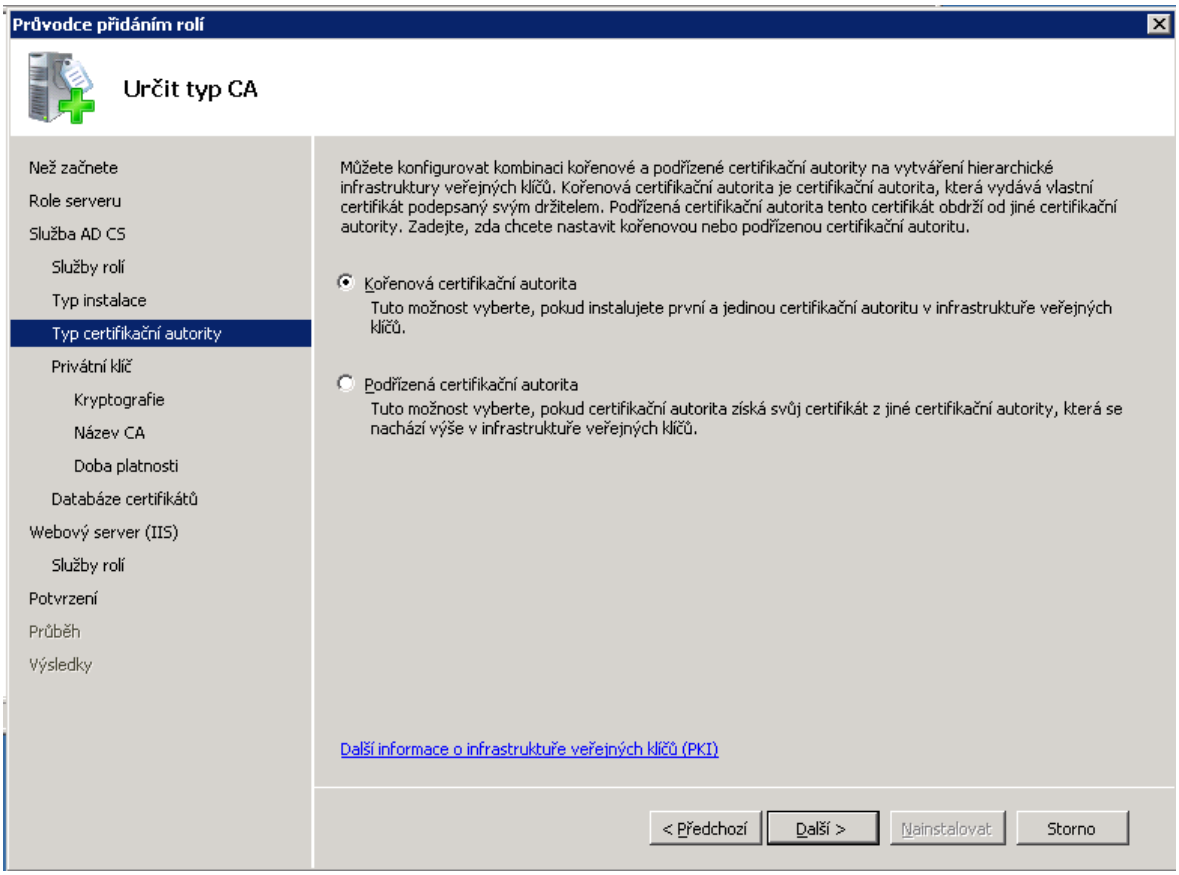
			192.168.60.203						
			192.168.60.204						
70	JPK	5, 50, 60, 100	192.168.70.200	JPK_A	192.168.70.11	netHSM_Prod_A	192.168.70.21	CR1	19
			192.168.70.201	JPK_B	192.168.70.12		192.168.70.22	CR2	19
			192.168.70.202	DC_A	192.168.70.5	netHSM_Prod_B	192.168.70.21	CR1	20
			192.168.70.203	DC_B	192168.70.6		192.168.70.22	CR2	20
			192.168.70.204						
100	Výrobní	70	192.168.100.200	DS	192.168.100.248	Muhl1	192.168.100.111	CV	3
			192.168.100.201	DS_B	192.168.100.249	Muhl2	192.168.100.112	CV	4
			192.168.100.202	DS_RP	192.168.100.228	Muhl3	192.168.100.113	CV	5
			192.168.100.203	DS_RP_B	192.168.100.229	MuhlVelký	192.168.100.114	CV	6
			192.168.100.204	DS_ID	192.168.100.226	MuhlMalý	192.168.100.115	CV	7
				DS_ID_B	192.168.100.227	Outco_1	192.168.100.21	CV	8
						Outco_2	192.168.100.22	CV	9
						Outco_3	192.168.100.23	CV	10
						Outco_4	192.168.100.24	CV	11
