



UNIVERZITET SINGIDUNUM

-MASTER STUDIJSKI PROGRAM-

SAVREMENE INFORMACIONO KOMUNIKACIONE TEHNOLOGIJE

**Informacione tehnologije i računarske mreže,
fizičko i virtualno okruženje datacentra**

Informacione tehnologije i računarske mreže, fizičko i virtualno okruženje datacentra

Mentor:

Prof. dr Mladen Veinović

Student:

Marko Šarac

TEMA: Informacione tehnologije i računarske mreže, fizičko i virtualno okruženje data centra

ABSTRAKT	6
UVOD.....	7
OPŠTI TIPOVI INFORMACIONE ARHITEKTURE.....	8
Okruženje centralnog računara	8
Okruženje PC računara.	8
Umreženo (distribuirano) okruženje.	8
OSNOVNI POJMOVI O MREŽAMA	9
Fizički medijumi prenosa.....	9
Uređaji za povezivanje	10
INFORMACIONI SISTEM	11
Odeljenski informacioni sistemi	12
Informacioni sistemi preduzeća	13
Međuorganizacioni sistemi.....	13
MREŽNI OPERATIVNI SISTEMI	13
Microsoft Windows.....	14
Novell NetWare	15
UNIX/Linux	15
Macintosh	16
IMPLEMENTIRANJE WINDOWS SERVERA 2003	16
ARHITEKTURA WINDOWS SERVERA 2003	19
Korisnički sloj.....	19
Sloj jezgra.....	20
DOMAIN CONTROLLER	22

ACTIVE DIRECTORY	23
GROUP POLICY	27
DNS (DOMAIN NAME SYSTEM).....	28
DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)	29
BEZBEDNOST.....	30
ANTIVIRUS PAKET PROGRAMA	32
ISA SERVER.....	33
DATACENTRI KAKVE SMO POZNAVALI DO DANAS	36
PROBLEMI FIZIČKOG DATACENTRA	37
MOGUĆA REŠENJA - REŠENJA KOJA NUDI VIRTUALIZACIJA	38
VMware	39
Hyper-V	41
Xen virtualizacija.....	44
PRIMENA REŠENJA DOBIJENIH VIRTUELIZACIJOM	47
ALL IN ONE DATACENTRI	51
OPORAVAK SISTEMA NAKON KATASTROFE	54
IMPLEMENTACIJA HIPER-V REŠENJA	56
POSTUPAK IMPLEMENTACIJE I VIRTUALIZACIJE POMOĆU HYPER-V HIPERVIZORA.....	60
Postupak instalacije i konfigurisanje	60
Proces kreiranja virtualne mašine	62
Rezultati testiranja	65
ZAKLJUČAK	73
LITERATURA	75
Internet izvori:	77

ABSTRAKT

Rad na temu Informacione tehnologije i računarske mreže, fizičko i virtualno okruženje data centra pisao sam sa ciljem da predstavi sve aspekte sa kojima se sistem administratori mreže i informacionih sistema sreću pri izgradnji i svakodnevnom održavanju računarskih mreža i informacionih sistema. Takođe sam želeo da predstavim i testiram neke od novih koncepata koje donosi virtualizacija datacentra. U radu su opisane hardverske komponente koje se koriste za izgradnju ovakvih sistema ali poseban osvrt u prvom delu rada dat je na mrežne operative sisteme sa naglaskom na Windows Server 2003 i njegovo implementiranje u mrežu. U drugom delu rada predstavljen je koncept virtualizacije, predstavljana su vodeća rešenja virtualizacije, i testirano i praktično primenjeno Microsoft Hyper-V rešenje koje sa sobom nosi Windows Server 2008. Kroz prvi deo rada sam ukazao na osnovne prednosti koje Windows Server 2003 nudi u odnosu na druge mrežne operative sisteme, dok je u drugom delu rada predstavljen i Windows Server 2008 sa naglaskom na Hyper-V tehnologiju. U radu su takođe predstavljani i rezultati i poređenja fizičkih i virtualnih radnih stanica i servera.

UVOD

Informaciona infrastruktura se sastoji od fizičkih uređaja, usluga i procedura koji podržavaju sve računarske resurse u jednoj organizaciji. Postoji pet glavnih komponenti infrastrukture: (1) računarski hardver, (2) razvojni softver, (3) mrežna i komunikaciona sredstva (uključujući Internet i intranetove), (4) baze podataka i (5) osoblje koje upravlja informacijama. Infrastrukture obuhvataju ove resurse, kao i njihovo objedinjavanje, održavanje i upravljanje njime.

Predmet analize su informacione tehnologije i računarske mreže, sigurnosna i bezbednosna rešenja, implementiranje Windows Servera 2003. Polazeći od teorijskih sugestija (iste uvodimo u koncept analize) tragamo za konkretnim rešenjima koja se odnose na procese uvođenja i implementiranja Windows Servera 2003. Predmet analize opremamo sa savremenim tehnološkim dostignućima koja omogućavaju realizaciju i gradnju savremene računarske mreže i informacionih sistema.

Cilj naše analize je da na naučno validan način opišemo oblike i procese izgradnje savremene računarske mreže zasnovane na Windows Serveru 2003. Pored ovog naučnog cilja rezultati naše analize treba da posluže rešavanju konkretnih problema.

U istraživanje polazimo sa sledećom hipotetičkom tvrdnjom zaštita i izgradnja računarskih mreža determinisana je primenom tehničko-tehnoloških dostignuća, odnosno primenom savremenih informacionih tehnologija u konkretnoj organizaciji. Našu generalnu hipotetičku tvrdnju operacionalizujemo preko i pomoću sledećih posebnih i pojedinačnih hipoteza:

- Informacione tehnologije i računarske mreže, kao i sigurnosna i bezbednosna rešenja determinisana su znanjem eksperata u oblasti primene informacionog sistema organizacije;
- na proces implementiranja informacionih tehnologija i računarskih mreža deluje poslovna kultura, a posebno bezbednosna kultura organizacije;
- Izgradnja informacionih sistema i računarskih mreža kao i zaštita podataka i informacija determinisana je pravnim normama organizacije;
- Mrežna arhitektura kao i sigurnosno/bezbednosna rešenja organizacije determinisana su položajem organizacije na tržištu;
- Informacioni sistem i računarska mreža organizacije determinisani su specifičnošću proizvoda (roba, usluga i ideja) organizacije;
- Implementacija Windows Servera 2003 determinisana je bezbednosnom politikom organizacije u kojoj se implementira;

OPŠTI TIPOVI INFORMACIONE ARHITEKTURE

Jedan od načina da se klasifikuje informaciona arhitektura je prema ulozi hardvera. Moguće je razlikovati dva ekstremna slučaja: okruženje centralnog računara i okruženje personalnog računara. Kombinacija ova dva slučaja kreira treći tip arhitekture, distribuirano ili mrežno okruženje.

Okruženje centralnog računara. U okruženju centralnog računara obrada se vrši u centralnom računaru. Korisnici rade na pasivnim (ili „glupim“) terminalima, koji se koriste za unošenje ili promenu podataka i pristup informacijama sa centralnog računara. Ovo je bila dominantna arhitektura sve do sredine 80-ih prošlog veka. Danas veoma malo organizacija koriste samo ovaj tip arhitekture. Njen naslednik je arhitektura gde se personalni računari koriste kao pametni terminali. Pametni terminal (ili inteligentni terminal) ne samo da sadrži tastaturu i ekran, već i disk drajv, kako bi mogao da izvrši ograničene zadatke obrade kada ne komunicira direktno sa centralnim računarom. Ipak, suština sistema je glavni računar sa svojim moćnim sposobnostima skladištenja i računanja. Mrežni računari (engl. Network Computers - NC), koji su uvedeni 1997. godine, redefinišu ulogu centralizovanog računarskog okruženja.

Okruženje PC računara. Kod PC konfiguracije, hardversku informacionu arhitekturu čine samo lični (PC) računari. Oni mogu biti nezavisni jedan od drugog, ali i povezani preko elektronskih mreža. Ova arhitektura je uobičajena za mnoge male i srednje organizacije.

Umreženo (distribuirano) okruženje. Distribuirana obrada deli posao obrade između dva ili više računara. Računari koji u tome učestvuju mogu biti ili svi centralni, ili srednjeg obima ili mikro, ili, u većini slučajeva, kombinacija ovih mogućnosti. Mogu biti na jednoj lokaciji, ili na više. Saradnička obrada je vrsta distribuirane obrade u kojoj dva ili više geografski odvojenih računara timski rade na konkretnom zadatku. Druga važna konfiguracija distribuirane obrade je model klijent/server, gde nekoliko računara deli resurse i može da komunicira sa drugim računarima preko LAN mreža. Kada distribuirani sistem pokrije celu organizaciju, smatra se da je to sistem celog preduzeća, a njegovi delovi često su povezani intranetom. Distribuirano okruženje centralnog računara i PC računara je veoma fleksibilno i obično ga koristi većina srednjih i velikih organizacija.

Zahvaljujući komunikacionim mrežama i naročito Internetu i intranetovima, mrežno računarstvo postaje dominantna arhitektura većine organizacija. Ova arhitektura omogućava unutrašnju i interorganizacionu saradnju u računarstvu;

dostupnost ogromnih količina podataka, informacija i znanja; i veliku efikasnost u upotrebi računarskih resursa.

OSNOVNI POJMOVI O MREŽAMA

Osnovni razlog za povezivanje računara u mrežu jeste deljenje podataka i resursa. Pojam mreža u svetu računara označava grupu od dva ili više međusobno povezanih računara koji mogu deliti resurse poput podataka, štampača, internet veze, aplikacija ili bilo kakve kombinacije takvih resursa. Mreže mogu biti veoma jednostavne, poput manje grupe računara koje dele podatke, ali i veoma složene, kada pokrivaju velika geografska područja. Razlike između računarskih mreža mogu biti velike, kao i između tehnologija koje su u njima primenjene, tako da je neophodno povezivanje osnova umrežavanja i načina zajedničkog rada mrežnih komponenti.

Lokalna računarska mreža (LAN, Local Area Network) je, po definiciji, ograničena na manji prostor (obično je to kancelarija) nekada cela firma funkcioniše u jednoj LAN mreži. Obično je veća LAN mreža podeljena na više manjih celina uglavnom zbog administrativnih poslova koji su umnogome olakšani deljenjem na logičke celine. Regionalna mreža (WAN, Wide Area Network) označava bilo koju računarsku mrežu koja prevazilazi granice nekog grada, regiona ili države.

U ovom radu biće detaljno objašnjeno korišćenje i segmentiranje veće lokalne mreže (LAN) sa konkretnim primerima i posebnim osvrtom na postavljanje i konfigurisanje Microsoft Windows 2003 servera za namene deljenja fajlova, interneta i autentifikacije korisnika.

Fizički medijumi prenosa

Pored toga što danas postoji nekoliko vrsta bežičnih mreža, poput onih koje koriste radio frekvencije ili infracrvene zrake, većina instaliranih LAN mreža koristi neku vrstu kabla. U praksi se koriste tri tipa kabla: Koaksijalni, Usporedne parice (UTP) i optički.

Koaksijalni kabl sadrži centralni provodnik koji je izrađen od bakra, preko koga se nalazi plastični omotač, sa dodatnim oklopom u vidu pletenice preko omotača, preko metalnog oklopa je postavljen plastični omotač PVC. Uz koaksijalne kablove se koriste BNC konektori preko kojih se stanice povezuju u mrežu. Koaksijalne BNC mreže se gotovo više ne koriste zato što su i po brzini koja je bila ograničena na 10Mbps i po funkcionalnosti prevaziđene modernijim mrežama tipa usporednih parica.

Kabl u vidu usporednih parica sastoji se iz većeg broja međusobno izolovanih provodnika koji su zajedno upredeni u parice, takođe postoje varijante sa metalnim oklopom. UTP kablovi koriste RJ45 tip konektora koji radi sa četiri parice tj. sa osam

provodnika. Ovi kablovi se danas najčešće koriste zato što su jeftiniji u odnosu na druge tipove kablova, lakši su za rukovanje i omogućavaju brzine prenosa do 1Gbps što je bilo ne zamislivo do pre 10 godina.

Optički kabl prenosi digitalne signale pomoću svetlosnih impulsa, tako da je potpuno otporan na elektromagnetne i radio smetnje. Svetlo se kroz kabl prenosi kroz stakleno ili plastično jezgro, oko njega se nalazi plastični omotač a iznad se nalazi savitljiva plastična košuljica koja je najčešće obmotana dodatnim oklopom i slojem PVCa. Optički kablovi prenose podatke brzinom do 10Gbps i do razdaljine od 40km što ih čini najboljim medijumom za prenos podataka.

Uređaji za povezivanje

Pored medijuma za prenos podataka u računarskim mrežama takođe se koriste i uređaji za povezivanje u mrežu:

- Mrežna kartica (NIC, Network Interface Card)
- Čvorište (hub)
- Komutator (switch)
- Most (bridge)
- Ruter
- Mrežni prolaz (gateway)

Mrežna kartica predstavlja karticu koja se u poslednjim generacijama računara gotovo kao pravilo nalazi na samoj matičnoj ploči omogućuje povezivanje računara u mrežu, ona obezbeđuje fizički spoj sa prenosnim medijumom na mreži. Čvorište (hub) je uređaj koji se više gotovo ne koristi u modernim računarskim mrežama zamenjen je komutatorom (switch), oba imaju sličnu ulogu da povezuju sve segmente mreže ali različit način rada. Dok čvorište šalje signal na sve portove, komutator prepoznaje sadržaj paketa i uvažava odredišnu MAC adresu dolaznog paketa kao i porta preko koga je primljen, pa će poslati signal samo na onaj port koji odgovara odredištu. Most predstavlja uređaj koji povezuje dva slična mrežna segmenta, postavlja se u mrežu prvenstveno radi povezivanja dva segmenta i razdvajanje saobraćaja na segmente u opterećenim mrežama. Ruter je uređaj koji povezuje veći broj segmenata u jedinstvenu mrežu, može donositi inteligentne odluke o tome kako na najbolji način da usmeri podatke ka odredištu, na osnovu podataka o performansama mreže. U poslednje vreme ruteri u sebi imaju i funkciju mrežnog prolaza (gateway).

Pored pomenutih u računarskim mrežama se sve češće sreću i uređaji poput modema (POTS, DSL, Kablovski), ISDN terminalnih adaptera, bežičnih pristupnih tačaka (WAP, wireless access point) kao i mrežnih barijera (Firewall).

INFORMACIONI SISTEM

Informacioni sistem (IS) prikuplja, obrađuje, skladišti, analizira i šalje informacije za specifičnu namenu. Kao bilo koji drugi sistem, informacioni sistem uključuje ulaze (podaci, instrukcije) i izlaze (izveštaji, kalkulacije). On obrađuje ulaze i stvara izlaze koji se šalju korisniku ili drugim sistemima. Računarski zasnovan informacioni sistem (eng. computer-based information system - CBIS) je informacioni sistem koji koristi računarsku tehnologiju da realizuje neki, ili sve planirane zadatke. Takav sistem može uključiti personalni računar i softver, ili nekoliko hiljada računara različitih veličina, stotine printera, plotera i drugih uređaja, kao i komunikacione mreže i baze podataka. U većini slučajeva informacioni sistem takođe uključuje ljude. Osnovne komponente informacionih sistema su:

- Hardver je skup tehničkih sredstava kao što su procesor, monitor, tastatura i štampač. Zajedno, oni prihvataju podatke i informacije, obrađuju i prikazuju ih.
- Softver je skup programa koji omogućavaju hardveru da obrađuje podatke.
- Baza podataka je skup povezanih fajlova, tabela, relacija, itd. Ona sadrži podatke i veze između njih.
- Mreža je sistem veza koji dozvoljava da različiti računari zajednički koriste resurse.
- Procedure su skup instrukcija o tome kako da se koriste navedene komponente da bi se informacija obradila i generisao željeni izlaz.
- Ljudi su oni pojedinci koji rade sa sistemom ili koriste izlazne informacije.

Karakteristike informacionih sistema dvadeset prvog veka:

- Više različitih informacionih sistema može postojati u jednoj organizaciji.
- Skup od nekoliko informacionih sistema se takođe smatra informacionim sistemom. Većina ovih sistema su međusobno povezani
- Informacioni sistemi su povezani pomoću elektronskih mreža. Ako je cela firma umrežena i ljudi mogu da komuniciraju jedni sa drugima i pristupe informacijama širom organizacije, onda se taj aranžman smatra sistemom cele firme
- Međuorganizacioni informacioni sistemi uključuju protok informacija kroz dve ili više organizacija, i koriste se prevashodno u aplikacijama elektronskog poslovanja
- Sistem celog preduzeća je međuorganizacioni informacioni sistem sastavljen od velikih i malih računara i hardvera, povezanih različitim tipovima mreža (kao što su virtuelne privatne mreže, mreže dodatih vrednosti, intranetovi i

Internet). Takođe uključuje softver, baze podataka, podatke, procedure i, naravno, ljude.

Ove karakteristike ukazuju na kompleksnost organizovanja i upravljanja informacionim sistemima. Zato je potrebno definisati glavne pojmove i organizovati ih na neki logičan način. Informacioni sistemi se grade da ostvare nekoliko ciljeva. Jedan od primarnih ciljeva je da se podaci na ekonomičan način obrade i transformišu u informaciju ili znanje.

Informacioni sistemi se mogu klasifikovati na nekoliko načina: prema organizacionim nivoima, glavnim funkcionalnim oblastima, podršci koju pružaju i IS arhitekturi. Bez obzira na to kako se klasifikuju, struktura ovih sistema je ista: naime, svaki sadrži hardver, softver, podatke, procedure i ljude.

Organizacije su sastavljene od komponenti kao što su odeljenja, timovi i radne jedinice. Na primer, većina organizacija ima personalno odeljenje, finansijsko i računovodstveno odeljenje i možda jedinicu za odnose sa javnošću. Ove komponente čine organizaciju koja može biti odgovorna višem organizacionom nivou, kao što je odsek, ili sedište u tradicionalnoj hijerarhijskoj strukturi. Mada se neke organizacije reorganizuju u nove strukture, kao što su one bazirane na međufunkcionalnim timovima, danas velika većina organizacija još uvek ima tradicionalnu hijerarhijsku strukturu.

Jedan od načina klasifikovanja informacionih sistema je po organizacionim strukturnim linijama. Tako možemo naći informacione sisteme izgrađene za sedišta firmi, za odseke, odeljenja, za operativne jedinice, pa čak i za pojedinačne radnike. Takvi sistemi mogu da budu samostalni ili međusobno povezani.

Tipični informacioni sistemi koji prate organizacionu strukturu su: odeljenski, za celu firmu i međuorganizacioni. Ovi sistemi su organizovani u hijerarhijski sistem u kome se svaki sistem višeg nivoa sastoji od više sistema nižeg nivoa koji mu prethode.

Odeljenski informacioni sistemi. Često organizacija koristi nekoliko aplikacionih programa u jednoj funkcionalnoj oblasti ili odeljenju. Aplikacioni program je program projektovan da izvrši konkretnu funkciju direktno za korisnika ili, u nekim slučajevima, za drugi aplikacioni program. Na primer, u upravljanju ljudskim resursima moguće je koristiti jedan program za praćenje ljudi koji su konkurisali za posao i drugi za nadgledanje prometa zaposlenih. Neke aplikacije mogu biti potpuno nezavisne jedne od drugih, dok su druge međusobno povezane. Skup aplikacionih programa u oblasti ljudskih resursa zove se informacioni sistem ljudskih resursa. To jest, on se smatra običnim odeljenskim informacionim sistemom, iako je sastavljen od nekoliko aplikacionih podsistema. Na različitim korporativnim lokacijama u velikim organizacijama, može postojati više odeljenja u okviru iste funkcionalne oblasti. Na primer, odeljenje ljudskih resursa moglo bi da postoji na nivou korporacije, ali i u

svakom odseku. Projektanti IS-a tada imaju dve mogućnosti: oni mogu da projektuju informacijski sistem odseka koji obuhvata podsistem ljudskih resursa, ili mogu da projektuju centralizovani sistem ljudskih resursa za celu korporaciju.

Informacioni sistemi preduzeća. Dok je odeljenski IS obično povezan sa funkcionalnom oblašću, zbir svih odeljenskih aplikacija u kombinaciji sa aplikacijama drugih funkcija obuhvata informacijski sistem cele firme. Jedna od najpopularnijih aplikacija preduzeća je planiranje resursa preduzeća (engl. Enterprise Resource Planning - ERP). ERP sistemi su sistemi koji dozvoljavaju kompanijama da zamene svoje postojeće sisteme jednim, objedinjenim sistemom. Ovaj proces obuhvata planiranje resursa i upravljanje resursima celog preduzeća. ERP sistem predstavlja novi model korišćenja računara na nivou celog preduzeća.

Međuorganizacioni sistemi. Neki informacijski sistemi povezuju više organizacija. Na primer, svetski avionski sistem rezervacija je sastavljen od više sistema koji pripadaju različitim aviokompanijama. Međuorganizacijski informacijski sistemi (engl. Interorganizational Information Systems - IOS) su sistemi koji povezuju dve ili više organizacija. Takvi sistemi su zajednički za poslovne partnere i široko se koriste za elektronsku trgovinu, često preko ektraneta. Specijalni IOS je internacionalna ili multinacionalna korporacija, čija su informatička postrojenja locirana u dve ili više zemalja. Međuorganizacioni informacijski sistemi igraju veliku ulogu u elektronskoj trgovini, kao i kod podrške u upravljanju lancem snabdevanja.

MREŽNI OPERATIVNI SISTEMI

Svaka mreža danas poseduje neki oblik softvera za upravljanje mrežnim resursima. Taj softver tj. Mrežni operativni sistem (NOS, network operating system) izvršava se na snažnim računarima i predstavlja jednu od najbitnijih komponenti svake mreže. Četiri najpopularnija mrežna operativna sistema predstavljaju:

- Microsoft Windows
- Novell NetWare
- UNIX/Linux
- Macintosh

NetWare, koji je razvijen u kompaniji Novell, predstavlja prvi operativni sistem koji je široko prihvaćen na PC tržištu. Windows, i pored činjenice da ga je Microsoft uveo tek 1993. godine, ipak zauzima znatan deo tržišta serverskih platformi, prvenstveno

zahvaljujući jednostavnosti upotrebe. UNIX, i pored toga što je najstariji mrežni operativni sistem, tek počinje da stiče popularnost kod PC korisnika, prvenstveno preko verzija koje su namenjene PC računarima, kao što je Linux. Popularnost raste delimično i zbog Interneta koji se zasniva na UNIX standardima i protokolima. Četvrti mrežni operativni sistem koji se danas koristi zauzima znatno manji deo mrežnog tržišta i kristi se uz Mac OS naziv mu je AppleShare IP.