						Outco_5	192.168.100.25	CV	12
						Outco_6	192.168.100.26	CV	13
						Outco_7	192.168.100.27	CV	14
						Outco_8	192.168.100.28	CV	15
						Outco_9	192.168.100.29	CV	16
						DV1	192.168.100.241	CV	17
						DV1_b	192.168.100.242	CV	18

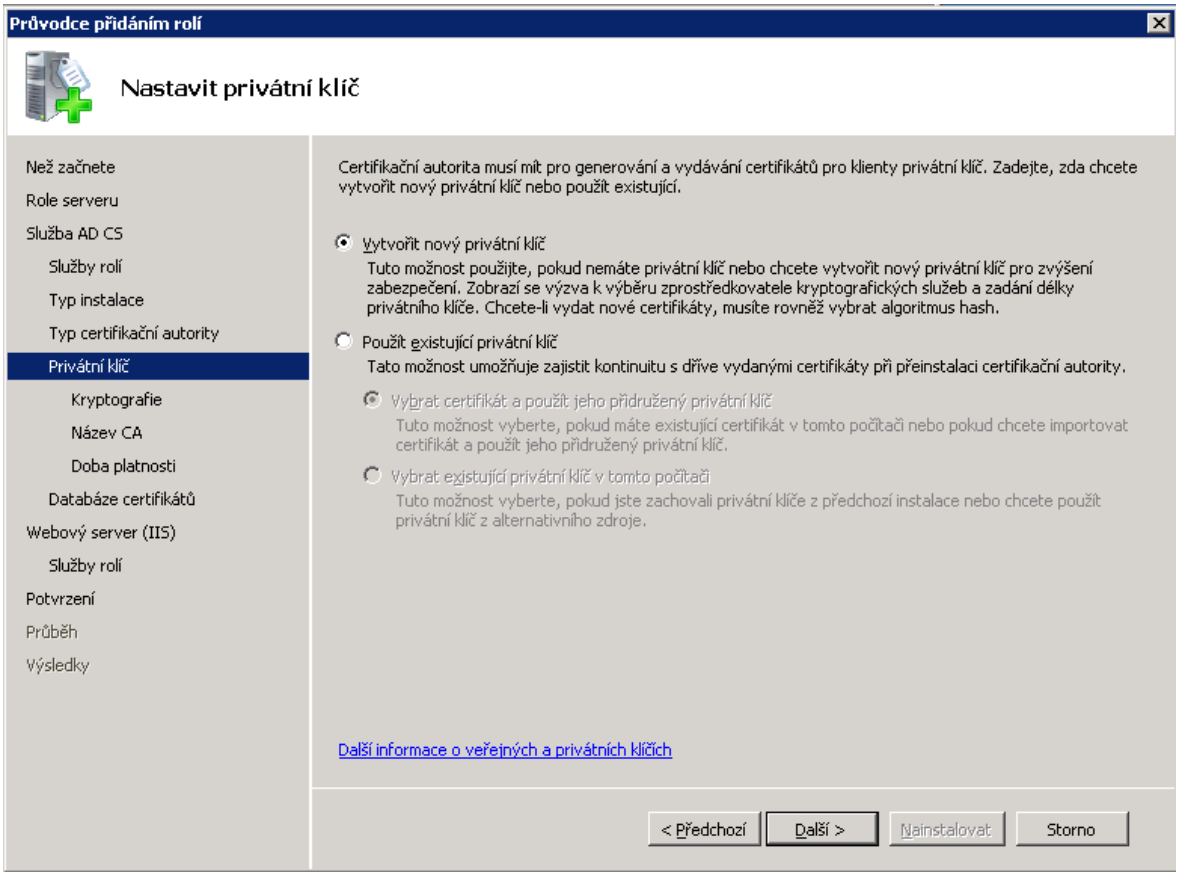
PŘÍLOHA P II: POSTUP INSTALACE CERTIFIKAČNÍ AUTORITY

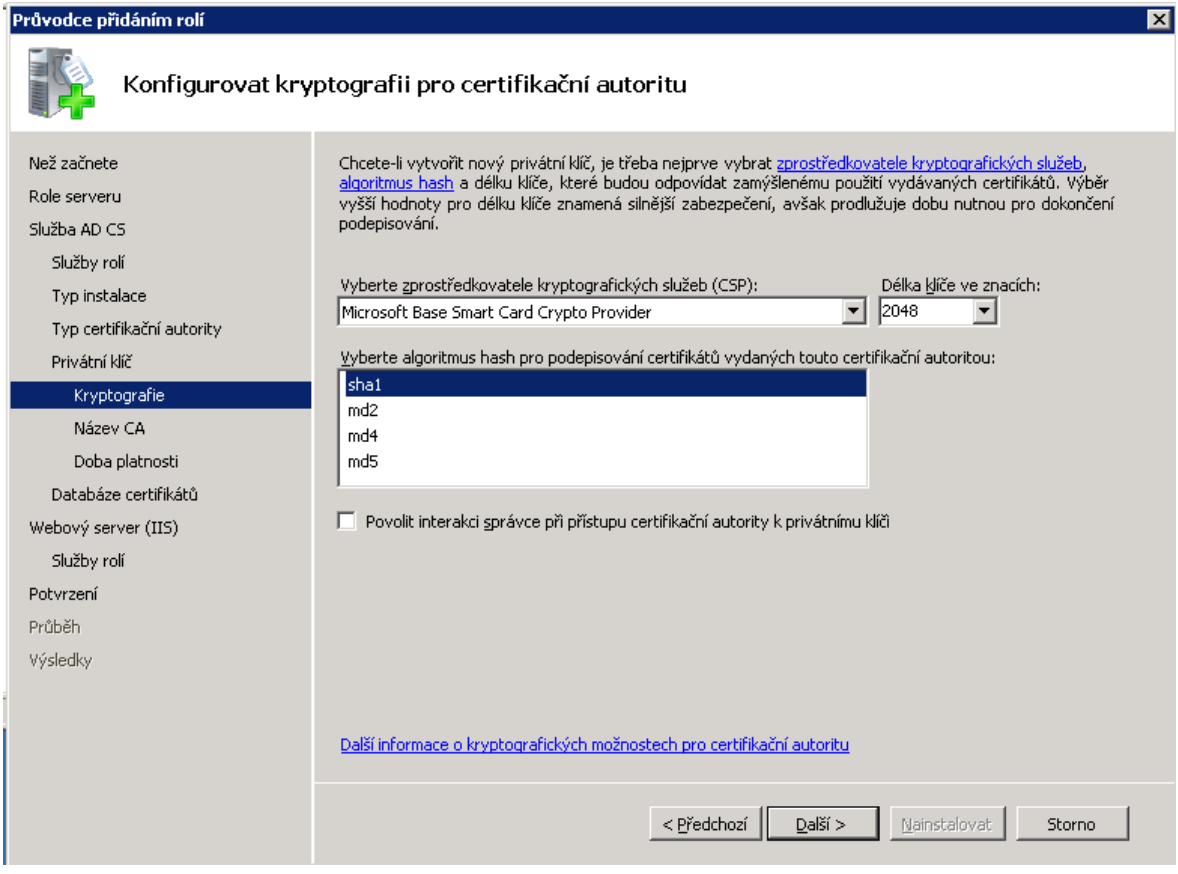


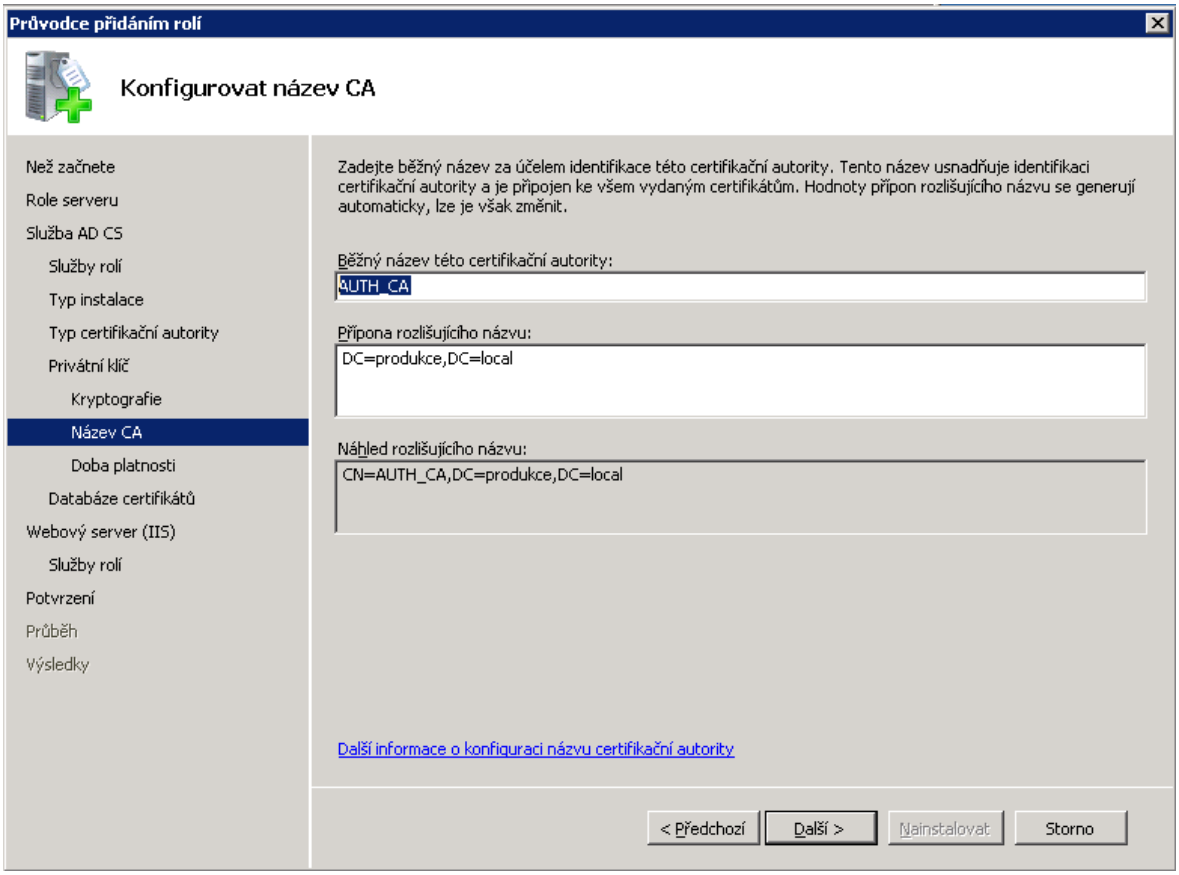


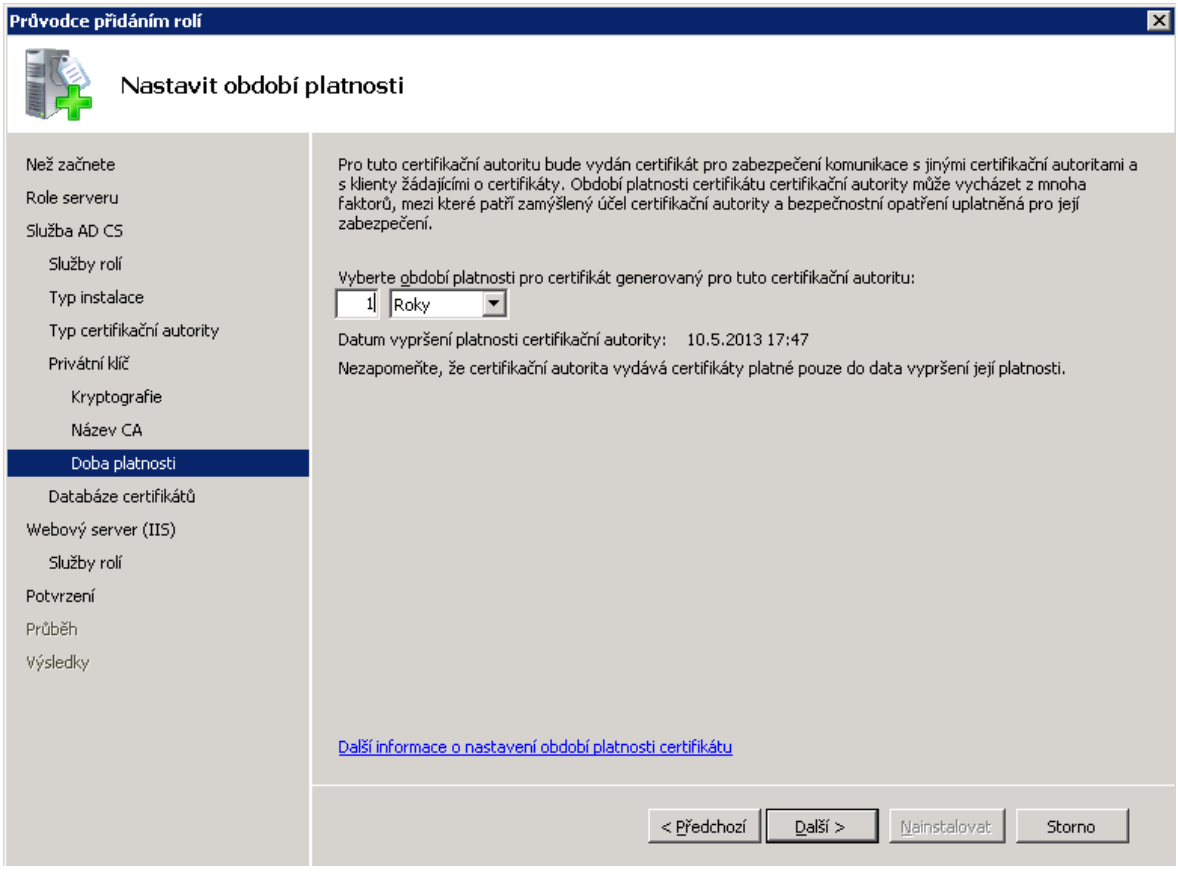

Průvodce přidáním rolí
Zadat typ instalace
Než začnete
Role serveru
Služba AD CS
Služby rolí
Typ instalace
Typ certifikační autority
Privátní klíč
Kryptografie
Název CA
Doba platnosti
Databáze certifikátů
Webový server (IIS)
Služby rolí
Potvrzení
Průběh
Výsledky
Certifikační autority mohou pro zjednodušení správy a vydávání certifikátů používat data adresářové služby. Zadejte, zda chcete nastavit podnikovou anebo samostatnou certifikační autoritu.