Microsoft Windows

Windows 2003 server, sa istim grafičkim interfejsom kao i ostale Windows verzije i jednostavnom administracijom serverske konzole, danas svakako predstavlja najpopularniji NOS u upotrebi. Microsoft se na tržište NOSa probio sa Windows NT 3.51 operativnim sistemom koji je bio stabilan i lak za korišćenje. Microsoft je pružio jaku marketinšku podršku ovom proizvodu, ubrzo za tom verzijom su se pojavili Windows 2000 server a zatim i 2003 server, čime je Windows platforma postala dominantna na NOS tržištu.

Nezavisni proizvođači stalno izbacuju na hiljade različitih softverskih naslova za Windows. Broj mrežnih programa nezavisnih proizvođača za Windows danas znatno nadmašuje broj pisanih za NetWare ili Linux. Jedan od razloga za rasprostranjenost softvera za Windows Server leži u činjenici da programeri mogu kreirati takve programe u istom razvojnem okruženju u kojima pišu i obične Windows programe, Microsoft obezbeđuje veliku količinu koda programerima uz minimalnu ili nikakvu nadoknadu.

Jednu od ozbiljnih mana Windows 2003 servera predstavljaju njegovi sistemi zaštite. Naime iste one osobine koje Windows Server čine jednostavnim za upotrebu predstavljaju i najranjivije karakteristike kada su u pitanju napadi hakera. Većina zakrpa koje Microsoft izbacuje za Windows Server vezana je upravo za sistem zaštite. Takođe, u stalnoj trci za ispunjenjem obećanih rokova Windows se obično distribuira pre nego što je stvarno spreman, da bi se ispravke i zakrpe tek kasnije slale na tržište. Takva žurba stvara mogućnost za pojavu rupa u sistemu zaštite koje ostaju nerešene sve dok ne budu otkrivene. Takvi propusti su bili uzrok velikog broja propusta u zaštiti tokom proteklih godina. Međutim ne može se reći da Windows Server ne može postati sigurna platforma sa dobri mrežnim barijerama i sa pripremljenim zakrpama Windows može postati siguran kao i bilo koja druga NOS platforma o čemu će posebno biti reči u ovom radu.

Novell NetWare

NetWare predstavlja jedan od najmoćnijih mrežnih operativnih sistema na tržištu, naročito je popularan u velikim mrežama (više od 20 servera), zahvaljujući karakteristikama poput centralizovane administracije svih korisnika i njihovih parametara. Predstavlja najfleksibilniji NOS koji može komunicirati sa praktično svakim računarskim okruženjem uključujući: Windows 95/98/ME/NT/2000/XP, Mac OS, VMS, OS/400, UNIX, OS/2. Kada neki od navedenih operativnih sistema pokušava da ostvari komunikaciju se NetWare severom, server će se pojaviti kao pripadnik tog tipa mreže, ovo je zato što je Novell razvio klijentski softver koji obezbeđuje rad se NetWare-om velikom broju klijentskih operativnih sistema.

NetWare je svakako najzaštićeniji mrežni operativni sistem. On koristi šifrovanje na bazi javnog ključa tokom prijave na sistem (lozinke se nikada ne šalju između klijenta i servera u obliku otvorenog teksta). Pored toga, korisnik ne može prići lokalnim datotekama bez prijave sa odgovarajućim klijentom. NetWare je jedini NOS koji ima NSA (National Security Agency) sertifikat u obliku C2 Red Book, što znači da je sistem zaštite dovoljan i za upotrebu u vladi SAD-a.

Aplikativna podrška je jedna od osnovnih nedostataka NetWare sistema. NetWare je isključivo namenjen serverskim platformama. Novell smatra da serveri treba da obezbede isključivo mrežne servise, ali ne i da rade sa desktop aplikacijama.

UNIX/Linux

Predstavlja jedan od najstarijih mrežnih operativnih sistema. Karakteristično je da postoji veliki broj verzija i mada je osnovna arhitektura svih verzija ista postoje fini detalji koji jednu verziju čine bolju u praksi u odnosu na drugu. Sve UNIX verzije poseduju kernel, koji sačinjava osnovu čitavog operativnog sistema. Kernel komunicira sa različitim tipovima korisničkog interfejsa i može da pristupa hardveru. Linux je jedna od verzija UNIX-a koja danas zaokuplja najviše pažnje. Osnovna karakteristika Linuxa je jednostavnost upotrebe. Razvio ga je Linus Torvald sa Univerziteta u Helsinkiju, Finska. Najveći broj Linux distribucija je besplatan, većina uključuje skup korisničkih aplikacija poput programa za obradu teksta, sistem grafičkog interfejsa i kompajlera izvornog koda.

UNIX serveri prvenstveno koriste standardne Internet protokole, kao što su TPC/IP, FTP, HTTP..., zbog toga potencijalni klijenti za ove servere može biti svaki klijent koji se može konfigurisati sa TCP/IP protokolom i web čitačem.

Većina verzija UNIX-a postoji već duže vreme na tržištu, tako da je dobar deo problema u sistemu zaštite već otkriven i greške otklonjene. I pored toga se stalno javljaju novi sigurnosni problemi, široka baza korisnika obezbeđuje njihovo brzo i

lako otklanjanje; većina korisnika sama uklanja uočene slabosti, zato što prosečan UNIX administrator izuzetno dobro izverziran za rešavanje sopstvenih problema.

Macintosh

Macintosh interfejs se smatra najjednostavnijim za upotrebu među svim raspoloživim grafičkim korisničkim interfejsima. Mac OS je kao serverska platforma uglavnom ograničen kada je reč o podršci klijentima. Mac OS X server funkcioniše savršeno u ulozi Internet servera, zahvaljujući tome što jezgro Mac OS X ustvari čini UNIX.

Mac OS X poseduje pouzdan sistem zaštite. Većina servisa koji mogu biti predmet hakerskog napada je isključena, što Mac u startu čini zaštićenijim od ostalih OS. Aplikativna podrška se svodi na Mac aplikacije koje su kompatibilne i sa aplikacijama pisane za starije verzije ovog OSa.

IMPLEMENTIRANJE WINDOWS SERVERA 2003

U nastavku rada predstaviću neke od osnovnih opcija koje Windows Server 2003 nudi, kao i da objasnim razloge masovne upotrebe Windows 2003 servera u malim i srednjim računarskim mrežama i preduzećima. Kao jedan od najbitnijih faktora u preduzećima koja koriste računare javlja se pitanje raspoloživosti sistema. U kontekstu informacionih sistema raspoloživost se odnosi na napore koje činimo da informacioni sistemi i usluge koje oni pružaju budu neprekidno na raspolaganju korisnicima i drugim procesima. Obično se govori o raspoloživosti tipa „24 sata, 7 dana u nedelji“, što bi, kada bi bilo moguće, bila stoprocentna raspoloživost.

Raspoloživost je veoma važna za kompanije koje sa svojim klijentima imaju ugovore o nivou kvaliteta usluga. Nivo usluga (Service Level, SL) u informacionoj tehnologiji označava raspoloživost računarskih sistema koji pružaju usluge za koje klijenti plaćaju svojim dobavljačima. SL se više ne odnosi samo na sisteme takvih dobavljača niti na odnose dobavljači-klijenti. Svima koji zavise od računarskog sistema, veoma je važno da on bude na raspolaganju „sve vreme“. Firmama koje se bave elektronskom trgovinom, a čija će zavisnost od Windows Servera 2003 postajati sve veća, posebno je važna stalna raspoloživost Internet usluga. Ako se prekine veza s vašim serverom, lako je izračunati gubitke. Prekidanje veze između servera i Interneta isto je kao zatvaranje vrata prodavnice, što vaše kupce odmah preusmerava ka konkurenciji. Elektronske prodavnice ne mogu sebi da priušte taj luksuz.

Glavni cilj i obaveza svakog administratora servera jeste da dobro upozna svoj posao i da istrajno obezbeđuje neprekidnu visoku raspoloživost servera i usluga. Sve usluge i komponente Windowsa 2003 trebalo bi staviti na spisak za procenu raspoloživosti ili na spisak za procenu rizika. Sledeća lista sadrži nekoliko oblasti kojima se Microsoft posvetio s namerom da obezbedi visoku raspoloživost:

- Sindrom odskočivog servera – restartovanje i ponovno podizanje sistema
- Grupisanje i redundansa servera – postavljanje servera u klaster grupe
- Redundansa kapaciteta za skladištenje podataka – RAID 1, 1-0, 5 - modovi
- Oporavljanje od katastrofe
- Bezbednost

Microsoft je u jezgru Windowsa 2003 znatno smanjio broj slučajeva u kojima je obavezno ponovno podizanje sistema, što važi i za nove usluge i pri rušenju postojećih aplikacija i usluga. Poboljšanje je naročito primetno u oblastima u kojima se unosi veliki broj izmena, kao što je konfiguracija mreže i sl. Na primer, odmah počinju da važe izmene statičkih IP adresa i nova podešavanja mrežnih kartica. Još uvek pos-toji veliki broj oblasti koje se mogu poboljšati. Dobar primer je instaliranje softvera (kao što su servisni paketi).

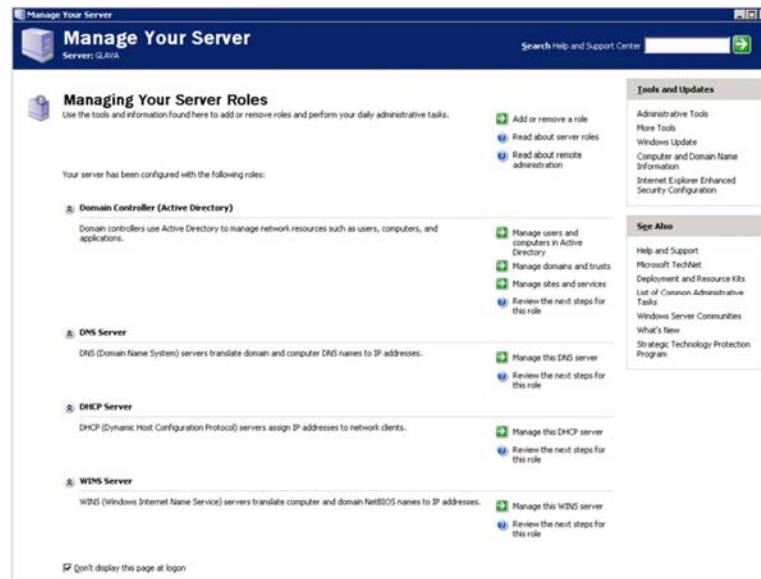
U Windows Server 2003 Enterprise ugrađene su i mogućnosti grupisanja (engl. clus-tering). Grupisanje je jedan od načina da se obezbedi otpornost na greške, tako što se korisnici koji su povezani s jednim serverom automatski prebacuju na drugi kada prvi server otkaže. U tehnologiji grupisanja servera koristi se izraz prespajanje nakon greške (engl. failouer). Grupisanje nije povezano samo s redundansom, već i s raspoređivanjem optere-ćenja (engl. load balancing) po pojedinim računarima u grupi, naročito se odnosi na mrežno opterećenje, jer se grupišu mrežni resursi. Tehnologije kao što su IntelliMirror i Group Control omogućavaju da korisnici znaju koji iz grupe od 50 servera trenutno opslužuje njihove zahteve. U grupisanju i raspoloživosti sistema uloge imaju mogućnosti kao što su sistem za rad s distribuiranim datotekama, preusmeravanje direktorijuma, nevezane datoteke, direktorijumi i druge.

Funkcije za skladištenje podataka imaju ključnu ulogu u raspoloživosti sistema. Windows 2003 podržava sve klase RAID nizova diskova. Sistem za rad s distribuiranim datotekama i NTFS 5.0 imaju nekoliko ključnih sposobnosti koje omogućavaju visoku raspoloživost sistema.

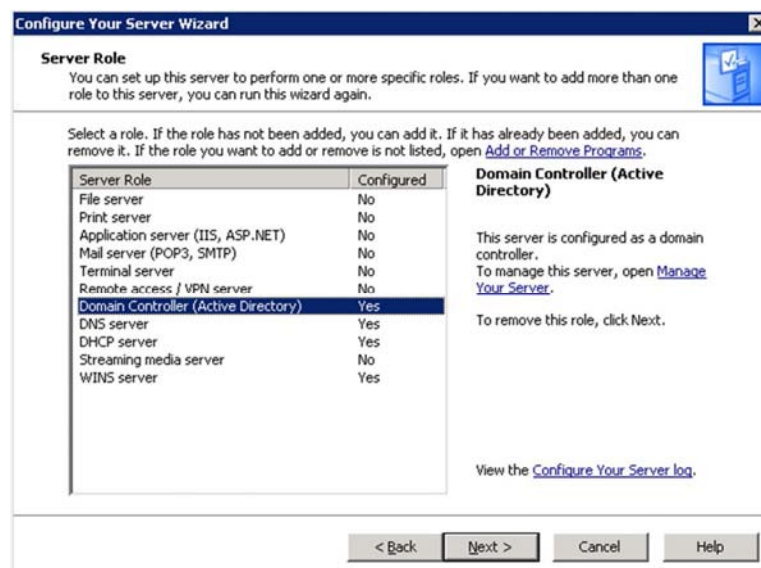
Microsoft je opremio Windows 2003 bezbednosnim funkcijama koje nijedan drugi operativni sistem ne može da ponudi. Svaka pristupna tačka na neki način može da se šifruje i zaštititi. Čak se može koristiti 128-bitni ključ, što je trenutno svetski nivo šifrovanja koji je nastao kao posledica fenomena elektronskog poslovanja i elektronske trgovine. Osim toga, Windows 2003 podržava i MIT-ov protokol Kerberos, verzija 5.0, što je de facto Internet standard koji omogućava jednokratno

prijavljivanje (Single Sign-On, SSO) i identifikaciju korisnika prilikom prijave na mrežu putem šifrovanja simetričnim ključevima i pomoću digitalnih certifikata.

Windows 2003 severu se može dodeliti više uloga u ovom radu biće predstavljene samo neke od njih, ali ujedno su to i uloge koje se najčešće sreću u gotovo svim kako manjim i srednjim tako i velikim računarskim mrežama. Windows 2003 server ima izuzetno jednostavan meni kojim se dodeljuju uloge serveru, već pri prvom startovanju pred korisnikom će se pojaviti meni Manage your server koji će dalje voditi korisnike kroz dodeljivanje uloge/uloga serveru.



Slika 1 i 2: Izgled menija Manage Your Server i podmenija Configure Your Server



- DC (Domain Controller), najbitnija uloga koju Windows 2003 server može da ima je baš ova uloga. Bez ovog severa moglo bi se smatrati da Windows 2003 mreža i ne postoji, na ovom serveru smešten je aktivni imenik. Preporučljivo je da ovaj server pruža isključivo usluge imenika i da razmenjuje replike s drugim serverima radi obezbeđivanja redundanse. Ipak je čest slučaj, ako ne i praksa da se pored uloge DCa glavnom računaru u mreži dodeljuje i uloge DNS i DHCP servera.
- Domain Name Server – DNS je server sistema za prevođenje imena u domen.
- WINS sever – namena mu je prevođenje NetBIOS imena u IP adrese, uglavnom se podiže na istom serveru gde je i DNS.
- DHCP – služi za automatsko dodeljivanje IP adresa računarima u mreži.
- IIS – Internet Information Server – ovaj server pruža Web i FTP usluge, to je izuzetno snažan internet server trebalo bi da se instalira na namenski server ili u kombinaciji sa file serverom.
- Print – ovaj server mreži obezbeđuje logičke štampače i stara se o redovima za štampanje.
- File – Podešen je za pružanje složenih usluga koje se odnose na rad sa datotekama i skladištenje podataka. Ovaj server je obično opremljen RAID 0 ili RAID 5 nizom diskova, mehanizmima za zamenu oštećenih diskova bez prekida rada i njihovo grupisanje, kako bi svim korisnicima datoteke bile neprekidno dostupne.
- ISA – Internet Security and Acceleration Server pruža uloge gateway-a i firewall-a sa detaljnim podešavanjima kao i mnoge druge usluge

ARHITEKTURA WINDOWS SERVERA 2003

Windows 2003 je modularni operativni sistem koji se sastoji od komponenata, a sagrađen je na osnovu Windows 2000 Servera. Svi objekti operativnog sistema imaju interfejse, pomoću kojih drugi objekti i procesi obezbeđuju njihovu funkcionalnost ili usluge. Komponente međusobno sarađuju prilikom obavljanja konkretnih zadataka operativnog sistema. Arhitektura Windowsa 2003 podeljena je u dva glavna sloja: korisnički sloj (engl. *user mode*) i sloj jezgra (engl. *kernel mode*).

Korisnički sloj

Korisnički sloj Windowsa 2003 u suštini je sloj za podršku aplikacijama, kako za Microsoftov softver, tako i za softver drugih proizvođača. Sastoji se od ugrađenih podsistema okruženja i od dodatnih (nezavisnih) podsistema. To je deo operativnog sistema koji omogućava drugim proizvođačima softvera da koriste usluge

operativnog sistema pozivajući objavljene API funkcije i objektno orijentisane komponente. Sve aplikacije i usluge instaliraju se u korisničkom sloju.

Sloj jezgra

Sloj jezgra (engl. *kernel mode*) Windowsa 2003 ima pristup sistemskim podacima i hardveru, a sastoji se od nekoliko komponentata:

Komponenta Windows 2003 Executive – *Executive* (izvršilac) je zajedničko ime za sve izvršne usluge, koje obuhvataju većinu ulazno/izlaznih rutina operativnog sistema i ključne komponente za upravljanje objektima, posebno onima koji su zaduženi za bezbednost. U grupu Executive spadaju i systemske usluge (dostupne u oba radna režima) i interne rutine koje rade u sloju jezgra (nedostupne kodu koji se izvršava u korisničkom sloju).

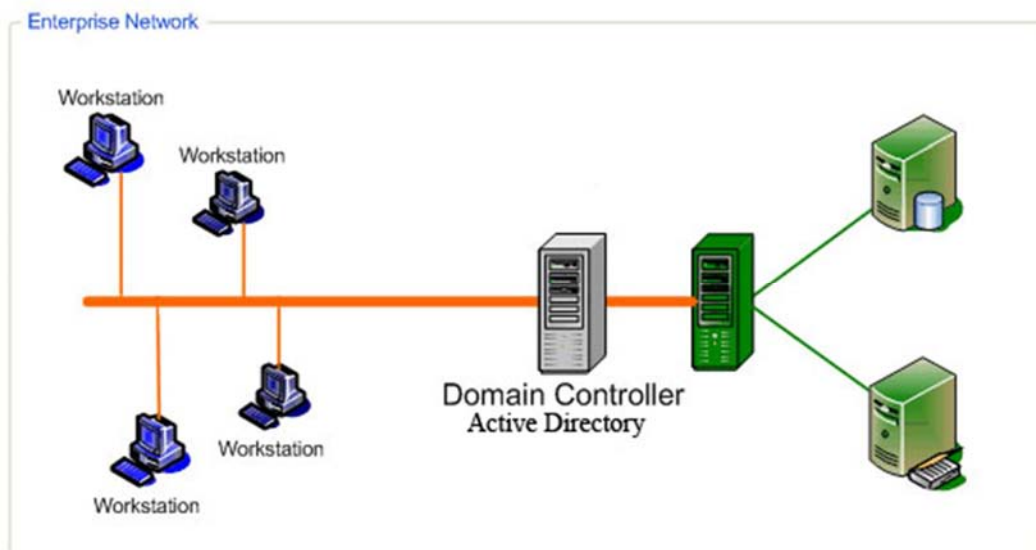
U sloju jezgra rade sledeće komponente:

- **File System (sistem datoteka):**
Prevodi zahteve upućene sistemu datoteka u format koji razumeju uređaji za skladištenje podataka.
- **Device Drivers (upravljajući programi):**
Komunicira sa upravljačkim programima koji direktno pristupaju hardveru.
- **Cache Manager (upravljač keša):**
Duboko unutar koda I/O Managera, ova komponenta upravlja performansama ulazno/izlaznih operacija tako što kreira operacije pisača na diskove. Ona takođe kešira zahteve za pisače i čitače i upravlja asinhronim pozadinskim operacijama upisivača na hardverske uređaje.
- **Security Reference Monitor (nadzornik bezbednosti):**
Ova komponenta se stara o poštovanju bezbednosnih mera koje važe za taj računar.
- **Interprocess Communication Manager (IPC) (upravljač međuprocenim komunikacijama):**
Delovanje ove komponente vidljivo je na mnogim mestima u operativnom sistemu. Njen najvažniji zadatak je upravljanje komunikacijama između klijentskih i serverskih procesa. Sastoji se od komponente Local Procedure Call (LPC) (poziv lokalne procedure), koja upravlja komunikacijama između klijentskih i serverskih procesa na istom računaru, i komponente Remote Procedure Call (RPC) (poziv udaljene procedure), koja upravlja

komunikacijama između klijentskih i serverskih procesa na različitim mašinama.

- **Memory Manager ili Virtual Memory Manager (VMM) (upravljач memorije ili upravljач virtuelne memorije):**
Upravlja virtuelnom memorijom. Ona obezbeđuje virtuelni adresni prostor svakom procesu koji postoji i štiti taj prostor radi očuvanja integriteta sistema. Njen zadatak je i kontrolisanje pristupa disku radi dobijanja virtuelne radne memorije, što je poznato i kao straničenje (engl. *Paging*).
- **Process Manager (upravljач procesima):**
Započinje i uništava procese i niti koje nastaju tokom rada sistemskih komponenta i aplikacija.
- **Plug and Play Manager (upravljач mehanizma „utakni i koristi”):**
Pruža usluge „utakni i koristi” i komunicira sa upravljačkim programima radi konfigurisanja i usluga vezanih za hardver.
- **Power Manager (upravljач napajanja):**
Upravlja napajanjem sistema. Ona radi u sadejstvu sa API funkcijama za upravljanje napajanjem i obrađuje događaje koji se tiču zahteva za upravljanje napajanjem.
- **Window Manager I Graphical Device Interface (GDI) (upravljач prozorima I interfejs grafičkog podsistema):**
Upravljački program win32K.sys koji objedinjuje usluge sledećih komponenta i upravlja sistemom za prikazivanje slike.
- **Window Manager:**
Upravlja sadržajem ekrana i prikazivanjem prozora. Ona obrađuje i ulazno/izlazne podatke s miša i tastature.
- **GDI:**
Ova komponenta je najsloženiji interfejs za programiranje. Za nju nikada nije bilo dovoljno memorije u danima 16-bitnog Windowsa. Stara se o iscrtavanju i prikazu grafike na ekranu, i sarađuje s komponentama koje prosleđuju grafičke objekte štampačkim objektima i drugim uređajima za prikazivače grafike.
- **Object Manager (upravljач objekata):**
Upravlja sistemskim objektima. Ona ih stvara, upravlja njima i briše ih kada više nisu potrebni. Sem toga, ona upravlja resursima koji se po potrebi dodeljuju tim objektima, npr. memorijom.