Rozlehlá síť
Tuto možnost vyberte, pokud je tato certifikační autorita členem domény a může k vydávání a správě certifikátů používat adresářovou službu.
Samostatná
Tuto možnost vyberte, pokud tato certifikační autorita pro vydávání a správu certifikátů nepoužívá data adresářové služby. Samostatná certifikační autorita může být členem domény.
Další informace o rozdílech mezi rozlehlou sítí a samostatným nastavením
< Předchozí
Další >
Nainstalovat
Storno

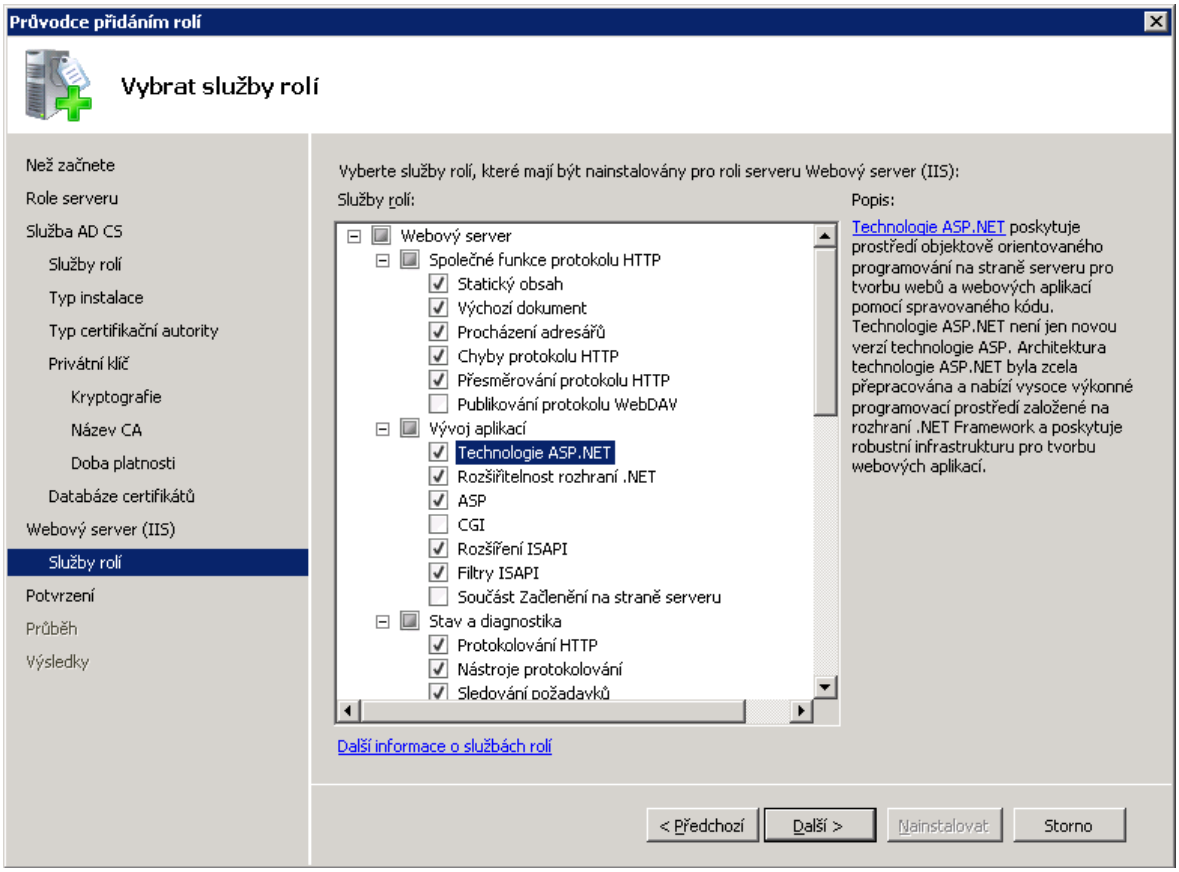

Průvodce přidáním rolí
Určit typ CA
Než začnete
Role serveru
Služba AD CS
Služby rolí
Typ instalace
Typ certifikační autority
Privátní klíč
Kryptografie
Název CA
Doba platnosti
Databáze certifikátů
Webový server (IIS)
Služby rolí
Potvrzení
Průběh
Výsledky
Můžete konfigurovat kombinaci kořenové a podřízené certifikační autority na vytváření hierarchické infrastruktury veřejných klíčů. Kořenová certifikační autorita je