DOMAIN CONTROLLER



Slika 3: Ilustrovani prikaz Domain controller arhitekture

Server Domain Controller (DC) predstavlja „srce“ svake lokalne mreže. Samo podizanje domena i povezivanje računara u jednu celinu omogućava upravo ovaj server. Podizanje domena odnosno instalacija istog nije komplikovan posao, ali uređenje pravila za korisnike na mreži može biti dugotrajan proces. U zavisnosti od veličine mreže odnosno broja računara i korisnika Domain Controller može biti instaliran kao pojedinačan računar, ili u kombinaciji sa servisima DNS i DHCP. Važnost DC-a se ogleda u aktivnom imeniku (Active Directory), koji predstavlja bazu podatak svih korisnika na mreži. Podizanje DC-a je nemoguće izvršiti nezavisno od instaliranja aktivnog imenika (AD). Servisi poput DNS i DHCP mogu biti nezavisni dok DC i AD uvek idu zajedno i na jednom serveru.

Domain Controller hardverski treba da bude „moćan“ računar; sa sistemom redundantnog napajanja kao i sistemom diskova u RAID setu, ovom računaru takođe je potrebno obezbediti kvalitetan izvor napajanja pa se preporučuje upotreba jakih firmiranih UPS uređaja kao i agregata. Jednom instaliran takav računar može da služi kao DC u okviru neke organizacije i do par godina. Na njega uvek treba obratiti posebnu pažnju. Prostorija u kojoj je DC smešten treba da ispunjava uslove koji su najoptimalniji za boravak računara na tom mestu, a to se pre svega odnosi na temperaturu. Kao i svaki računar tako i DC može biti oštećen - hardverski ili softverski. Zbog bezbednosti i velike funkcije koju obavlja DC treba pribegavati podizanju još jednog servera koji će predstavljati backup DC, odnosno biti replika postojećem serveru.

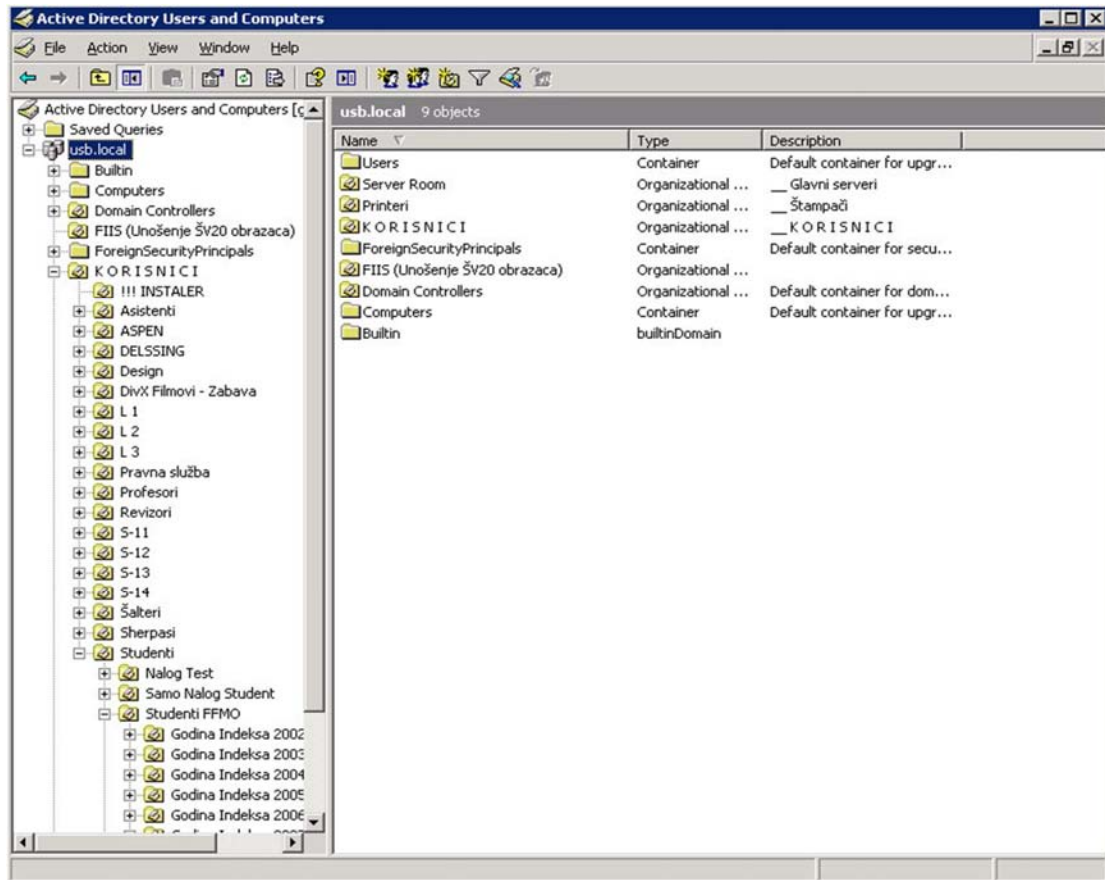
ACTIVE DIRECTORY

Aktivni imenik je centralno čvorište (engl. hub) mreže. Bez aktivnog imenika, ne može se reći ni da Windows 2003 mreža postoji. Premda još uvek ima nedostataka, impresionira broj alati dodat je aktivnom imeniku u verziji Windows 2003. Ovde ću nabrojati samo neke od alati koje Windows 2003 nudi a administratori ih svakodnevno koriste:

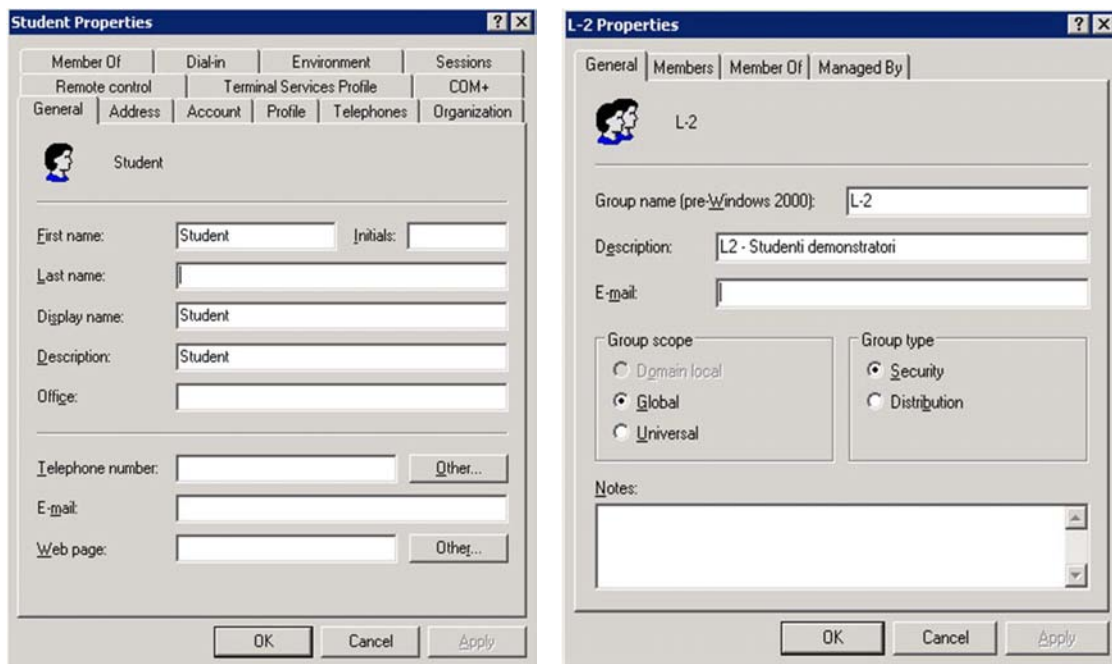
- Nevezani direktorijumi. Tehnologija nevezanih direktorijuma (engl. Offline folders) omogućava da napravite kopiju datoteke sa servera i da radite s njom i nakon što prekinete vezu s mrežom. Kada prekinete vezu sa serverom, datotekom s kojom ste radili upravlja se kao da se ona još uvek nalazi na serveru. Što se vaše aplikacije tiče, ona „misli“ da je i dalje povezana sa serverom. Izmene u datoteci snimate na disk na uobičajeni način kao kada radite na mreži. U ovom slučaju, odredište je resurs koji se ne nalazi u mreži, ali koji je slika datoteke i direktorijuma sa servera. Kada ponovo uspostavite vezu s mrežom, datoteka se ponovo sinhronizuje - najnovije izmene se unose u kopiju datoteke koja se nalazi na serveru.
- Preusmeravanje direktorijuma (engl. folder redirection) još jedna je od mogućnosti aktivnog imenika koja direktorijum čini redundantnim. Ako se prekine veza sa serverom, a vi ste i dalje povezani s mrežom, kada sledeći put snimate datoteku na disk, ona se preusmerava u drugu kopiju direktorijuma na drugom serveru.
- Lutajući profili (engl. roaming profiles) nasleđeni su iz Windowsa NT, ali su u Windowsu 2003 znatno unapređeni. Osnovna ideja je da vas vaš korisnički profil sledi gde god se krećete.
- Usluge daljinskog instaliranja (Remote Installation Services, RIS) skup su više komponenata i usluga koje vam omogućavaju da daljinski instalirate Windows XP Professional i Windows XP Home Edition na stone i prenosive računare.
- Instaliranje i održavanje aplikacija. Usluge koje pruža Active Directory omogućavaju daljinsko uklanjanje i instaliranje softvera na radnim stanicama korisnika.

Tehnologija Active Directory omogućava da administrativne funkcije i odgovornost raspodelite na više celina. Tako ih možete organizovati i unutar mreže

ili domena radi lakšeg administriranja. Usluga distribuiranog imenika omogućava vam da administriranje korisnika i mrežnih resursa raspodelite širom organizacije. Na starijim NT sistemima mogli ste da definišete korisnike i grupe sa administratorskim pravima, ali je bilo gotovo nemoguće da od tih administratora sakrijete druge mrežne resurse.



Slika 4: Izgled konzole Active Directory Users and Computers.

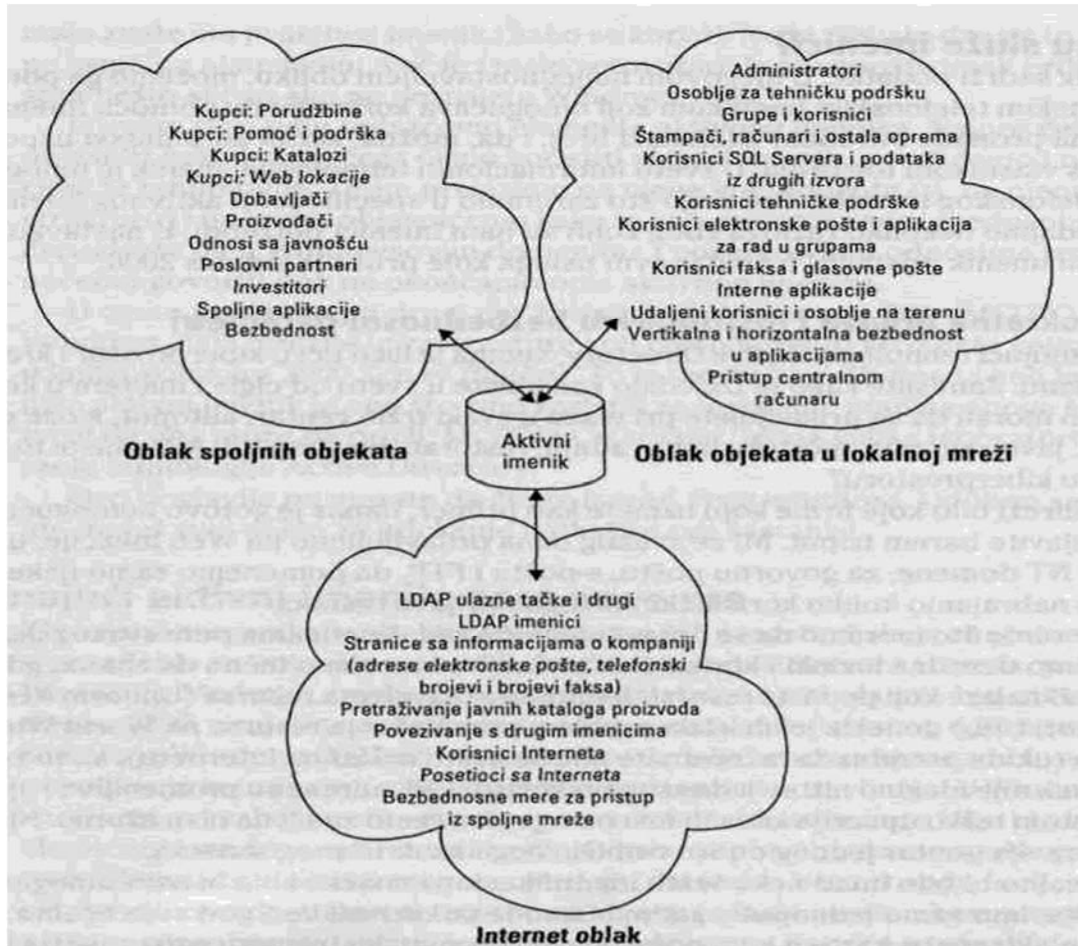


Slika 5: Izgled podmenija za podešavanje pojedinačnog naloga i podmenija za podešavanje Security grupa gde može biti smešteno više naloga ili organizacionih jedinica

Svaki korisnik pre nego što počne koristiti resurse mreže mora imati korisničko ime i lozinku. Korisničko ime i lozinka se dobijaju otvaranjem naloga u aktivnom direktorijumu. Administrator otvara nalog i smešta korisnika u određenu već definisanu grupu. U okviru jedne organizacije za administratora je veoma važno da zna koliko korisnika uopšte postoji na mreži, da li ti korisnici imaju svoje računare i kojom vrstom posla se bave. Velike organizacije sa velikim brojem korisnika uvek moraju imati veći broj otvorenih naloga u okviru aktivnog direktorijuma. Pored zaposlenih lica koji imaju svoje računare i koji imaju pravo pristupa mrežnim folderima, postoje korisnici koji će se tretirati kao gosti. Oni će tražiti pravo pristupa najčešće internetu, a pristup samoj lokalnoj mreži i resursima njima ne bi trebalo omogućiti. U skladu sa tim u aktivnom direktorijumu može da postoji nalog koji će na desktopu prikazivati samo ikonu određenog brauzera za pristup internetu. Takvi korisnici će biti članovi određene grupe na koja su primenjena pravila zabrane pristupa svemu sem internetu.

Pošto aktivni imenik može da bude izdelfen tako da potpuno preslikava organizacionu strukturu preduzeća, moguća je i raspodela administrativnih poslova po delovima te strukture. Drugim rečima, logično je da nekoga ko radi u određenom odeljenju zadužite za obavljanje rutinskog dela upravljanja resursima tog odeljenja.

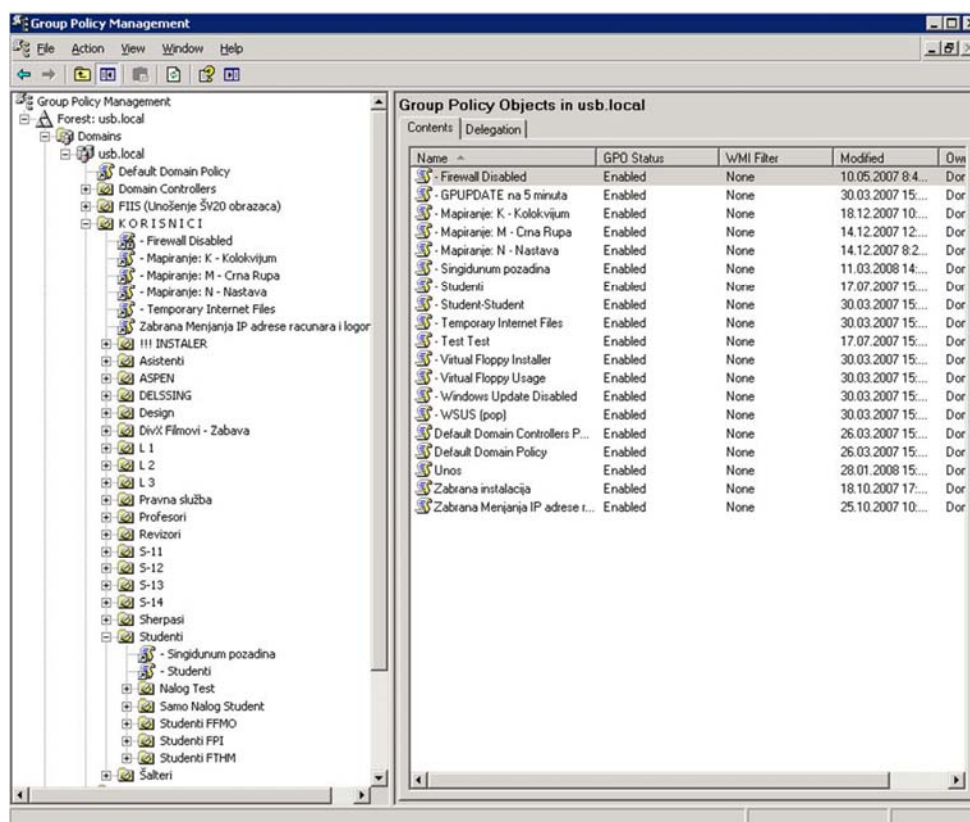
Aktivni imenik je univerzalno distribuirano spremište za podatke kroz koje na standardizovan način može da se pristupa svim mrežnim objektima, kao što su konfiguracije aplikacija, usluge, računari, korisnici i procesi, i to širom cele lokalne mreže ili šire mreže čiji je ona deo.



Slika 6: Izgled i uloga aktivnog imenika u mrežnoj organizaciji

GROUP POLICY

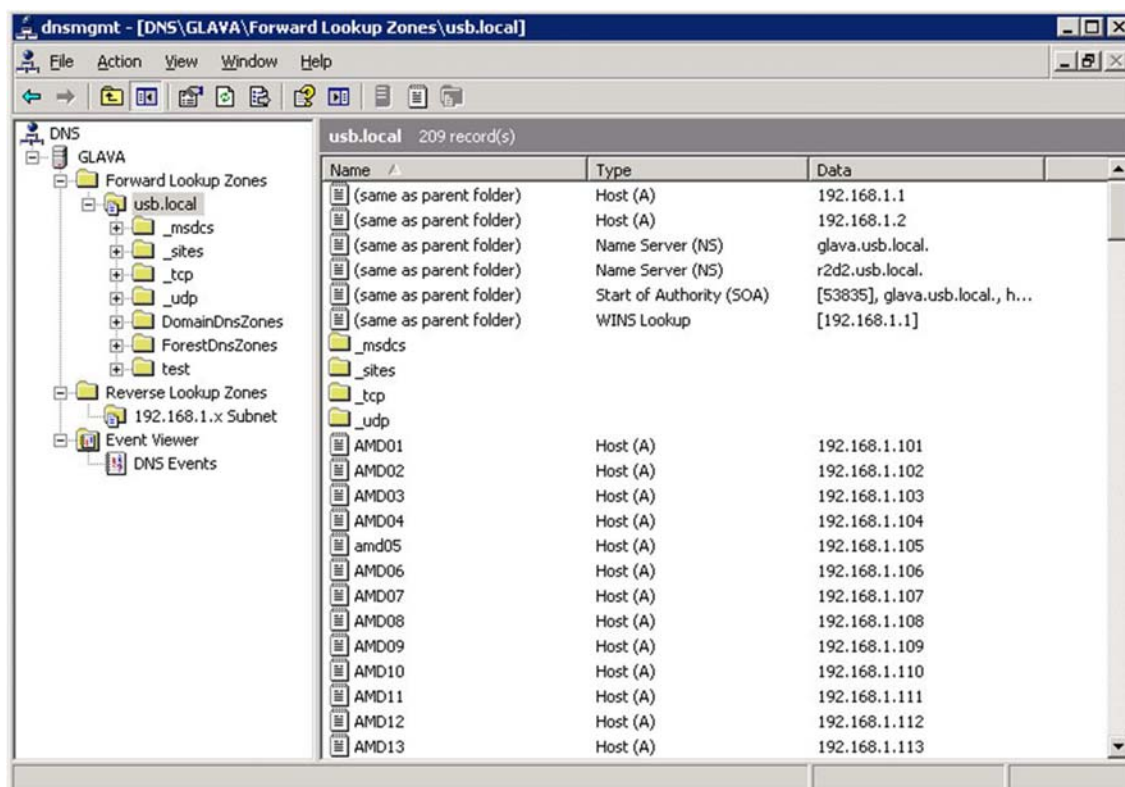
Upravljanje Windows mrežama i Windows Serverom 2003 znatno je olakšala nova tehnologija Group Policy (grupna strategija), koja omogućava upravljanje korisničkim parametrima, bezbednosnim merama, domenom, parametrima radne površine i drugim podešavanjima. Ukratko, većim delom radnog prostora upravlja se pomoću grupnih strategija. Kao i organizacione jedinice aktivni direktorijum po instalaciji sadrži kreirane grupe. Svaki korisnik mora biti član neke grupe, a potom i organizacione jedinice. Postojeće grupe u okviru aktivnog direktorijuma mogu poslužiti administratoru da korisniku dodeli ili oduzme prava pristupa mrežnim resursima (postojeće grupe imaju unapred određena prava, odnosno na njih su primenjene polise). Tehnologija Group Policy primenjuje se na svim nivoima organizacije, u aktivnom imeniku, od domena do organizacionih jedinica itd. Alatka za taj posao je editor grupne strategije (Group Policy Editor, GPE). GPE omogućava da stvarate objekte koji su u aktivnom imeniku pridruženi organizacionim jedinicama ili koji se pozivaju na njih. Objekti grupne strategije (Group Policy Objects, GPO) mogu da budu zaštićeni NTFS pravima pristupa na isti način kao datoteke i direktorijumi.



Slika 7: Izgled konzole Group Policy Management.

DNS (DOMAIN NAME SYSTEM)

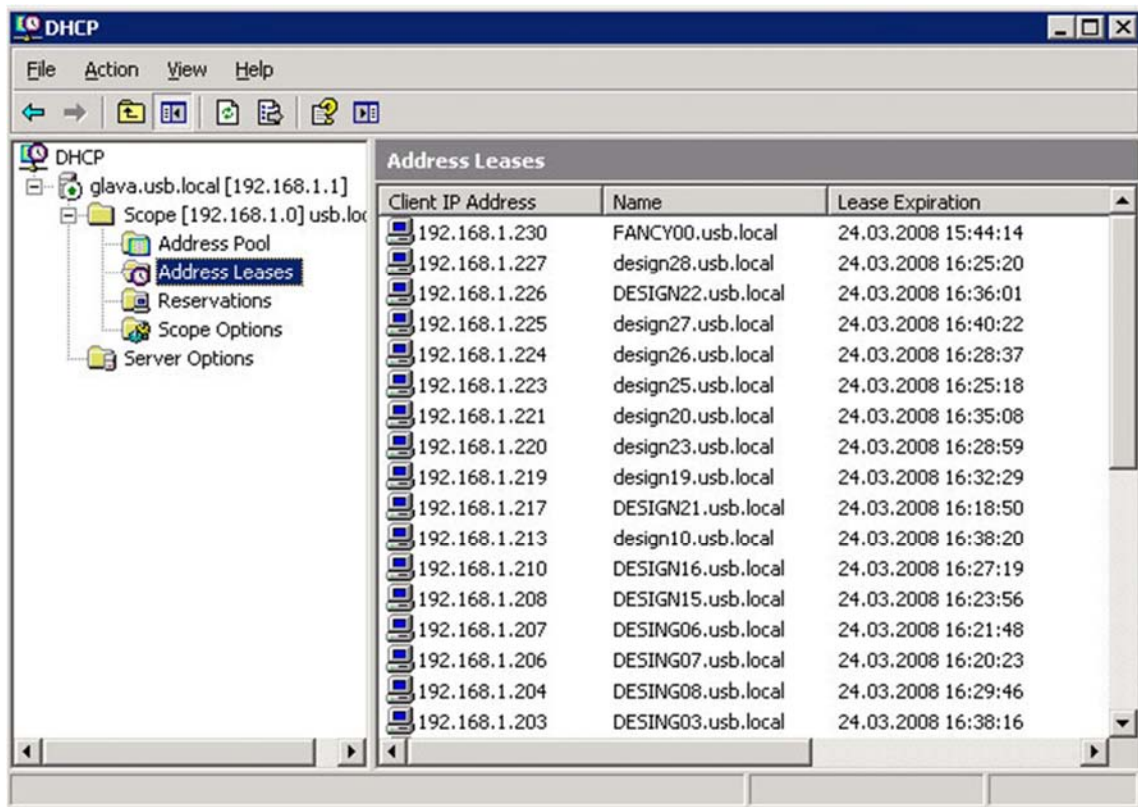
DNS servis uopšteno govoreći predstavlja servis za razrešavanje imena računara u njegov jedinstveni broj (IP adresa) i obrnuto. Kada se pristupa instalaciji DNS servera potrebno je razmotriti sve parametre lokalne mreže na koju želite da primenite ovaj servis. Kao što smo napomenuli servisi poput DNS i DHCP mogu biti instalirani zajedno sa DC (Domain Controller) ili potpuno nezavisno. Po instalaciji servisa potrebno je izvršiti određena podešavanja da bi DNS pravilno razrešavao imena računara. U okviru Windows XP operativnog sistema parametre mrežne kartice je moguće manuelno konfigurisati. Međutim ukoliko DC radi ispravno, DNS servis mora biti automatski uočen na mreži. Instaliran DNS po osnovnim podešavanjima razrešava imena računara u IP adresu. Za to je zadužena Forward Lookup zona. Prilikom njenog kreiranja sistem nas upućuje u način rada tako konfigurisanog DNS-a.



Slika 8: Izgled konzole Domain Name System

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

DHCP (Dynamic Host Configuration Protocol) je servis koji dodeljuje računarima jedinstvene IP adrese. Uz pomoć ovog servisa sistem sam automatski nadgleda računare i vodi računa da IP adrese budu pravilno raspoređene odnosno dodeljenje. Domen može da funkcioniše i bez ovog servisa, ali to može da prouzrokuje probleme i mnogo manuelnih podešavanja koje mora da izvrši administrator. Pri instalaciji kao i kod DNS-a mora se voditi računa o strukturi mreže, serveru na koji instaliramo servis kao i svim ostalim računarima u domenu koji imaju funkciju servera. Korišćenje DHCP iziskuje određena podešavanja da bi DHCP adrese bile isporučene svim računarima i da se uvek ima kontrola nad celokupnim procesom.



Slika 9: Izgled konzole Dynamic Host Configuration Protocol

BEZBEDNOST

Ništa što radite nije važno ako nemate strategiju koja vodi računa o bezbednosti vaše mreže. Vaši pažljivo osmišljeni i implementirani sistemi mogu da prestanu sa radom, ili da pokleknju pod napadima odbijanja usluge ili destruktivnog softvera. Vaši podaci mogu da budu ukradeni, promenjeni, obrisani, ili uništeni virusima, nesrećama ili direktnim napadom. Zlonamerni napadač, čak i sa udaljenog mesta može da kontroliše vaš računar, sadržaj vaše web lokacije može da se promeni, ili da se uništi reputacija kompanije.

Protokoli za bezbednost mreže se koriste da bi se njima upravljalo i obezbedilo ovlašćivanje, provera autentičnosti, poverljivost, integritet i neodbijanje. U Windows Server 2003 mreži, glavni protokoli su Kerberos, New Technology Local Area Network Manager (NTLM), Internet Protocol Security (IPSec), i njihovi različiti potprotokoli. Drugi protokoli podržavaju ove protokole i drugi bezbednosni parametri podržavaju i štite korišćenje ovih protokola za bezbednost.

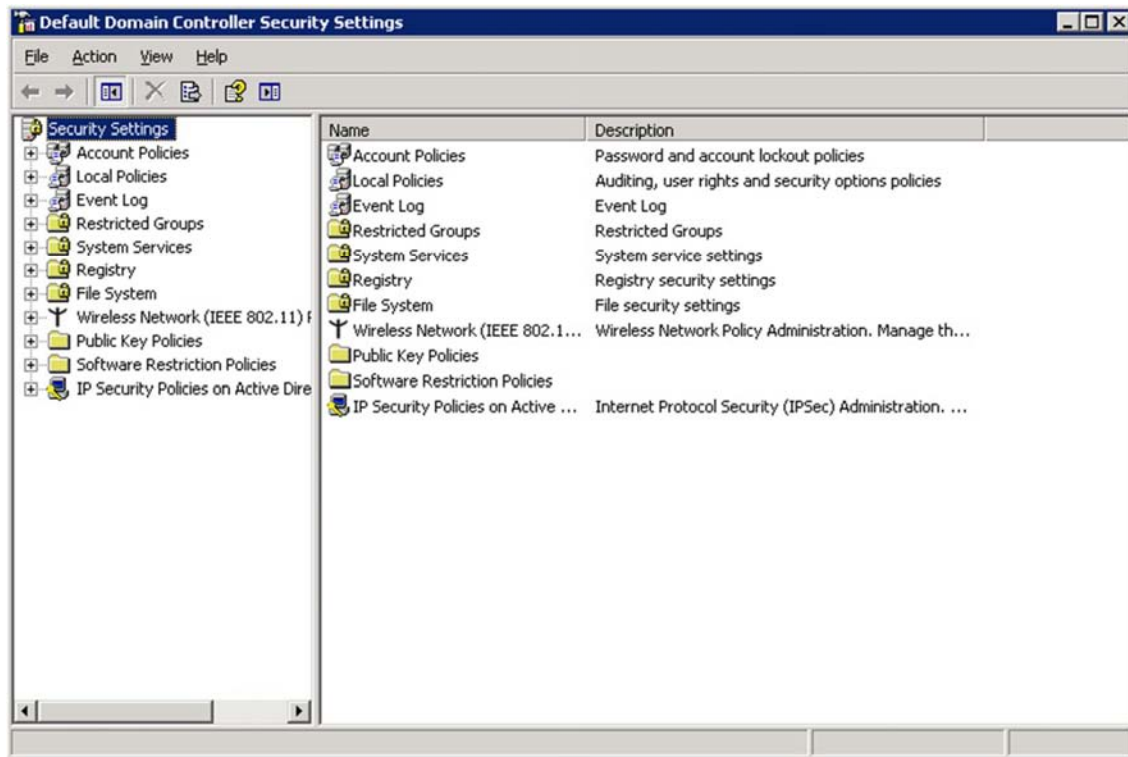
U sledećoj tabeli prikazani su šabloni za bezbednost i protokoli koji ih podržavaju:

Paradigma	Svrha	Protokoli
Provera autentičnosti	Dokazuje da ste onaj za koga se predstavljate	Kerberos i NTLM (NT LAN Manager [LM] protokol u startu nije dostupan, ali može se podesiti.)
Ovlašćivanje	Određuje šta možete da radite u mreži kada se proveri autentičnost	Kerberos i NTLM
Poverljivost	Održava tajnost podataka	Kerberosove, NTLM-ove, i IPSecove šifarske komponente (radi zaštite i druge komunikacije pored provere autentičnosti).
Integritet	Obezbeđuje primanje upravo onih podataka koji su i poslali	Kerberosove, NTLM-ove, i IPSecove komponente
Neodbijanje	Utvrdjuje ko je tačno poslao i primio poruku	Kerberos i IPSec

Zadatak implementiranja konfiguracija za bezbednost servera u Windows mreži je trostruk. Prvo, morate razumeti šta čini dobnu bezbednost. Drugo, morate umeti da implementirate bezbednost na opremi za informacione sisteme kojima upravljate u svojoj organizaciji. Konačno, morate voditi računa da su alati i metodologije na raspolaganju za brzu primenu bezbednosne konfiguracije, i morate razumeti kako da ih koristite i održavate. Na kraju, rukovodstvo mora utvrditi bezbednosna pravila koja najviše odgovaraju. U prošlosti, mnogi alati i parametri u bazi Registry su bili potrebni da se zadovolji politika bezbednosti. Danas, međutim,

bezbednosni šabloni, i posebno njihova globalna primena u grupnoj politici, mogu da reše ovaj treći zadatak: brza primena i održavanje u celoj kompaniji.

U pristupnom radu ću samo pomenuti i pokazati izgled Domain Controller Security Settings-a dok će u drugom delu rada ova konzola biti detaljno objašnjena kao i sve mogućnosti koje ona nudi. Na sledećoj slici je prikazan izgled konzole Domain Controller Security Settings:



Slika 10: Domain controller Security Settings MMC konzola

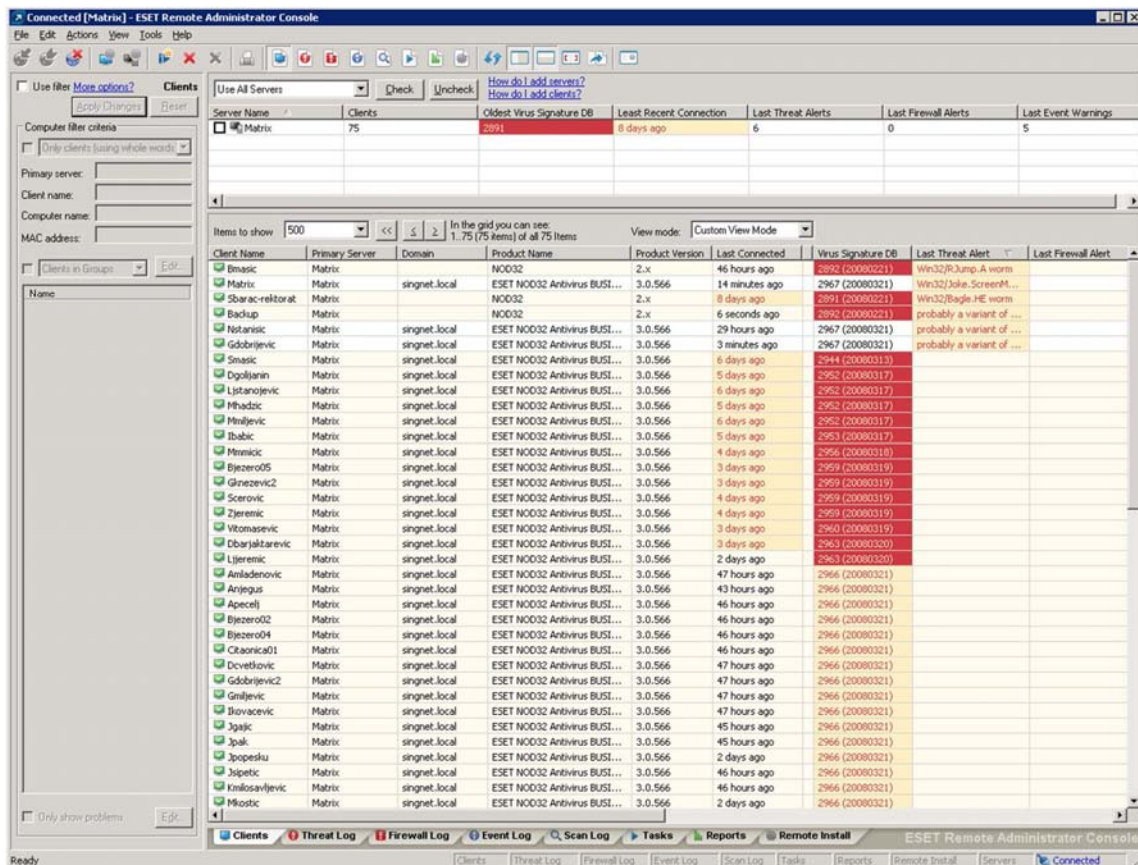
ANTIVIRUS PAKET PROGRAMA

Priča o bezbednosti nebi bila potpuna bez dobrog antivirus programa. Kao što sam u početku rada istakao Microsoft Windows platforma bilo da se radi o radnoj stanici ili o serveru predstavlja sistem najpodložniji napadima hakera i virusa samim tim potrebna mu je adekvatna i dodatna zaštita pored one koju nudi Microsoft. Kvalitetnu i sveobuhvatnu zaštitu jednog Windows 2003 domena pronašao sam u ESET-ovoj distribuciji antivirusnog rešenja NOD32.

NOD32, na tržištu pod tim nazivom od 1997. godine, je bio prvi proizvod na tržištu koji je svojim korisnicima nudio tehnologiju heurističkog detektovanja nepoznatih virusa. Često nazivan i Antivirusni Sistem Nove Generacije, NOD32 konstantno ostavlja konkurenciju iza sebe na svim testovima na svim poljima, od broja detektovanih virusa preko performansi procesa skeniranja do jako malog utroška sistemskih resursa. NOD32 Antivirus System je dobro izbalansirana, vrlo savremena i pouzdana zaštita od svih vrsta pretnji koje danas ugrožavaju PC računare. Podržava Microsoft operativne sisteme DOS, Windows 9x/ME/NT/2000/XP/2003, operativne sisteme Linux/Unix, Novell, MS Exchange Server, Lotus Domino server i druge e-mail servere. Napredne metode za detekciju obezbeđuju zaštitu čak i od budućih pretnji i nepoznatih virusa.

Serverska instalacija NOD32 u mnogome administratorima olakšava život preko svoje konzole nazvane: Remote Administrator Console, ova konzola umnogome podseća na same Microsoftove konzole sa detaljnim pregledom stanja zaštićenosti računara, napadima virusa, ažurnosti antivirus baza...

Na sledećim slikama je prikazan izgled NOD32 Remote Administrator Console, kao i tab za daljinsko instaliranje NOD32 antivirus programa na klijentski računar:



Slika 11: Izgled NOD32 Remote Administrator Console

ISA SERVER

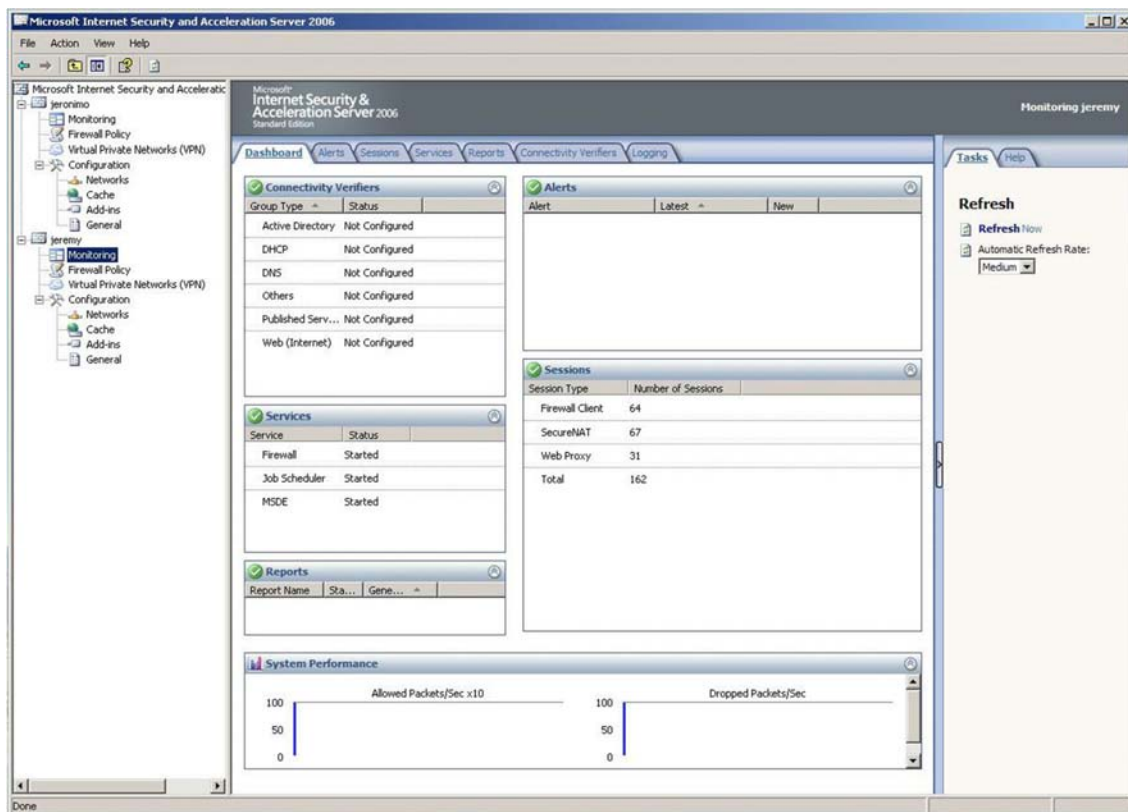
Microsoft ISA Server je moćno rešenje za priključivanje mreže na Internet, u najkraćem, obuhvata firewall i proxy softver prijateljskog korisničkog okruženja. ISA je softver koji za sigurnosnu zaštitu Internet veze nudi podesivi firewall i filter na različitim slojevima komunikacije. Posедуje i značajne mehanizme za zaštitu od napada, izveštaje o korišćenju Interneta.... ISA Server odlikuje izuzetna skalabilnost, odnosno prilagodljivost velikim i malim sistemima. Više instaliranih ISA servera mogu da sarađuju, čime se dobija distribuirani keš. Ovakav keš može se koristiti za balansiranje velikog saobraćaja, i za otpornost sistema: u slučaju da neki od servera ispadne iz pogona, sistem će nastaviti da radi. Firewall je danas obavezan prilikom priključivanja na Internet. To je princip koji radi na nivou paketa i cilj je da ka unutrašnjosti prođu samo paketi koji su vezani za neki zahtev koji je bio upućen u svet. Rekosmo da ovaj firewall može da se koristi na različitim slojevima

komunikacije, a ono što niste navikli da vidite kod firewall-a su tzv. aplikacioni filteri. To su pravila na najvišem sloju komunikacije, koja mogu da se zasnivaju na sadržaju niza paketa. Firewall je prirodno rešenje za aplikacije koje se ponašaju samo kao klijenti u TCP/IP saobraćaju, dok serverskim TCP/IP aplikacijama predstavlja prepreku. Međutim, vrlo su česte aplikacije tipično klijentskog tipa koje zahtevaju i serverski saobraćaj, pa običan firewall predstavlja branu za njihovo korišćenje. Stoga je ISA server veoma koristan na aplikativnom nivou. Primer je FTP aplikacija koja pravi dve konekcije, klijentsku i serversku. Dobro rešenje za prolazak FTP klijenata kroz ISA server je instalacija FTP aplikacionog filtera – ISA server će dinamički otvarati potreban port prema spoljnim konekcijama, prevoditi adrese prema unutrašnjim klijentima koji će biti „iza zida“. Ovaj filter čak nudi i mogućnost da fino podešavate prava: određenim korisnicima, recimo, možete dozvoliti samo čitanje fajlova.

Aplikacioni filter SMTP saobraćaja je dodatna mera zaštite za e-mail server, nezavisno od toga koji softver koristite za upravljanje elektronskom poštom. Filter štiti od buffer overrun napada. Možete koristiti Message Screener za napredno filtriranje SMTP saobraćaja po tipu attachment-a. DNS filter brani od nekoliko overflow DNS napada i transfera zona putem DNS klijenata. ISA prepoznaje Ping-Of-Death, IP spoofing, WinNuke, Land, UDP bomb, skeniranje portova... reč security iz naziva ima smisla! Pored „fabričkih“ mogućnosti ISA server se može proširivati, jer je Microsoft objavio Software Development Kit.

Postoji više načina da usmerite radne stanice na ISA server. Prva je da ga koristite kao svaki Web proxy server za surfovanje: u Web browser-u odredite adresu i port proxy servera. U tom slučaju će radne stranice biti uskraćene za Internet aplikacije i protokole koji ne podržavaju ovakav Web proxy način, a one aplikacije koje podržavaju proxy često moraju biti ručno podešene. Drugi način je da koristite ISA kao NAT (Network Address Translation) server. ISA server će biti raskrsnica, prevoditi javne IP adrese u privatne (i obrnuto), omogućavajući nesmetan saobraćaj većini TCP/IP protokola. Najčešće je dovoljno na klijentu podesiti adresu ISA servera za default gateway. Time će svi paketi koji nisu namenjeni lokalnoj mreži biti prosleđeni ISA serveru koji će prevesti privatnu adresu u javnu i poslati zahtev na Internet. Svaki računar koji koristi TCP/IP može se ovako podesiti. Nažalost, ISA server i dalje nema informaciju o tome koji korisnik je poslao zahtev, već samo koji računar. To je razlog što postoji treći tip klijenata. Firewall Client je aplikacija koja se instalira na radnim stanicama. Aplikacija postoji za sve verzije Windows-a i predstavlja čvrstu vezu računara sa ISA serverom. Korisnici ne moraju ni znati da je ova aplikacija instalirana – sve izgleda kao da su povezani direktno na Internet, osim što systray-u imaju dodatnu informaciju o dostupnosti ISA servera; ako ISA server nije dostupan, aplikacija će se isključiti što olakšava korišćenje laptop-a na poslu i

kod kuće. Kada imate ovakve klijente, pravila za pristup Internetu putem TCP i UDP protokola možete vezati za pojedinačne korisnike. Statističke izveštaje o upotrebi Interneta moći ćete da pravite i po korisnicima. Klijent je odlično integrisan u Windows – sve proradi kao od šale, klijent i server uvek znaju koji korisnik je ulogovan i koristi Internet... ISA klijentske aplikacije možete instalirati i centralizovano koristeći grupne polise. Administratorska konzola je standardna MMC konzola, čime je omogućena administracija na daljinu. Windows Performance Monitor biće obogaćen dodatnim brojačima (counter) za praćenje performansi ISA servera. Na osnovu brojača aktivnih konekcija na firewall-u i broja zahteva po sekundi na ISA kešing delu, administrator dobija precizan pregled iskorišćenosti hardverskih i softverskih resursa tokom rada servera.