certifikační autorita, která vydává vlastní certifikát podepsaný svým držitelem. Podřízená certifikační autorita tento certifikát obdrží od jiné certifikační autority. Zadejte, zda chcete nastavit kořenovou nebo podřízenou certifikační autoritu.
Kořenová certifikační autorita
Tuto možnost vyberte, pokud instalujete první a jedinou certifikační autoritu v infrastruktuře veřejných klíčů.
Podřízená certifikační autorita
Tuto možnost vyberte, pokud certifikační autorita získá svůj certifikát z jiné certifikační autority, která se nachází výše v infrastruktuře veřejných klíčů.
Další informace o infrastruktuře veřejných klíčů (PKI)
< Předchozí
Další >
Nainstalovat
Storno

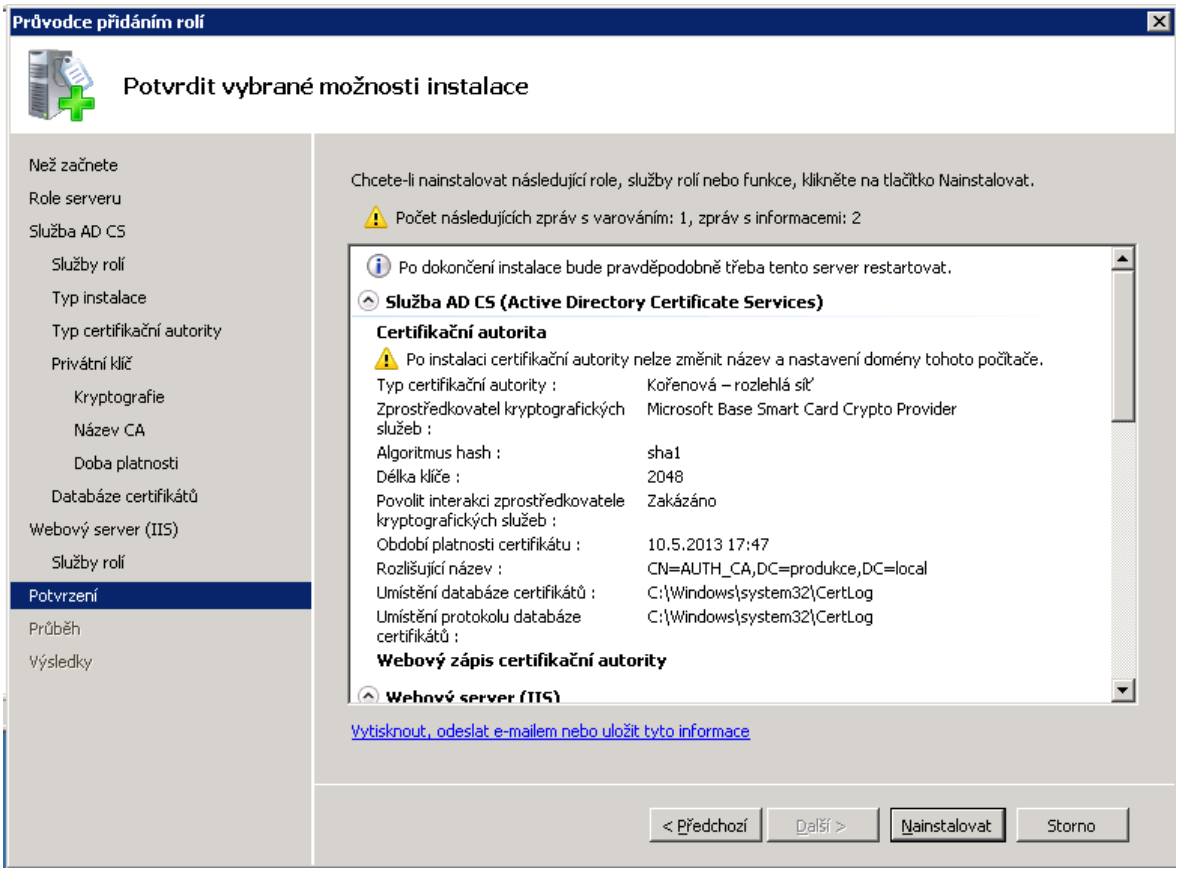

Průvodce přidáním rolí
Nastavit privátní klíč
Než začnete
Role serveru
Služba AD CS
Služby rolí
Typ instalace
Typ certifikační autority
Privátní klíč
Kryptografie
Název CA
Doba platnosti
Databáze certifikátů