Slika 12: Osnovni ekran pri logovanju na ISA server

DATACENTRI KAKVE SMO POZNAVALI DO DANAS

Tema prvog dela rada odabrana na osnovu višegodišnjeg angažovanja na poslovima administriranja računarskih mreža zasnovanih na MS Windows 2003 operativnom sistemu. Kao osnovni cilj prvog dela rada je postavljena analiza mogućnosti koje ovaj operativni sistem nudi kao odgovor na sve zahtevnije servise koji se koriste u savremenim računarskim mrežama. Analizom su obuhvaćeni različiti aspekti obrađenih funkcionalnosti tako da ona sadrži objektivno poređenje prednosti korišćenih pristupa i ograničenja koje ti pristupi postavljaju. Upoređivanje realizacija mrežnih servisa u okviru MS Windows 2003 operativnog sistema je vršeno u odnosu na realizacije u konkurentnim mrežnim operativnim sistemima na tržištu (Novel, Unix, Linux, Mac OS).

U vreme pisanja prvog dela rada pojavio se i novi Microsoftov mrežni operativni sistem, Windows Server 2008 koji je sa sobom doneo i mogućnost virtualizacije. Iako virtualizacija nije novina u ovom trenutku, ovo je prvi put da je ona ponuđena kao sastavni deo nekog operativnog sistema ili čak kao samostalni potpuno besplatni host operativni sistem.

Ovo je logično dovelo do omasovljivanja virtualizacije i do uvođenja novih rešenja u informacione sisteme kako za administratore tako i za same korisnike. U drugom delu rada predstavljena su tri najčešće korišćena tipa virtualizacije, a Microsoft Hyper-V je i detaljno testiran.

PROBLEMI FIZIČKOG DATACENTRA

Klijent-server model je sa sobom doneo koncept: jeftin standardni industrijski server na kome je pored operativnog sistema instalirana najčešće jedna aplikacija (na primer: domen kontroler, server baza podataka, mejl server, itd.). Vremenom, zahvaljujući razvoju Interneta, broj aplikacija (servisa) se sve više povećavao, da bi u poslednje vreme, sa pojavom web servisa, dostigao paradoksalne razmere. Masovna pojava novih servisa, dovela je do enormnog povećanja broja servera u datacentru. S druge strane, efikasnost iskorišćenja ovih servera je sve više opadala. Neke procene (IDC) govore da je iskorišćenost procesora prosečnih industrijskih servera ispod 10%, što ekonomičnost infrastrukture datacentra ozbiljno dovodi u pitanje.

Pored faktora ekonomičnosti IT infrastrukture, deluju i drugi činioci koji virtualizaciju dovode u prvi plan: promena pristupa u projektovanju mikroprocesora, tj. pojava procesora sa dva, četiri, a uskoro i više jezgara, brze i jeftine memorije i naprednih I/O arhitektura. Prosečan današnji industrijski server je "prejak" za servise (aplikacije) koje su na njemu instalirane. Dalje, od IT servisa korisnici očekuju vrlo visoku raspoloživost (reda 99,9%), koju nije moguće obezbediti konvencionalnim tehnikama. Rast broja servisa zahteva vrlo brzu i čestu instalaciju novih servera. Nabavka hardvera, s druge strane, je proces koji traje danima i nedeljama, te klasična nabavka smanjuje agilnost IT usluga. Od IT usluga se, pored svega navedenog, očekuje da obezbede kontinuitet poslovanja preduzeća čak i u slučaju katastrofa (požari, poplave, zemljotresi...). Obezbediti rezervnu IT infrastrukturu na udaljenoj lokaciji i ekonomično je implementirati dupliranjem hardvera/softvera iz glavnog datacentra, jednostavno nije moguće. Zbog toga mnoga preduzeća ni nemaju odgovarajuća rešenja za navedene situacije. Time ozbiljno rizikuju nastavak poslovanja posle katastrofe.

MOGUĆA REŠENJA - REŠENJA KOJA NUDI VIRTUALIZACIJA

Korišćenjem virtualizacije moguće je podići efikasnost korišćenja IT resursa na 60-80% (približno kao u mainframe okruženju). Pri tome je broj fizičkih servera, kako pokazuju slučajevi mnogih od preko 20.000 korisnika, moguće smanjiti za 8-30 puta. Posledično, znatno se smanjuje i utrošak električne energije u datacentru (koja se, zapravo, pretvara u toplotu) i fizički prostor potreban za instalaciju datacentra (koji u npr. u centru grada predstavlja vrlo skupu imovinu).

Napredne opcije omogućavaju da servis (kako ga vide krajni korisnici) bude znatno više raspoloživ od hardvera na kome je instaliran. Iskustva korisnika pokazuju da neki servisi bez prekida rade blizu 1000 dana, s tim što su u međuvremenu više desetina puta migrirani sa hosta na host. Stavljanje novog virtualnog servera na raspolaganje IT razvoju / korisnicima je postupak koji traje nekoliko minuta (kloniranje, kreiranje na osnovu šablona), u poređenju sa 3-4 nedelje za nabavku i instalaciju fizičkog servera.

Održavanje hosta više ne predstavlja stresan posao, jer su servisi pre početaka intervencije već migrirani, primenom DRS-a, na druge hostove, tako da krajnji korisnici ne primećuju nikakav zastoj.

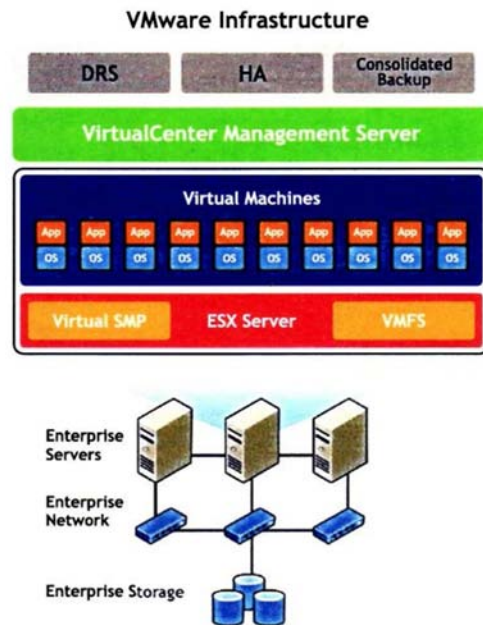
Arhitektura rezervnog datacentra (koji se koristi u slučaju katastrofe) može biti vrlo kompaktna i ekonomična - potpuno virtualizovana. Štaviše, ova infrastruktura može biti de-ljiva sa drugim korisnicima i samim tim više puta jeftinija nego sopstvena. Instalacija i administracija operativnih sistema i aplikacija koje oni podržavaju postaje znatno jednostavnija (iskustvo pokazuje da se potrebni resursi (ljudi, vreme) smanjuju na trećinu).

Distribucija, testiranje i evaluacija novog softvera koji se isporučuje u formi virtualnih mašina je znatno ubrzana i olakšana. Na sajtu vmware.com se može se naći više od 300 takvih mašina, a isti koncept su prihvatili i svi drugi veliki (Microsoft, Oracle...) i mali isporučioци softvera i rešenja.

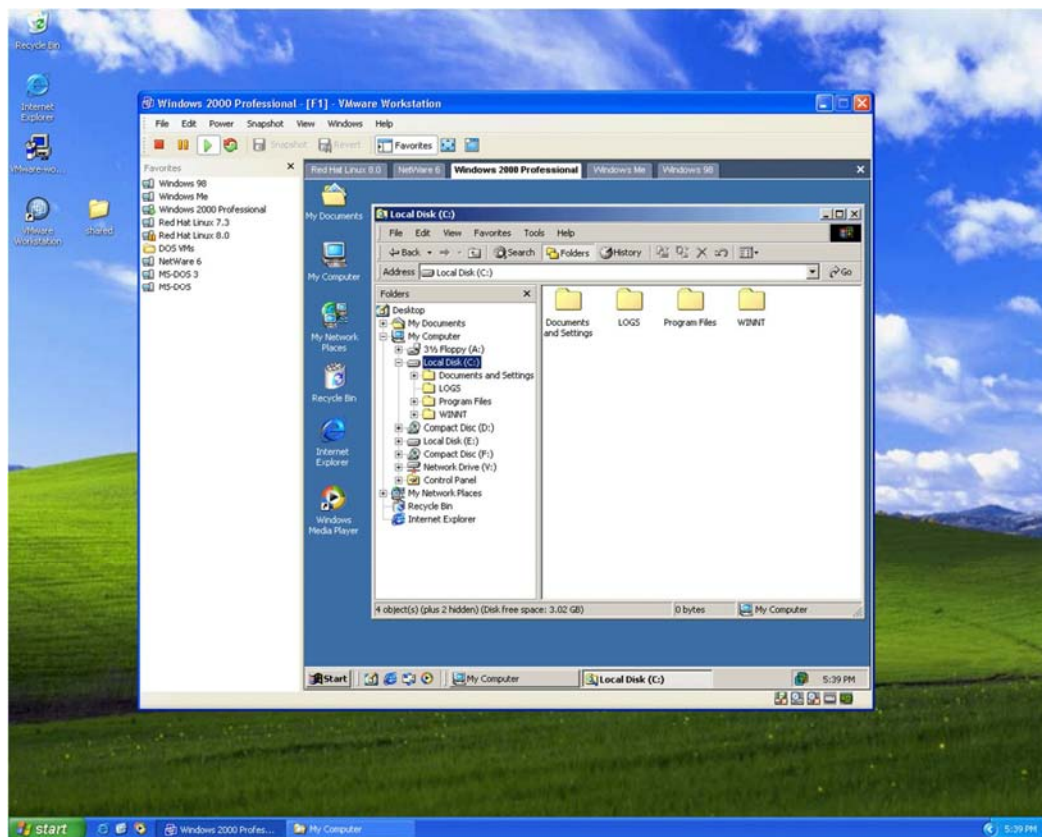
Na osnovu navedenog nije teško zaključiti zašto je u SAD procenat virtualizovanog dela infrastrukture datacentra vrlo visok - preko 40% (koji i dalje raste). Procene analitičara (Gartner, IDC) govore da za 2-3 godine neće biti fizičkog servera bez instaliranog hipervizora za virtualizaciju, te da će ovo dovesti do promene koncepcije operativnog sistema opšte namene i modela licenciranja softvera.

VMware - Radi se vodećem rešenju za virtualizaciju standardne x86-64 arhitekture, čije osnovne komponente predstavljaju:

- visokoproduktivni hipervizor ESX 3.0 (sa posebno optimizovanim mikrokernelom - VMkernel) - koji pruža 83-98% performansi nevirtualizovanih rešenja; ESX pored toga podržava širok spektar standardnog hardvera, od Intel i AMD procesora, do SAN, iSCSI i NAS podsistema diskova (fajlova), 10 Gb/s Etherneteta sa balansom opterećenja
- modul za centralizovan menadžment virtualnog data centra (ESX hostovi, resursi, licence, ovlašćenja, virtualne mašine) Virtual Center Management Server
- napredni opcioni moduli: podrška za multiprocesorske virtualne mašine sa dva ili četiri logička procesora - Virtual SMP; VMotion - tehnologija koja omogućava migraciju servisa (virtualnih mašina) u radnom stanju i bez prekida u radu sa jednog na drugi fizički host; distribuirani raspoređivač resursa (DRS), koji omogućava izbalansirano korišćenje resursa na hostovima u klasteru i migraciju servisa (korišćenjem VMotion) na manje opterećene hostove; restart servisa u slučaju otkaza hosta, na drugim hostovima — High Availability; konsolidovani bekap, koji omogućava bekap stanja virtualne mašine u zadatom trenutku i povratak u to stanje u slučaju otkaza
- alat za migraciju fizičkih servera u virtualni oblik i konverziju iz jednog formata virtualne mašine u drugi - Converter 3.0
- konsultantske usluge procene efekata virtualizacije (obračun RIO, TCO) - Capacity Planner
- usluge edukacije i sertifikacije zaposlenih u datacentru za primenu navedenih rešenja



Slika 13: Prikaz VMware Infrastrukture



Slika 14: Prikaz VMware Workstation konzole

Hyper-V - Windows Server 2008 je najbogatiji Windows Server operativni sistem do sada. Sa ugrađenim i unapređenim mogućnostima za Web i virtualizaciju, ovaj operativni sistem je dizajniran da poboljša pouzdanost i prilagodljivost infrastrukture servera, kao i da uštedi vreme i smanji troškove. Moćne alate obezbeđuju bolju kontrolu nad serverima i usmeravaju zadatke konfiguracije i upravljanja. Pored toga, unapređene bezbednosne funkcije ojačavaju zaštitu operativnog sistema, štite podatke i mrežu i obezbeđuju čvrstu, izuzetno pouzdanu osnovu za rad. Pomoću funkcije Hyper - V, Microsoft obezbeđuje platformu virtualizacije sa hipervizorom koja omogućava prilagodljivost zahvaljujući smanjenju troškova, boljem korišćenju hardvera, optimizovanoj infrastrukturi i boljoj dostupnosti servera.

Hyper-V, ključna funkcija sistema Windows Server 2008, jeste osnovna komponenta Microsoft strategije virtualizacije centra sa podacima na radnu površinu. Ostale komponente ove strategije uključuju:

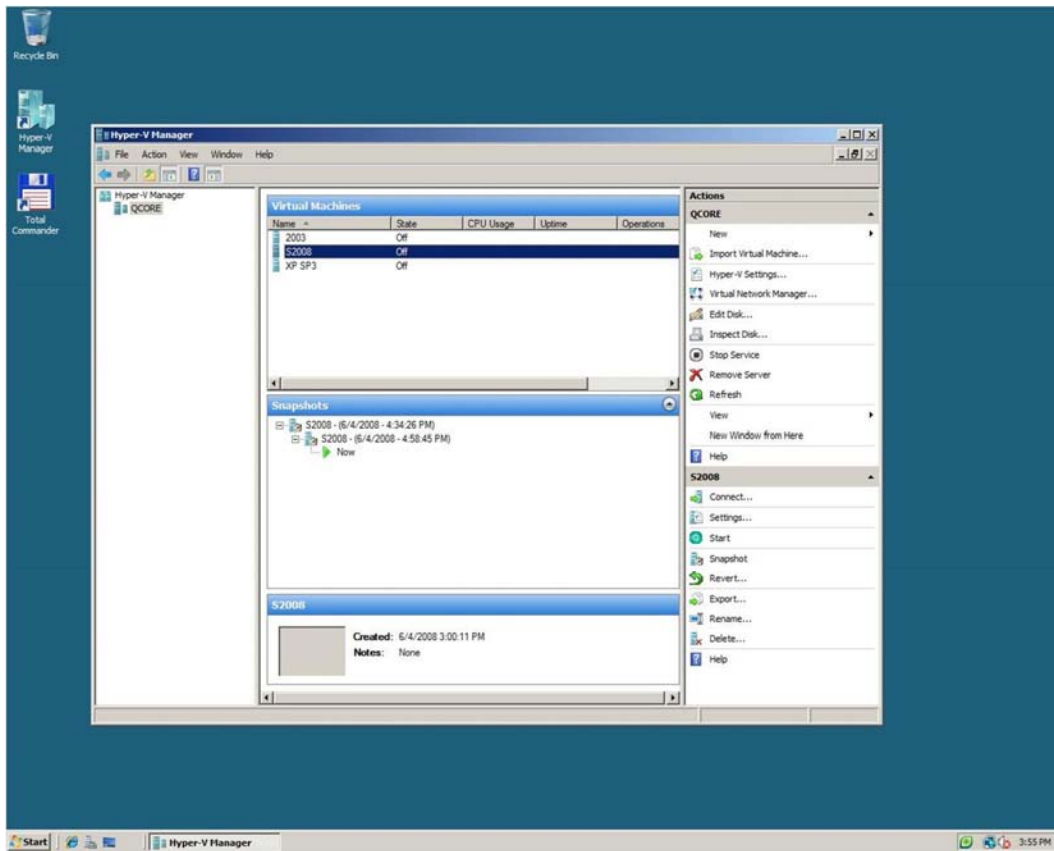
- Virtualizaciju prezentacije pomoću usluge Microsoft Terminal Services
- Virtualizaciju radne površine pomoću opcije Microsoft Virtual PC
- Virtualizaciju aplikacije pomoću opcije Microsoft SoftGrid

Ostale prednosti uključuju:

- Kontinuitet poslovanja i kontrola u slučaju pada sistema, čime se omogućava pouzdano poslovanje
- Testiranje i razvoj, koje omogućava testiranje u virtualnim okruženjima umesto na „živim“ računarima
- Prelazak na dinamički centar sa podacima, čime se optimizuje korišćenje servera i obezbeđuju sistemi koji se sami kontrolišu
- Kontrola poslovnih centara, čime se smanjuje potreba za lokalnim IT osobljem
- Smanju je se potrošnja električne energije kao i zagrevanje, optimizuje korišćenje resursa i omogućava administratorima mreže da se usredsrede na oblasti koje mogu da poboljšaju, umesto samo da izvršavaju rutinske zadatke. Time se štedi na osoblju, obuci i resursima.

Hyper-V je platforma za virtualizaciju koja obezbeđuju najveću moguću prilagodljivost zahvaljujući dinamičkim, pouzdanim i skalabilnim mogućnostima kombinovanim sa kompletnom integrisanim alatki za upravljanje fizičkim i virtualnim

resursima, što znači da možete da kreirate agilan i dinamički centar sa podacima i napredujete u pravcu dinamičkih sistema koji se sami kontrolišu. Hyper-V, ključna funkcija sistema Windows Server 2008, obezbeđuje povećanu pouzdanost, veću skalabilnost i dinamičke mogućnosti koje omogućavaju virtualizaciju većine poslovnih zadataka u okviru infrastrukture.



Slika 15: Prikaz Hyper-V menadžera u Serveru 2008

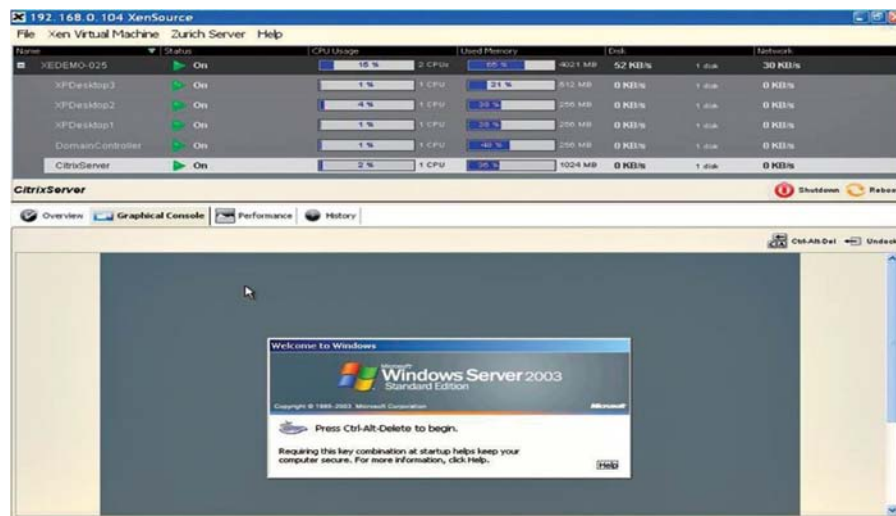
Ključne karakteristike funkcije Hyper-V:

- Nova i unapređena arhitektura. Zahvaljujući novoj arhitekturi sa 64-bitnim hipervizorom sa mikrojezgrom, funkcija Hyper-V nudi široki spektar metoda za podršku uređaja, kao i poboljšane performanse i bezbednost.
- Sveobuhvatna podrška za operativne sisteme. Sveobuhvatna podrška za istovremeno pokretanje različitih tipova operativnih sistema, uključujući 32-bitne i 64-bitne sisteme na različitim serverskim platformama, kao što su Windows, Linux i drugi.

- Symmetric Multiprocessors (SMP) podrška. Zahvaljujući podršci za najviše četiri procesora na virtualnoj mašini, možete u potpunosti da iskoristite aplikacije sa više niti na virtualnoj mašini.
- Raspoređivanje opterećenja na mreži. Hyper-V sadrži nove mogućnosti virtualnog prebacivanja. To znači da se virtualne mašine mogu jednostavno konfigurirati da koriste uslugu Windows Network Load Balancing (NLB) za raspoređivanje opterećenja na virtualnim mašinama na različitim serverima.
- Nova arhitektura deljenja hardvera. Zahvaljujući novoj arhitekturi virtualnog dobavljača usluga/klijenta virtualnih usluga (VSP/VSC), Hyper-V obezbeđuje poboljšani pristup i korišćenje osnovnih resursa, kao što su disk, umrežavanje i video.
- Brza migracija. Hyper-V omogućava brzu migraciju virtualne mašine sa jednog fizičkog sistema domaćina na drugi uz minimalni period van funkcije, kombinujući poznate mogućnosti dostupnosti sistema Windows Server i alatke za upravljanje usluge System Center.
- Snimak virtualne mašine. Hyper-V nudi mogućnost pravljenja snimka pokrenute virtualne mašine tako da se lako možete vratiti na prethodno stanje i unaprediti rešenje za pravljenje rezervne kopije i oporavak sistema.
- Skalabilnost. Sa podrškom za više procesora i jezgara na nivou domaćina i poboljšanom pristupu memoriji na virtualnim mašinama, sada možete virtualno skalirati okruženje virtualizacije da biste podržali veliki broj virtualnih mašina u okviru domaćina i nastavili da kombinujete brzu migraciju radi skalabilnosti na više domaćina.
- Proširivost. Windows Management Instrumentation (WMI) interfejsi i programski interfejsi aplikacije (API) zasnovani na standardima u funkciji Hyper-V nezavisnim prodavcima softvera i programerima omogućavaju da brzo kreiraju prilagođene alatke, uslužne programe i proširenja za platformu za virtualizaciju.

Kada se Hyper-V uloga omogući, Hyper-V Manager postaje dostupan kao deo administrativnih alatki. Pomoću opcije Hyper-V Manager korisnici mogu lako da kreiraju i konfigurišu virtualne mašine.

Xen virtualizacija - Kompanija XenSource ima dvostruku ulogu u razvoju paketa Xen za virtualizaciju. Osnovana je 2005. godine s ciljem da, s jedne strane, daje podršku razvoju open source projekta Xen koji je razvio Ian Pratt, jedan od osnivača XenSource-a. S druge strane, ova kompanija na bazi otvorenog rešenja razvija napredne verzije softvera namenjene preduzećima različitih veličina, nudeći im uz softver i dodatne usluge.



Slika 16: Prikaz Xen virtual menadžera

Kompanija je na bazi osnovnog Xen razvila tri verzije softvera za virtualizaciju. XenExpress je najjednostavnija varijanta, koja podržava pokretanje do četiri virtualne mašine, potpuno je besplatna. Nešto naprednija je verzija XenServer; na njoj je moguće pokrenuti do osam virtualnih mašina. Najnaprednije rešenje je XenEnterprise, robustan softver namenjen najzahtevnijim korisnicima. Uz godišnju pretplatu za dva snažnija rešenja, XenSource obezbeđuje i tehničku podršku za rešavanje svih zahteva korisnika Xen virtualizacije.

Iako ima ogromne mogućnosti, XenEnterprise se vrlo lako upotrebljava i omogućava brzo pokretanje gostujućih mašina zasnovanih na Windows i Linux operativnim sistemima. Koristeći dokazano rešenje za virtualizaciju, Xen hypervisor, on omogućava laku instalaciju sa CD-a ili sa mrežne lokacije, te donosi bezbednost Xen tehnologije za pokretanje x86 servera. XenEnterprise omogućava kreiranje neograničenog broja virtualnih mašina – jedino realno ograničenje su hardverski kapaciteti računara na kojem se ovaj sistem pokreće. I proizvođačima procesora, koji stalno dodaju jezgra i nove kapacitete, jasno je da sve to nije lako iskoristiti u

potpunosti, pa razvijaju i sopstvene tehnologije vezane za virtualizaciju, kakve su Intel VT i AMD Virtualization (AMD-V). Njih Xen u potpunosti podržava kroz paravirtualizaciju, a hardverska podrška virtualizaciji obezbeđuje izuzetne performanse virtualnih servera, tako da je njihovo vreme reakcije blisko nevirtualizovanim mašinama.

XenEnterprise omogućava lako konsolidovanje postojeće serverske infrastrukture, jednostavniji razvoj i testiranje softvera, „zakrpa“, pa i celih operativnih sistema. Omogućava i pokretanje starih operativnih sistema i aplikacija na novom hardveru, koji u osnovi pokreće najnoviji softver, kao i još mnogo različitih scenarija upotrebe kada je lakše koristiti virtualni prostor. Za svoj rad može da koristi do 16 GB RAM-a i najviše 32 procesora, koje deli između neograničenog broja virtualnih mašina, a najnovija mogućnost, dodata tokom drugog kvartala 2007, tiče se „žive“ migracije virtualnih servera i podrške klasterovanom deljenom sistemu za skladištenje podataka. Na Xen platformu moguće je instalirati Windows i Linux virtualne mašine. Podržani su Windows 2000, XP i Server 2003, te praktično sve GNU/Linux distribucije, uključujući Red Hat Enterprise Linux, Novell SuSE i Debian Sarge. Jedino ograničenje predstavlja činjenica da je za pokretanje Windows virtualnih mašina neophodna podrška za Intel VT ili AMD-V tehnologiju.



Slika 17: Prikaz rada Virtualnih mašina pod Xen virtualizacijom

Administratorima XenEnterprise nudi grafičku konzolu preko koje lako mogu pratiti i uticati na rad virtualnih mašina. Tu je moguće videti iskorišćenost kapaciteta hardvera i performanse virtualnih mašina, te ispratiti čitav životni vek virtualnih mašina – od kreiranja i pokretanja, preko startovanja i zaustavljanja, do rebootovanja i deinstalacije. Administratori mogu svaku virtualnu mašinu „u letu“ zaustaviti ili joj alocirati resurse kako se zahtevi menjaju. Xen rešenja se veoma brzo razvijaju i unapređuju. O tome svedoči i činjenica da krajem prošlog leta još nije bilo moguće pokrenuti Windows virtualne mašine, a danas to funkcioniše. To je garancija da će nove tehnologije koje hardver ponudi vrlo brzo dobijati podršku u Xen rešenjima.

PRIMENA REŠENJA DOBIJENIH VIRTUELIZACIJOM

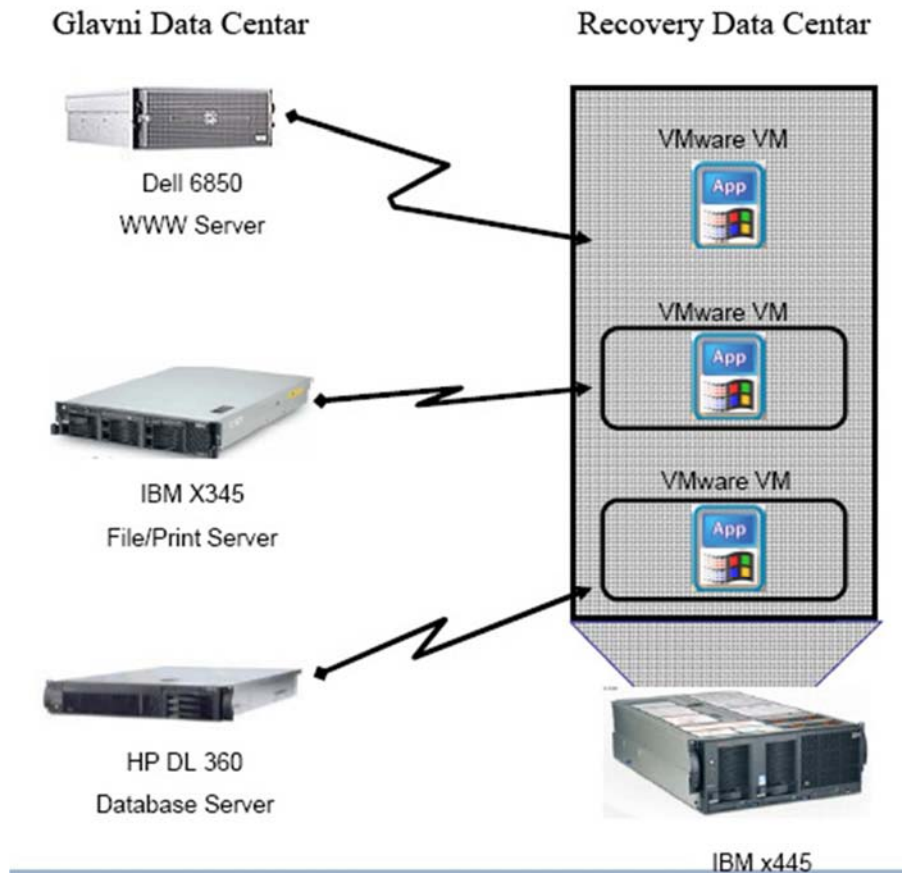
Sa razvojem kancelarijskih ogranaka u mnogim organizacijama, mnogi su shvatili da postoji problem vezan za autentifikaciju. Ogranci firmi obično dobijaju kontroler domena preko kojeg se korisnici mogu autentifikovati u lokalnom DC-u umesto da moraju da idu na spori, ili čak srušeni, WAN link, koji može da dovede do grešaka ili blokiranja autentifikacije i nemogućnosti da pristupite čak i lokalnim resursima.

Rešenje je bilo da se postave kontroleri domena u kancelarijskim ograncima. Iako je ovo rešilo inicijalni problem autentifikacije, javili su se bezbednsoni problemi. Pošto većina ogranaka kancelarija nema isti nivo IT stručnosti kao glavna kancelarija, a svakako nemaju isti nivo fizičke bezbednosti, kontroleri domena ogranaka kancelarija postaju veoma slabe tačke u čitavoj Active Directory infrastrukturi. Promene koje napravi nestručan korisnik u ogranku kancelarija može da ima efekte na čitavu organizaciju i ako neko ukrade DC u ogranku kancelarije, to potencijalno može da kompromituje sve naloge u organizaciji. Rešenje Windows Server-a 2008 je Read Only Domain Controller (RODC). RODC sadrži read only kopiju Active Directory baze podataka i jedine informacije o nalogima koje se skladište u RODC-u su za naloge u ogranku kancelarije. Pošto se nikakve izmene u Active Directory-ju ne mogu napraviti u RODC-u, ne postoji bojazan da će nestručni korisnik napraviti nepopravljivu štetu u Active Directory-u. I pošto obično nema administrativnih korisnika u ograncima kancelarija, postoji relativno mali rizik da će RODC u ograncima kancelarija posedovati naloge administratora koji se mogu kompromitovati u slučaju krađe RODC-a. RODC-ovi se takođe mogu konfigurisati da keširaju samo određene naloge. I u slučaju da se RODC ukrade, lista keširanih korisničkih naloga na RODC-u je dostupna kroz administraciju Active Directory-ja u glavnoj kancelariji. To omogućuje administratoru Active Directory-ja da isključi ili resetuje prava pristupa ovih naloga iz glavne kancelarije.

Kako ogranci najčešće nemaju razvijenu IT infrastrukturu, već se često njihovo poslovanje zasniva na jednom serveru a RODC je servis koji ne zauzima puno procesorskog vremena pa je njegovo pokretanje i predviđeno na virtuelnom računaru.

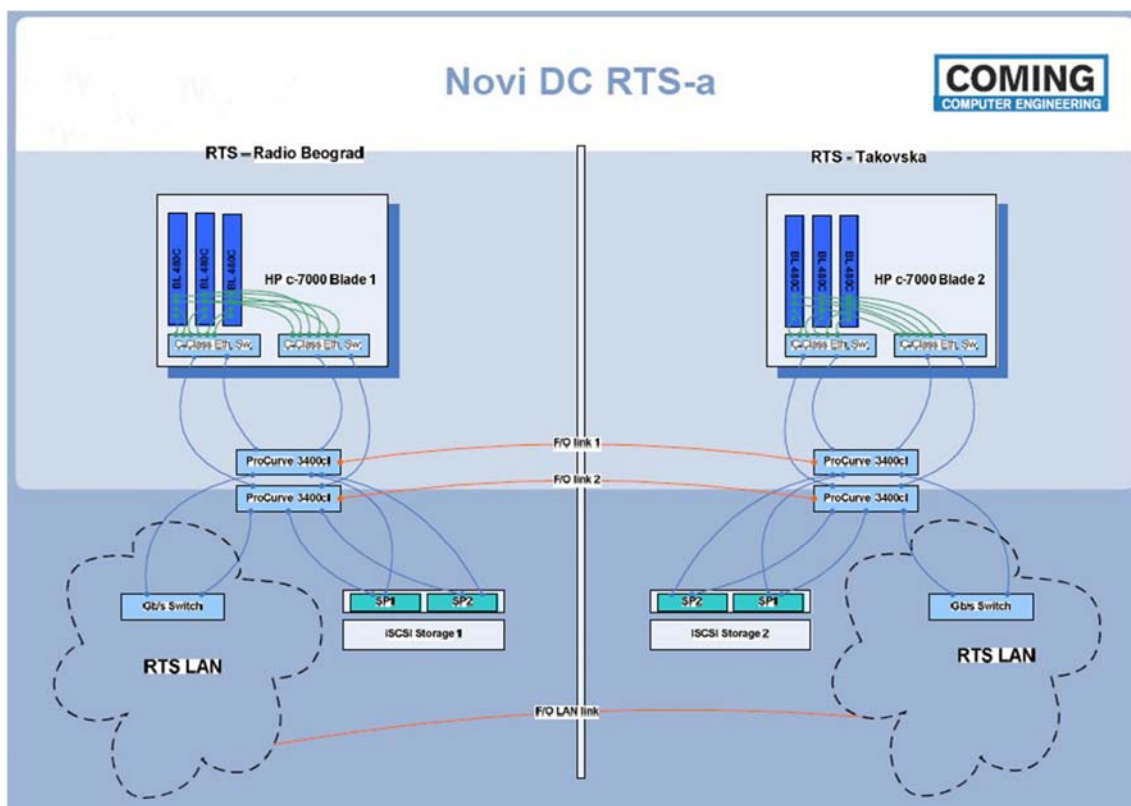
U ovom radu takođe ćemo obraditi i pojmove fail over clustera i gradnje recovery data centa, objasni ćemo principe na kome rade ali detaljna uputstva za njihovu implementaciju će ipak biti obrađena u drugom radu. Kao što smo u početku rada rekli gradnja dva fizička data centra bi bila izuzetno skupa i ekonomski ne isplativa, ali takođe je neverovatno sračunati i mogućnost gubitka svih podataka u

slučaju požara ili poplave u data centru. Ovakvi događaji ozbiljno bi uzdrmali i doveli u pitanje buduće poslovanje svake firme. Rešenje se javilo kroz virtualizaciju fizičkih servera iz primarnog data centra na udaljenu lokaciju na kojoj bi se nalazila jedna fizička mašina koja bi pokretala virtualne mašine da rade posao fizičkih u slučaju otkaza nekog od fizičkih računara iz primarnog data centra. Ovakvo rešenje predstavljeno je na sledećoj slici:



Slika 18: Prikaz virtualizacije fizičkog data centra na recovery data centar koji se nalazi na isturenoj lokaciji

Da virtualizacija nije samo još jedno od futurističkih rešenja koje se neće primenjivati u praksi već samo u teoriji govori i slučaj Evrovizije koja je odžana u Beogradu, a za čiji su se ne smetan radi sigurnost streeminga i podataka brinule upravo virtualne mašine i Blade serveri čiju je implementaciju izvršila firma Coming iz Beograda preko koje smo i dobili sledeću sliku koja predstavlja šemu RTSovg Data Centra u vreme održavanja Evrovizije:



Slika 19: Šema RTS data centra u vreme održavanja Evrovizije

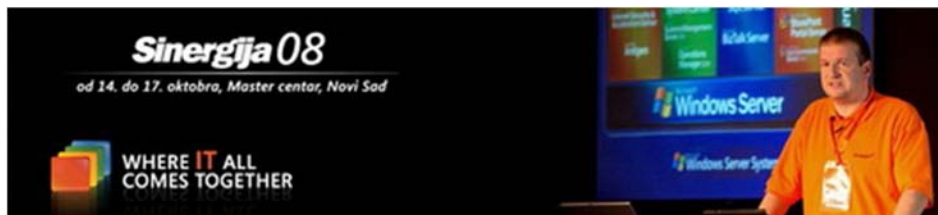
Po rečima direktora firme Coming Draga Samardžića sve je instalirano i svih 400 korisnika je definisano za svega 5 dana, a virtualno okruženje omogućilo je i da se tokom rada sistema manji broj ljudi angažuje na održavanju ukupno 200 računara koliko je korišćeno za vreme Evrovizije.

Bilo je potrebno napraviti sistem koji će obezbediti brz i pouzdan rad preko 600 korisnika istovremeno. Pored 200 tankih klijenata i 200 stonih računara, bilo je obezbeženo 100 lokacija za žično povezivanje prenosnih računara, kao i kapaciteti za preko 100 bežičnih konekcija. Za softversku osnovu sistema odabrano je VMware Infrastructure 3 rešenje za kreiranje virtuelnih hostova i virtuelnih računara, a za upravljanje virtuelnim mašinama korišćen je softver VMware VDM. Svi podaci kojima su korisnici pristupali smeštani su na dva NetApp FAS2020 iSCSI uređaja sa po 2,1 TB primarnog SAS prostora za podršku virtuelnim sistemima i 3,5 TB sekundarnog SATA prostora za pravljenje rezervnih kopija sistema, odnosno 11,2 TB ukupnog prostora. Za samo umrežavanje, upotrebljeni su Cisco ruteri i HP Procurve svicing oprema, dok je za srce sistema odabrana HP blejd platforma. Odlučeno je da se u dve šasije C7000, koje objedinjuju servere i interkonekciju, ugradi ukupno 6 HP Proliant BL480c servera, svaki sa po dva četvororojezgarna procesora na 3GHz i sa po 28 GB RAM memorije. Ovi serveri su od pokretanja radili preko 25 dana bez

prestanka i nisu prijavili niti jedan problem. Odabrano je rešenje sa dve šasije zbog kompletne redundanosti sistema (može da otkáže polovina napajanja i ventilatora za hlađenje a da sistem nastavi da radi normalno), kao i zbog toga što će ova platforma svoj životni vek nastaviti kao osnova IT sistema Radio televizije Srbije i rešenje za oporavak nakon katastrofalnog događaja (disaster recovery).

Microsoftovo rešenje virtualizacije Hyper-V našlo je praktičnu primenu baš za vreme Microsoftove konferencije Sinergija 08 koja je održana u Novom Sadu.

Akcent Sinergije 08 je stavljen na nekoliko oblasti, među kojima istaknutu poziciju zauzimaju predstavljanje novih proizvoda (novi Microsoft SQL Server ili Windows Server 2008), tehnologija virtuelizacije, koja je primenjena u praksi na ovogodišnjoj konferenciji, kao i mogućnosti integracije IT-ja i proverenih poslovnih modela koje će biti predstavljene kroz IT Management oblast predavanja, i modeli uspešne primene postojećih proizvoda i rešenja. Jedan od ključnih tehnoloških noviteta ove jeseni, Microsoft Hyper-V rešenje za virtuelizaciju, predstavljaće okosnicu informatičke infrastrukture Sinergije 08. Sve računare na konferenciji koji će biti dostupni učesnicima, novinarima i osoblju konferencije, će pokretati virtuelizovani operativni sistemi, a u srcu informatičkog sistema će se koristiti virtuelizovani serveri i aplikacije. Kroz laboratorije nazvane „Virtualization Workshop“ posetioći će moći da se bliže upoznaju sa teorijskim postavkama ovog koncepta, ali i da se na licu mesta upoznaju sa realnim sistemom koji koristi Hyper-V rešenje.



Slika 20: Najava za Sinergiju 08

Ovako je izgledala najava za Sinergiju 08, a u Master centru Novog sada korišćeno je preko 150 radnih stanica koje se zasnivalo na tankim klijentima i virtualnim računarima koji su radili na osam HP Blade servera pod Windows Server 2008 Enterprise operativnim sistemom.

ALL IN ONE DATACENTRI

Savremeno preduzeće male ili srednje veličine (Small and Medium Business) danas u pogledu IT usluga zahteva istu pažnju isporučilaca IT opreme i rešenja kao i tzv. „velika“ preduzeća. Imajući u vidu da, mereno u Internacionalnim razmerama, kod nas postoji mali broj velikih preduzeća (sa godišnjim prihodom koji prevazilazi 200 miliona evra prema SAP klasifikaciji), praktično svi isporučioци IT rešenja su upućeni na SMB segment (ako izuzmemo individualne korisnike).

Specifičnosti SMB segmenta IT usluga se mogu najbolje sagledati kroz analizu izazova i ograničenja sa kojima se ta preduzeća su oćavaju u pogledu uvođenja i korišćenja IT servisa. Navešćemo samo neke:

- broj i složenost servisa sličnog reda kao i kod velikih preduzeća
- (EERP rešenja, rešenja za komunikaciju i kolaboraciju, bezbednost itd.)
- učestali („hitni“) zahtevi za brzom i ekonomičnom implementacijom novih servisa
- potreba da se za nove servise nabavi i ova oprema ogranićen obim i kvalitet interno raspoloživih ljudskih resursa IT-u
- nedostupnost i neekonomičnost outsorsing rešenja
- dug period implementacije ovih rešenja (usluga)
- sve manja tolerancija neraspoloživosti servisa
- nedovoljan IT budžet (posebno u domenu investicija)

Mnogi od navedenih problema u IT uslugama su svojstveni svim SMB preduzećima iz vrlo jednostavnog razloga: da bi opstala ova preduzeća sve svoje resurse moraju usmeriti u jezgro svog poslovanja („core procesi“). Zato bi svako sveobuhvatno IT rešenje za SMB segment trebalo da poseduje: jednostavnost, prilagodljivost, potpunu automatizaciju operacija, obezbeđenu neprekidnu podršku, sigurnost i bezbednosti, iznad svega, ekonomičnost i isplativost u kratkom roku (8 meseci).

Polazeći od navedenih pretpostavki i ogranićenja, HP je dizajnirao jednostavno, prilagodljivo i ekono-mično rešenje nazvano All-In-One Datacentar. Osnovna ideja se sastoji u tome da se složenost IT infras-trukture (hardver, softver) sakrije od korisnika primenom Microsoft Hyper V infrastrukture, a da se korisnički servis i isporučuju u virtuelizovanom obliku i da su prethodno potpuno prilagođeni zahtevima korisnika. Ovakvo rešenje obezbeđuje potpunu hardversku nezavisnost korisničkih servisa, što za posledicu ima znaćajno pojednostavljenje IT infrastrukture, laku nadgradnju i održavanje, te vrlo visoku raspoloživost svih korisničkih servisa.

S druge strane, korisnički servisi se isporučuju u obliku koji je najpodesniji, najjednostavniji i najjeftiniji za korisnika. Sav aplikativni softver (servisi) se instalira na apstraktan (virtuelni) hardver, na operativnom sistemu iz koga su isključeni svi nepotrebni servisi (moduli). Isporučilac rešenja, s druge strane, dobija rešenje koje se lako i jeftino može održavati. Novi korisnički servisi se isporučuju u obliku fajlova (virtuelnih diskova), bilo udaljenim pristupom ili korišćenjem jeftinih medija (CD/DVD, flash memorijski stik).

U svom izvornom obliku All In One DC podržava sledeće servise:

- aktivni direktorijum (DNS infrastruktura)
- antivirusni server (servis)
- internet proksi servis
- internet fajervol servis
- e-mail servis
- servis za kolaboraciju i kreiranje sadržaja (wiki, blog)
- fajl i print servisi
- ERP rešenje (trenutno Microsoft Dynamics AV 4)
- CRM (open source, Microsoft CRM)
- interno pretraživanje sadržaja dokumenata (IBM Omni Find)
- upravljanje dokumentima (i radnim tokovima)
- podrška za bežično umrežavanje
- IP telefonija
- Video nadzor
- Registracija radnog vremena
- DBMS servisi (kao osnova za druge aplikativne servise; Microsoft SQL Server, Oracle)
- Virtuelne korisničke računare

Infrastruktura koja čini sistemsku podlogu za ove servise se sastoji od sledećih komponenti:

- Windows Server 2008 Datacenter
- dva HP DL360 servera (dva procesora sa po četiri jezgra) sa ESX hipervizorom
- HP DL 360 server za menadžment virtuelne infrastrukture i bekap
- HP Ultrium urdeaj za bekap na LTO trake
- gigabitni mrežni komutator

Kao podsistemi diskova nude se dva rešenja:

- SAN HP MSA 1500 sa SATA diskovima (kapaciteta 6 TB!), Brocade SAN komutator
- HP All inOne 400 pod sistem diskova u NAS konfiguraciji (do 1TB)
- backup softver Vizioncore ESX Ranger
- za mobilne korisnike prenosivi sanduci za instalaciju opreme.



Slika 21: Fizički izgled All in One Datacentra sa SAN konfiguracijom.

Pored osnovne namene, objašnjene u prethodnom tekstu, All in One DC se lako može prilagoditi za mobilne korisnike: sajmovi, kongresi, vojska, policija, zdravstvo i si, kao i za oporavak u slučaju nezgode („disaster recovery"). Rad i obezbeđenja još veće ekonomičnosti, isto rešenje za rezervni DC može koristiti više preduzeća.

OPORAVAK SISTEMA NAKON KATASTROFE

Disaster recovery je proces oporavka pristupa podacima hardveru i softveru neophodan za nastavak kritičnih poslovnih procesa nakon prirodne ili katastrofe izazvane ljudskim faktorom.

Obezbediti kontinuitet poslovanja (Business Continuity) u svim uslovima od esencijalnog je značaja -posebno u današnje vreme. Ozbiljnost jednog preduzeća reflektuje se sa više aspekata, ali je jedan od primarnih upravo predanost i volja menadžmenta ka planiranju, razvoju i finansiranju rešenja za oporavak nakon eventualne katastrofe.