Webový server (IIS)
Služby rolí
Potvrzení
Průběh
Výsledky
Certifikační autorita musí mít pro generování a vydávání certifikátů pro klienty privátní klíč. Zadejte, zda chcete vytvořit nový privátní klíč nebo použít existující.
Vytvořit nový privátní klíč
Tuto možnost použijte, pokud nemáte privátní klíč nebo chcete vytvořit nový privátní klíč pro zvýšení zabezpečení. Zobrazí se výzva k výběru zprostředkovatele kryptografických služeb a zadání délky privátního klíče. Chcete-li vydat nové certifikáty, musíte rovněž vybrat algoritmus hash.
Použít existující privátní klíč
Tato možnost umožňuje zajistit kontinuitu s dříve vydanými certifikáty při přeinstalaci certifikační autority.
Vybrat certifikát a použít jeho přidružený privátní klíč
Tuto možnost vyberte, pokud máte existující certifikát v tomto počítači nebo pokud chcete importovat certifikát a použít jeho přidružený privátní klíč.
Vybrat existující privátní klíč v tomto počítači
Tuto možnost vyberte, pokud jste zachovali privátní klíče z předchozí instalace nebo chcete použít privátní klíč z alternativního zdroje.
Další informace o veřejných a privátních klíčích
< Předchozí
Další >
Nainstalovat
Storno


Průvodce přidáním rolí
Konfigurovat kryptografii pro certifikační autoritu
Než začnete
Role serveru
Služba AD CS
Služby rolí
Typ instalace
Typ certifikační autority
Privátní klíč
Kryptografie
Název CA
Doba platnosti
Databáze certifikátů
Webový server (IIS)
Služby rolí
Potvrzení
Průběh
Výsledky
Chcete-li vytvořit nový privátní klíč, je třeba nejprve vybrat zprostředkovatele kryptografických služeb, algoritmus hash a délku klíče, které budou odpovídat zamýšlenému použití vydávaných certifikátů. Výběr vyšší hodnoty pro délku klíče znamená silnější zabezpečení, avšak prodlužuje dobu nutnou pro dokončení podepisování.
Vyberte zprostředkovatele kryptografických služeb (CSP):
Microsoft Base Smart Card Crypto Provider
Délka klíče ve znacích:
2048
Vyberte algoritmus hash pro podepisování certifikátů vydaných touto certifikační autoritou:
sha1
md2
md4
md5
Povolit interakci správce při přístupu certifikační autority k privátnímu klíči
Další informace o kryptografických možnostech pro certifikační autoritu
< Předchozí
Další >
Nainstalovat
Storno


Průvodce přidáním rolí
Konfigurovat název CA
Než začnete
Role serveru
Služba AD CS
Služby rolí
Typ instalace
Typ certifikační autority
Privátní klíč
Kryptografie
Název CA
Doba platnosti
Databáze certifikátů
Webový server (IIS)
Služby rolí
Potvrzení
Průběh
Výsledky
Zadejte běžný název za účelem identifikace této certifikační autority. Tento název usnadňuje identifikaci certifikační autority a je připojen ke všem vydaným certifikátům. Hodnoty přípon rozlišujícího názvu se generují automaticky, lze je však změnit.