U tom pogledu skala rešenja ima veliki raspon: od gotovo nikakvog do potpune redudanse zvane "duplirajmo sve". No, kako doći do efikasnog, optimalnog i prilagođenog, rešenja?

Odgovor je, inicijalno, u konstantnoj opservaciji kompletnog sistema i svih raspoloživih resursa. Prvo morate razumeti kako normalni procesi u poslovanju mogu biti narušeni ili uništeni, jer bez jasne slike kako će se potencijalni udar odraziti na poslovne aktivnosti, ne možete steći jasnu sliku o neophodnim aktivnostima za vreme i nakon katastrofe.

Finansijski, iako menadžmentu najrazumljiviji, samo je jedan od efekata i posledica katastrofe. Ostali, koji se mogu odnositi na ljude ili okruženje, sliku u javnosti, politiku ili zakonske posledice, mogu imati daleko snažniji uticaj.

Statistika ukazuje na činjenicu da samo 6% preduzeća, koja pretrpe ozbiljan udar nastave da posluju, 94% doživi krah, nakon manjih (kratkotrajnijih) padova, 40-50% nastavi sa poslovanjem, te možemo red da je sveukupno 10% preduzeća pripremljeno za dugoročnije udare.

Planiranje oporavka (Disaster Recovery planning), kao deo šireg planiranja neprekidnosti poslovanja (Business Continuity Planning) dugotrajan je, zahtevan i jako bitan proces. Za početak treba jasno definisati sve komponente poslovanja, zatim precizno, uključujući i statistiku praćenja sistema, definisati odnos troškova planiranja i održavanja rešenja prema troškovima pada sistema, razmotriti moguće vrste rizika, a potom tražiti adekvatno rešenje. Takvo rešenje, naravno, mora biti efikasno, prilagodljivo i mora se konstantno razvijati - naročito u pogledu skraćivanja vremena nedostupnosti sistema, smanjenja troškova održavanja, povećanja brzine odziva, povećanja sigurnosti i si., a sve sa jasnim ciljem da se drastično smanji rizik narušenosti poslovanja. Planiranje, kao takvo, mora biti sastavni deo biznis plana svakog preduzeća, koje drži do svog renomea.

Kompleksnost rešenja srazmerna je kompleksnosti samog poslovanja. Da li će korisnici sami razviti svoje rešenje ili će se oslanjati na već gotova, njihova je dobra procena. No, ne sme se izgubiti iz vida da vrhunski svetski stručnjaci u renomiranim kompanijama rade na takvim rešenjima decenijama i postižu fantastične rezultate kreirajući rešenja kojima, s obzirom na pouzdanost, raspoloživost i nivo implementacije, odnos price/performance nema premca.

U žiži interesovanja danas, svakako je IT Disaster Recovery, sa posebnim osvrtom na datacentar. Takva rešenja i njihov dalji razvoj jednostavno su nezaobilazna. Porast broja i vrsta servisa upravo je ekvivalentan obimu hardware-a koji treba da ih podrži, sa jedne, a sa druge strane iskorišćenost hardware-a je procentualno sve manja. Optimizacija je sveobuhvatan i delikatan proces, te se trend sa enormnom tendencijom rasta, virtuelizacija, svim svojim karakteristikama i prednostima nameće kao deo tog rešenja.

Korišćenjem Microsoft Hyper-V infrastrukture moguće je podići efikasnost korišćenja IT resursa na 60 -80% (približno kao u mainframe okruženju). Pri tome je broj fizičkih servera, kako pokazuju slučajevi mnogih od preko 20.000 korisnika, moguće smanjiti za 8-30 puta.

Ako se osvrnemo i na drastično smanjenje potrošnje energije za napajanje i hlađenje data centra, uzrokovano konsolidacijom, povećanjem gustine virtuelnih mašina, kao i smanjenjem veličine prostora, nužno do-lazimo do zaključka kolika je upotrebna vrednost jednog ovakvog rešenja za Business Continuity/Disaster recovery.

IMPLEMENTACIJA HIPER-V REŠENJA

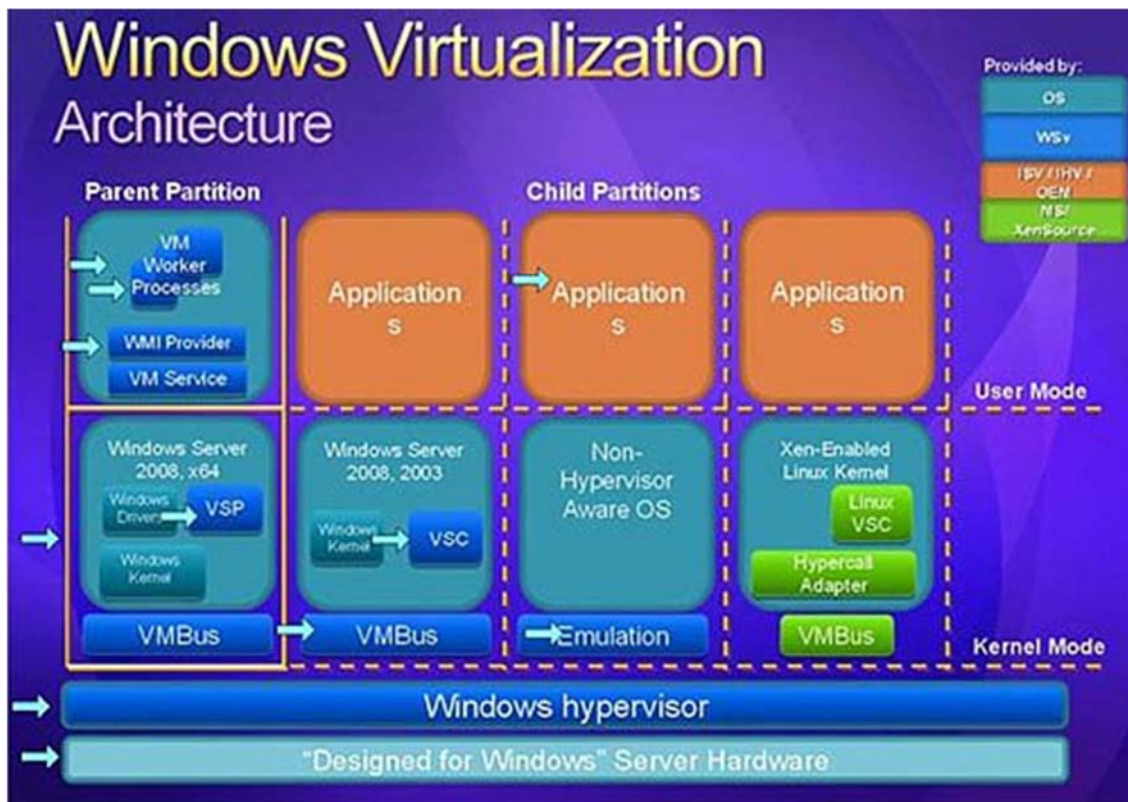
Virtualizacija je trend koji je u protekloj godini zabeležio gotovo najveći rast kada je u pitanju prihvatanje među korisnicima, kako poslovnim tako i običnim.

Na polju virtualizacionog softvera prisutne su brojne kompanije koje nastoje da osvoje što bolju poziciju kada je u pitanju broj korisnika koji će koristiti njihovu tehnologiju. Virtualni računari imaju potrebu za operativnim sistemom na kojem će raditi, a nedavno istraživanje Saga Research-a ukazuje da je u trenutnom talasu virtualizacije operativni sistem koji se najviše koristi Windows.

Sega Research je odeljak firme Chadwik Martin Bailey koja radi istraživanja u raznim oblastima tržišta. Istraživanje Sage Researcha sprovedeno među provajderima tehnoloških usluga i profesionalnih korisnika tehnologija je ukazalo da 96% ispitanika koristi Windows operativni sistem na svojim virtualnim serverima. Mnogi od korisnika koriste više od jednog brenda operativnog sistema za pokretanje svojih virtualnih računara.

Iza Windows-a sledi Linux, obzirom da 52% ispitanika koristi ovaj open source operativni sistem. Unix se nalazi na trećem mestu sa 30% zastupljenosti, dok je Solaris četvrti sa 29%. Ove cifre naravno ne daju ukupnu brojku od 100% zbog toga što pojedini korisnici na svojim serverima koriste dva ili čak i tri od nabrojanih operativnih sistema. Mac OS koristi 12% ispitanika dok NetWare zauzima skromnih 6%.

Ovo istraživanje je samo dalo grubu sliku o operativnim sistemima na kojima su bazirani virtualni serveri. Kompanija koja je radila istraživanje nije obezbedila podatke o tome koliko virtualnih računara i koje vrste radi na virtualizovanim serverima niti koje virtualizacione softvere koriste. Ali sa druge strane, iako su dosta površni, ovi rezultati ukazuju na to da je Microsoft iako je kasnio sa svojim Hyper V hypervisor-om na tržištu ipak uspeo više nego uspešno da se ukrca na voz virtualizacije.



Slika 22: Šematski prikaz rada virtualizovne arhitekture

Hyper-V radi pomoću tri osnovne komponente: hipervizor, virtualizaciona grupa i novi virtualizovani I/O model. Windows hipervizor u osnovi radi tako što kreira različite „particije“ za svaki virtualizovani slučaj koda pod kojim će raditi. Virtualizacione grupe i I/O komponente obezbeđuju interaktivnost sa samim Windows-om i sa različitim particijama koje su kreirane. Sve tri pomenute komponente rade zajedno. Korišćenjem servera opremljenih procesorima kao što su Intel VT- ili AMD-V, Hyper-V interaguje sa hipervizorom, koji u stvari predstavlja veoma mali deo softvera koji je prisutan direktno u procesoru.

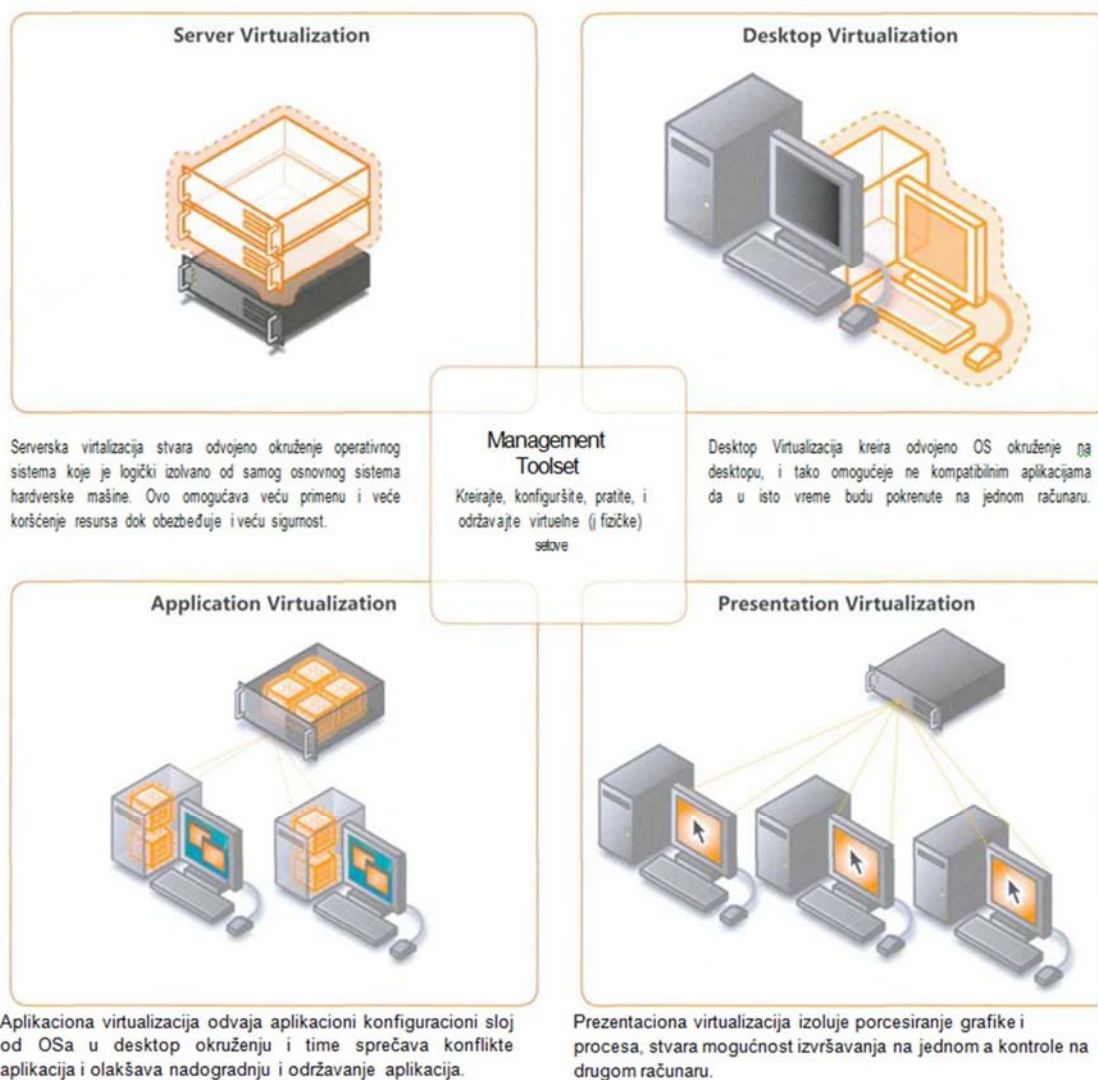
Ovaj softver se uvlači u nizove na procesoru koje host operativni sistem može da koristi za efikasno upravljanje višestrukim virtualnim sistemima, koji rade na pojedinačnom fizičkom procesoru. Obzirom da u ovom slučaju nema softvera niti driver-a drugih kompanija koji treba da se instaliraju kompatibilnost je gotovo zagarantovana. Zajedno sa efikasnošću upravljanja procesom, virtualizacija omogućava i dodavanje resursa bez isključivanja sistema. Od procesora do memorije i od mrežne karte do dodatnih medija za skladištenje možete dodavati uređaje bez potrebe za isključivanjem sistema.



Slika 23: Ilustrovani prikaz uštede korišćenjem virtualizacije

Možete virtualizovati migraciju, uštedeti novac koji biste potrošili na troškove razvoja i zatim proceniti koliko fizičkih mašina je potrebno da biste završili migraciju. Ideja virtualizacije nije samo snižavanje troškova, već i kreiranje servisa koji ne bi bili mogući na virtualizovanim serverima. U ovom kontekstu Hyper-V uključuje podršku za clustering širom višestrukih gostujućih operativnih sistema. Takođe možete da iskoristite prednosti nove disk kvorum karakteristike u Windows Serveru 2008, koja omogućava da imate clusterne na višesturkim lokacijama – recimo na različitim kontinentima.

Na sledećoj slici nalazi se primeri primene Microsoft Hyper-V virtualizacije:



Slika 24: Mogućnosti primene Microsoft Hyper-V tehnologije

POSTUPAK IMPLEMENTACIJE I VIRTUALIZACIJE POMOĆU HYPER-V HIPERVIZORA

Za potrebe istraživanja i rada koristili smo dve računara zasnovana na Intel Quad Core procesorima opremljenih sa 8GB radne memorije, na ovim računarima podigli smo četiri virtualna računara, svakom računaru smo dodelili po jedan fizički procesor, i različite količine memorije, sve virtualne mašine su koristile isti mrežni adapter koji je bio virtualizovan za svaku virtualnu mašinu ponaosob.

Konfiguracija računara koju smo koristili pri testiranju:

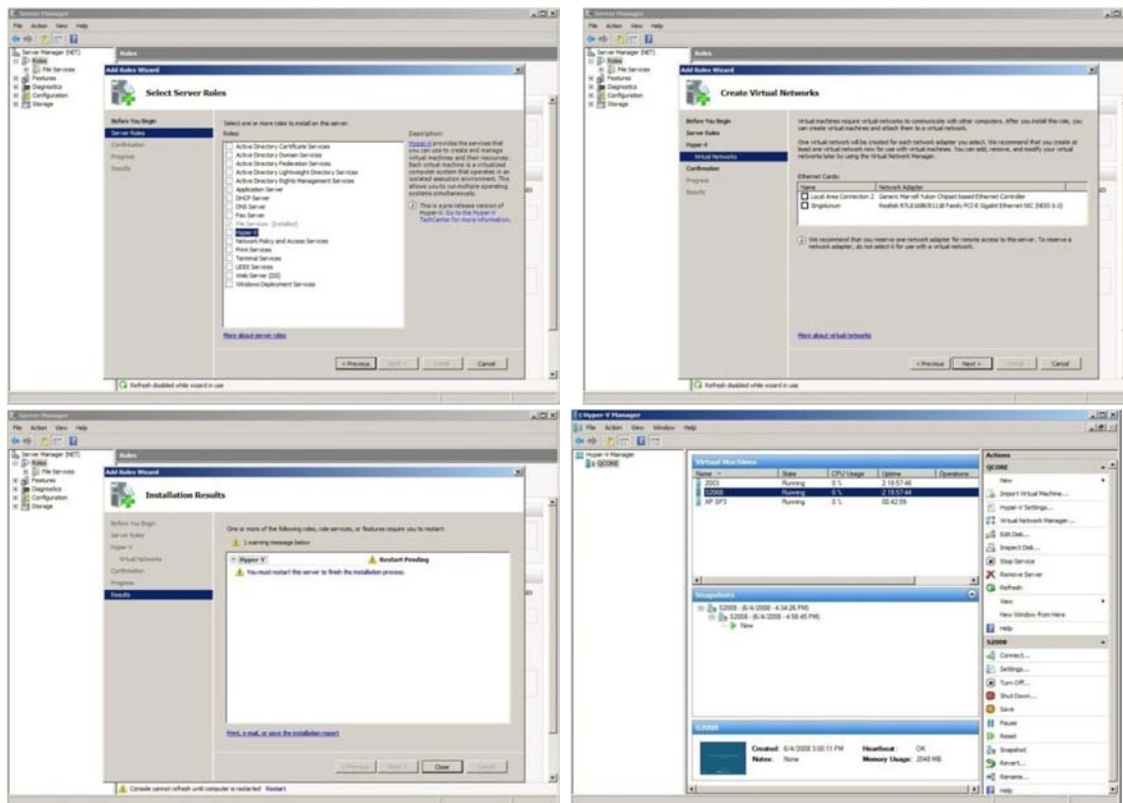
Matična ploča	<i>Gigabyte GA-P35-DS3R</i>
Procesori	<i>Intel Core 2 Quad Q9300</i>
Memorija	<i>4 X 2 GB Kingstone DDR2 800MHz</i>
Grafička karta	<i>N-VIDIA 8500GT</i>
Hard disk	<i>2x WD Caviar 320Gb/WD3200JS, 7200rpm, 8MB</i>
Opički uređaj	<i>Pioneer 115D</i>
Napajanje	<i>Chieftec 700W</i>

Postupak instalacije i konfigurisanje

Na pomenutom računaru podigli smo najnoviji Microsoft-ov serverski operativni sistem Windows 2008 Enterprise x64, takođe smo podigli i sve potrebne drajvere. Jedino se uz x64 verziju Servera 2008 može koristiti Hiper-V što je u neku ruku i logično pošto 32bitna verzija ima problema sa ograničenjem ram memorije na 3 GB što je nedovoljno za ozbiljan rad sa virtualnim mašinama. Koliko će virtualnih mašina moći istovremeno da bude aktivno na jednom fizičkom serveru uglavnom zavisi od količine memorije i svodi se na princip što više memorije to bolje. Procesori se dinamički dele tako da isti procesor možete dodeliti na više različitih virtualnih mašina, hard diskovi se takođe kreiraju virtualno tako da možete kreirati virtualni hard disk u vidu virtualne slike od 2000GB na fizičkom disku veličine 80GB, disk će se popunjavati dinamički a kada se stvori potreba za prostorom preko 80GB sliku je moguće raširiti na više fizičkih diskova ili čak i preko mrežnih diskova tako da stvarno dobijete korišćenje diska od 2000GB za koga virtualna mašina ili njeni korisnici neće ni biti svesni da rade na virtualnom disku ili mašini. RAM je jedina komponenta koja

se ne deli dinamički i koja se mora definisati unapred, naravno moguće ga je dodavati i oduzimati virtualnim mašinama, ali nije moguće da ga više različitih mašina koristi dinamički kao što je to slučaj sa hard diskovima ili procesorima.

Hiper-V se u Windows Serveru 2008 javlja kao jedna od rula koju treba aktivirati, postupak je krajnje jednostavan, i nudi vrlo malo prostora za grešku administratora, praktično jedi izbor koji se pred administratora postavlja je izbor koji će se mrežni adapter koristiti pri kreiranju virtualnih mrežnih adaptera tj. preko kog adaptera će virtualne mašine komunicirati sa fizičkom mrežom, postupak instalacije može se videti na paru screenshotova koji slede:



Slika 25: Postupak instalacije Hyper-V menadžera

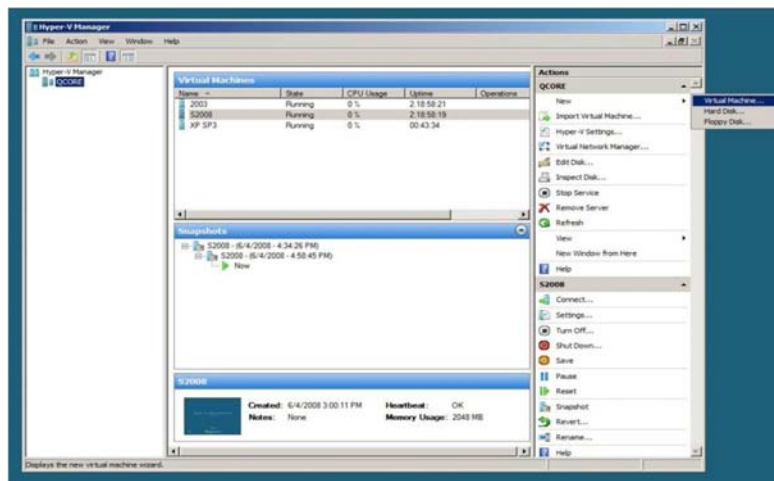
Po završetku instalacije role server će zatražiti da bude restartovan kako bi finalizovao instalaciju i nadogradio komponente, već pri sledećem startovanju servera javiće se Hyper-V menadžer pomoću koga se manipuliše sa virtualnim mašinama (izgled Hyper-V menadžera vidi se na poslednjem od četiri screenshota koji su priloženi na ovoj strani).