Běžný název této certifikační autority:
AUTH_CA
Přípona rozlišujícího názvu:
DC=produkce,DC=local
Náhled rozlišujícího názvu:
CN=AUTH_CA,DC=produkce,DC=local
Další informace o konfiguraci názvu certifikační autority
< Předchozí
Další >
Nainstalovat
Storno


Průvodce přidáním rolí
Nastavit období platnosti
Než začnete
Role serveru
Služba AD CS
Služby rolí
Typ instalace
Typ certifikační autority
Privátní klíč
Kryptografie
Název CA
Doba platnosti
Databáze certifikátů
Webový server (IIS)
Služby rolí
Potvrzení
Průběh
Výsledky
Pro tuto certifikační autoritu bude vydán certifikát pro zabezpečení komunikace s jinými certifikačními autoritami a s klienty žádajícími o certifikáty. Období platnosti certifikátu certifikační autority může vycházet z mnoha faktorů, mezi které patří zamýšlený účel certifikační autority a bezpečnostní opatření uplatněná pro její zabezpečení.
Vyberte období platnosti pro certifikát generovaný pro tuto certifikační autoritu:
1
Roky
Datum vypršení platnosti certifikační autority: 10.5.2013 17:47
Nezapomeňte, že certifikační autorita vydává certifikáty platné pouze do data vypršení její platnosti.
Další informace o nastavení období platnosti certifikátu
< Předchozí
Další >
Nainstalovat
Storno


Průvodce přidáním rolí
Vybrat služby rolí
Než začnete
Role serveru
Služba AD CS
Služby rolí
Typ instalace
Typ certifikační autority
Privátní klíč
Kryptografie
Název CA
Doba platnosti
Databáze certifikátů
Webový server (IIS)
Služby rolí
Potvrzení
Průběh
Výsledky
Vyberte služby rolí, které mají být nainstalovány pro roli serveru Webový server (IIS):
Služby rolí:
Webový server
Společné funkce protokolu HTTP
Statický obsah
Výchozí dokument
Procházení adresářů
Chyby protokolu HTTP
Přesměrování protokolu HTTP
Publikování protokolu WebDAV
Vývoj aplikací
Technologie ASP.NET
Rozšiřitelnost rozhraní .NET
ASP
CGI
Rozšíření ISAPI
Filtry ISAPI
Součást Začlenění na straně serveru
Stav a diagnostika
Protokolování HTTP
Nástroje protokolování
Sledování požadavků
Popis:
Technologie ASP.NET poskytuje prostředí objektově orientovaného programování na straně serveru pro tvorbu webů a webových aplikací pomocí spravovaného kódu. Technologie ASP.NET není jen novou verzí technologie ASP. Architektura technologie ASP.NET byla zcela přepracována a nabízí vysoce výkonné programovací prostředí založené na rozhraní .NET Framework a poskytuje robustní infrastrukturu pro tvorbu webových aplikací.
Další informace o službách rolí
< Předchozí
Další >
Nainstalovat
Storno


Průvodce přidáním rolí
Potvrdit vybrané možnosti instalace
Než začnete
Role serveru
Služba AD CS
Služby rolí
Typ instalace
Typ certifikační autority
Privátní klíč
Kryptografie
Název CA
Doba platnosti
Databáze certifikátů
Webový server (IIS)
Služby rolí
Potvrzení
Průběh
Výsledky
Chcete-li nainstalovat následující role, služby rolí nebo funkce, klikněte na tlačítko Nainstalovat.
Počet následujících zpráv s varováním: 1, zpráv s informacemi: 2
Po dokončení instalace bude pravděpodobně třeba tento server restartovat.
Služba AD CS (Active Directory Certificate Services)
Certifikační autorita
Po instalaci certifikační autority nelze změnit název a nastavení domény tohoto počítače.
Typ certifikační autority : Kořenová – rozlehlá síť
Zprostředkovatel kryptografických služeb : Microsoft Base Smart Card Crypto Provider
Algoritmus hash : sha1
Délka klíče : 2048
Povolit interakci zprostředkovatele kryptografických služeb : Zakázáno
Období platnosti certifikátu : 10.5.2013 17:47
Rozlišující název : CN=AUTH_CA,DC=produkce,DC=local
Umístění databáze certifikátů : C:\Windows\system32\CertLog
Umístění protokolu databáze certifikátů : C:\Windows\system32\CertLog
Webový zápis certifikační autority
Webový server (IIS)
Vytisknout, odeslat e-mailem nebo uložit tyto informace
< Předchozí
Další >
Nainstalovat
Storno