U Hyper-V menadžeru moguće je:

- Definirati virtualne hard diskove
- Definirati virtualne mrežne adaptere
- Povezivati virtualne mrežne adaptere
- Kreirati virtualne mašine, snapshot-ovi
- Manipulirati sa virtualnim mašinama
- Povezivati (klasterovati) virtualne mašine, uključivati monitoring i heartbeat opcije
- Povezivati virtualne mašine koje se nalaze na jednoj fizičkoj mašini sa virtualnim mašinama drugog fizičkog računara
- Učitavati virtualne mašine sa drugih fizičkih računara
- Kreirati virtualne mašine od fizičkih računara

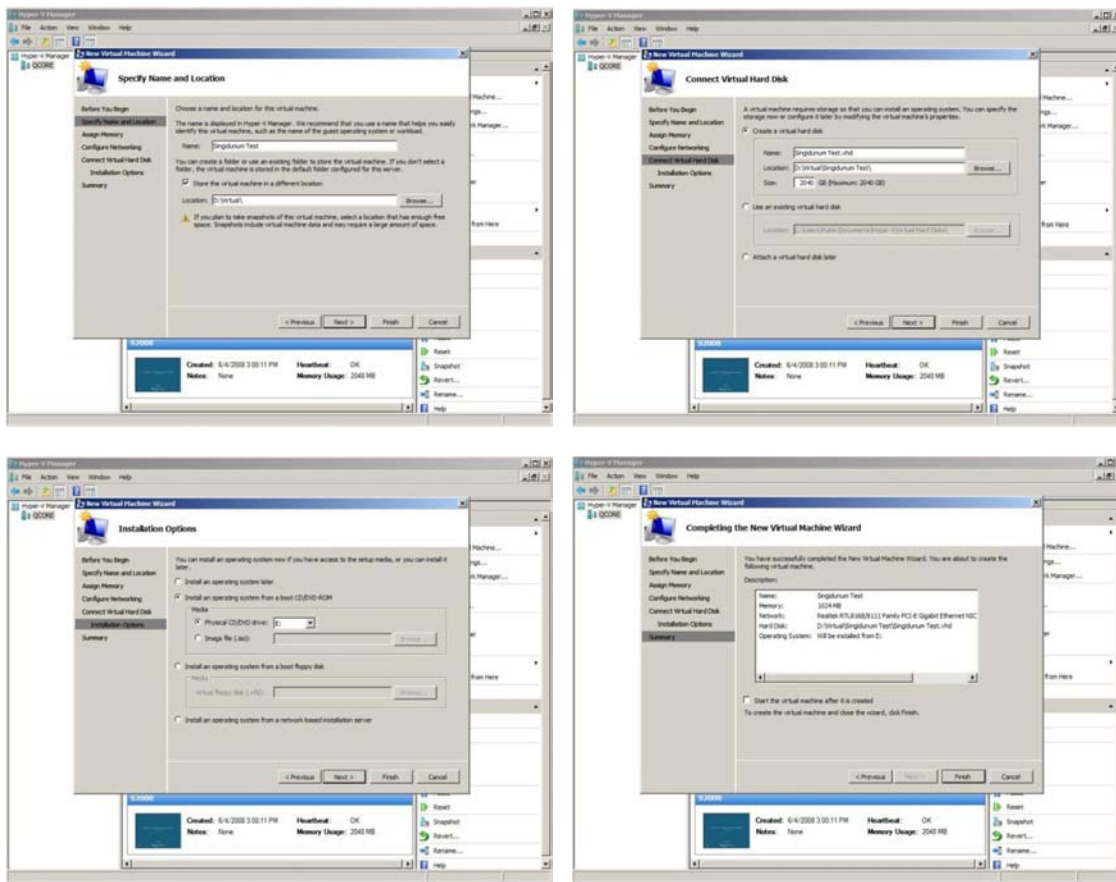
Proces kreiranja virtualne mašine

Iz Hyper-V Manager-a izabere se opcija New Virtual Machine, nakon čega se pojavljuje wizard koji dalje vodi administratora kroz proces kreiranja virtualne mašine i izbor fizičkih resursa koje će ova virtualna mašina koristiti.



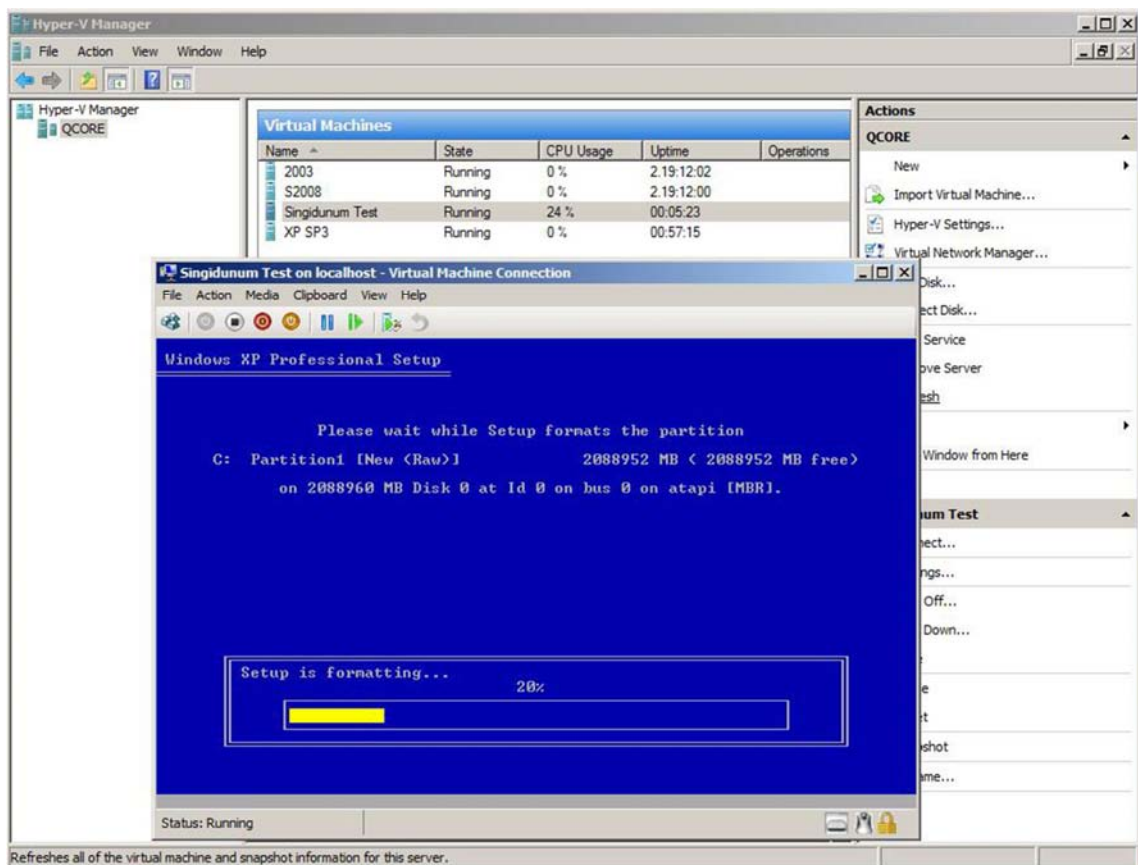
Slika 26: Hyper-V menadžer i kreiranje nove virtualne mašine

Kroz dalje menije, vrši se podešavanje uređaja virtualne mašine, određuje se koliko će hard diska, memorije i procesora koristiti virtualna mašina, menije kroz koje administrator prolazi pri kreiranju virtualne mašine prikazani su na sledećim slikama:



Slika 27: Postupak kreiranja virtualne mašine

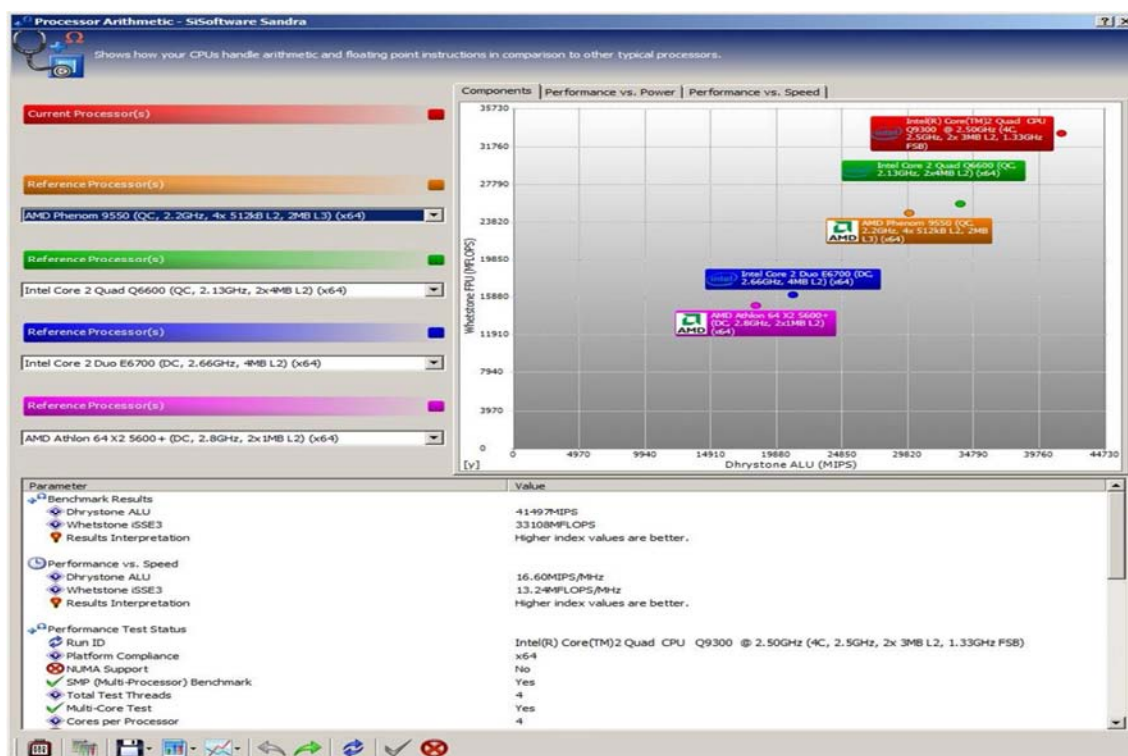
Sama instalacija operativnog sistema na virtualnoj mašini se odvija isto kao što bi se odvijala i na fizičkom računaru osim što se u ovom slučaju odvija u prozoru fizičkog računara, izgled i tok instalacije operativnog sistema na virtualnoj mašini, kao i opterećenost celog sistema fizičke mašine pri radu četiri virtualne mašine može se videti na sledećoj slici:



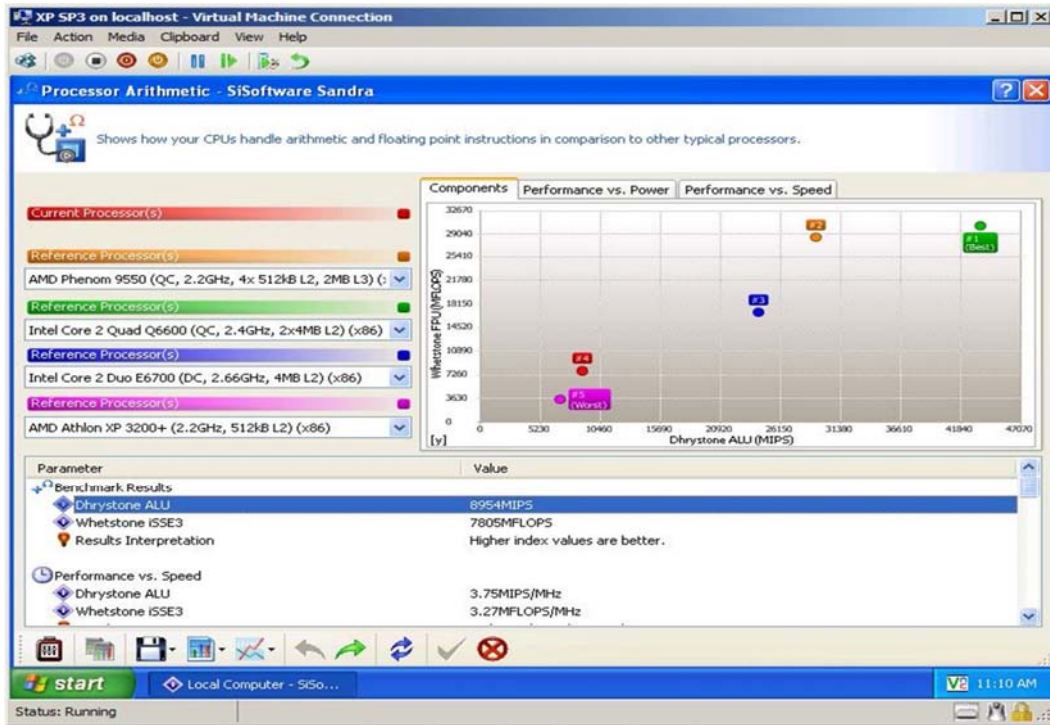
Slika 28: Hyper-V menadžer i postupak instalacije Windows XP operativnog sistema pod virtualnom mašinom

Rezultati testiranja

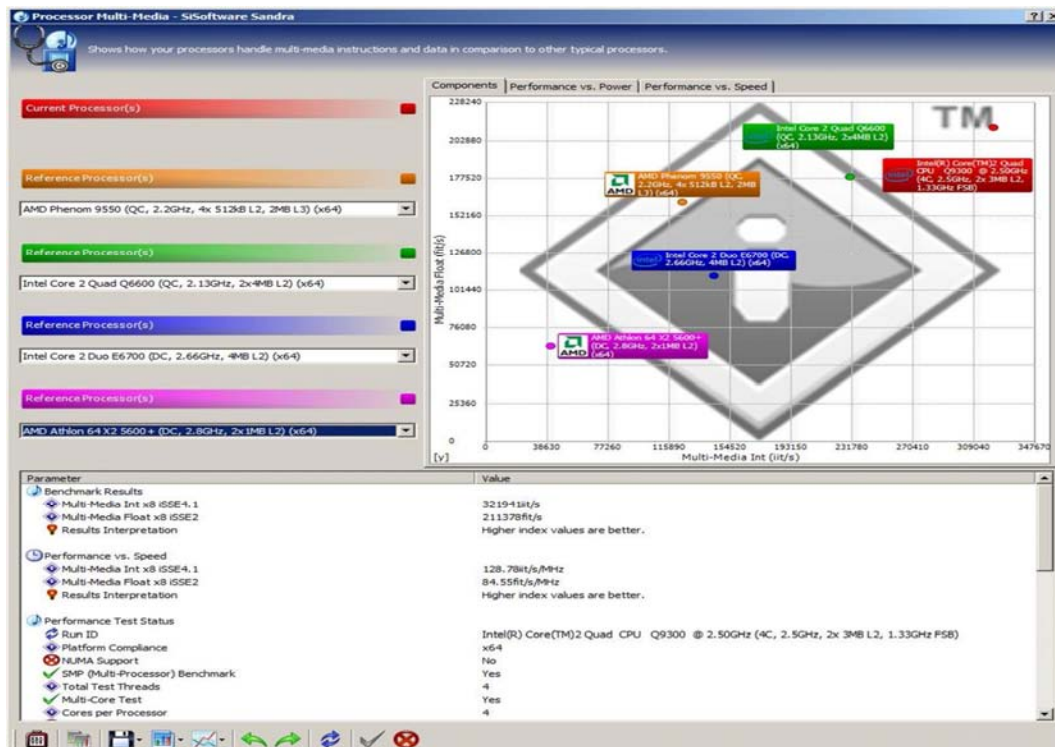
Na sledećim stranama nalaze se rezultati testiranja i poređenja fizičkih računara sa virtualnim mašinama, testirali smo pomoću programa SiSoftware Sandra kao i pomoću 3D rendering test programa Cinebench R10. Testirali smo i poredili brzine procesora pri aritmetičkim i multimedijalnim operacijama, takođe smo testirali brzine memorija i hard diskova u fizičkom i virtualnom okruženju. Sve dobijene rezultate poredili smo i sa referentnim sistemima pa su i njihovi rezultati predstavljeni na grafikonima koji slede.



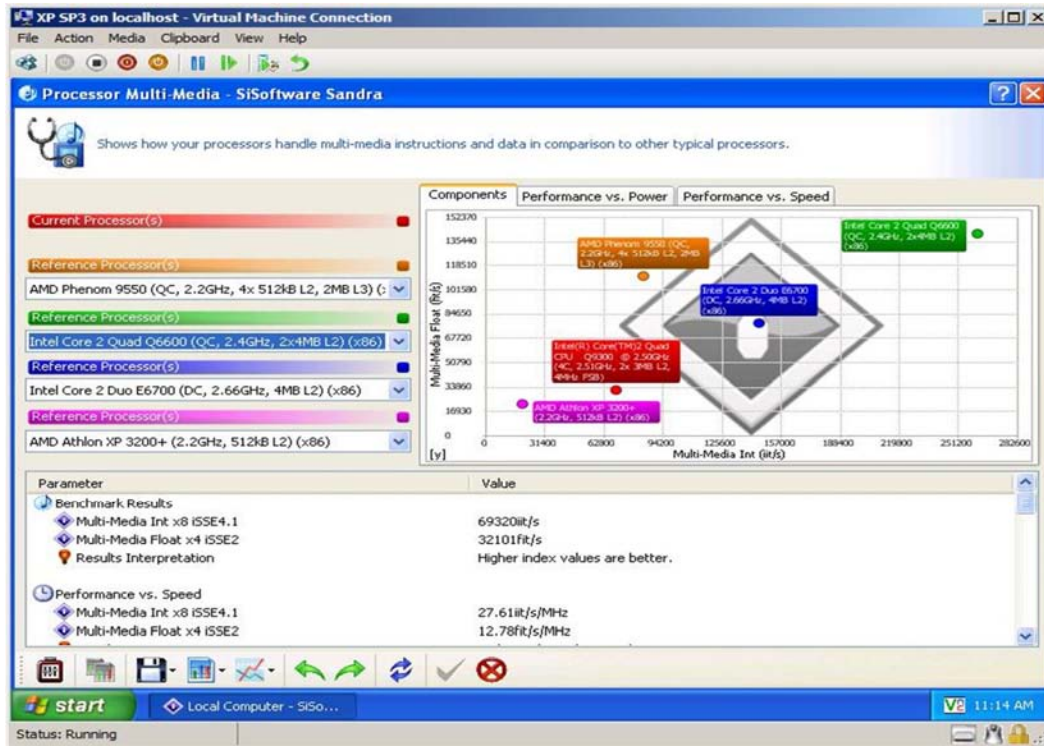
Slika 29: Fizički računar, test aritmetičkih operacija



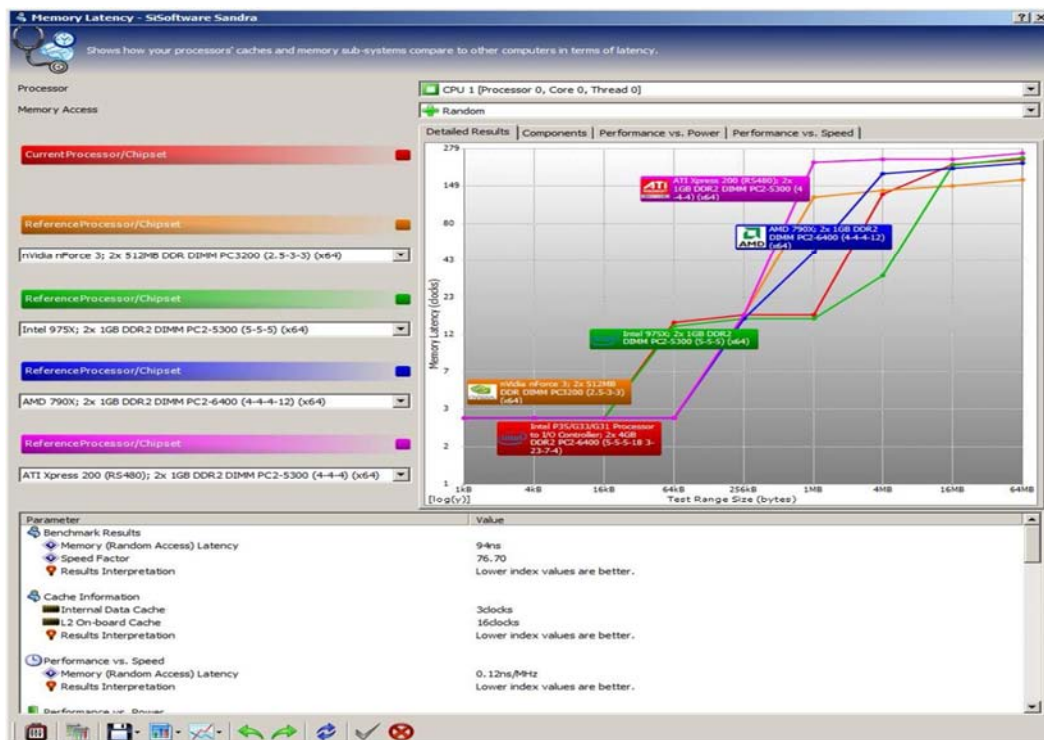
Slika 30: Virtualna mašina se jednim jezgrom i 512MB memorije, test aritmetičkih operacija



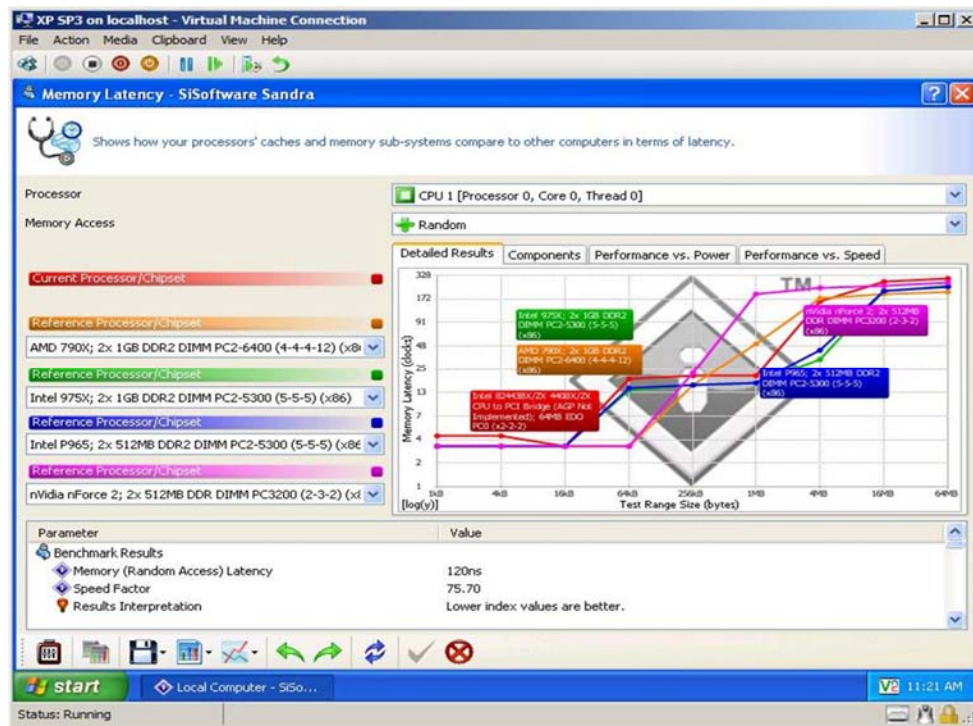
Slika 31: Fizički računar, test multimedijalnih operacija



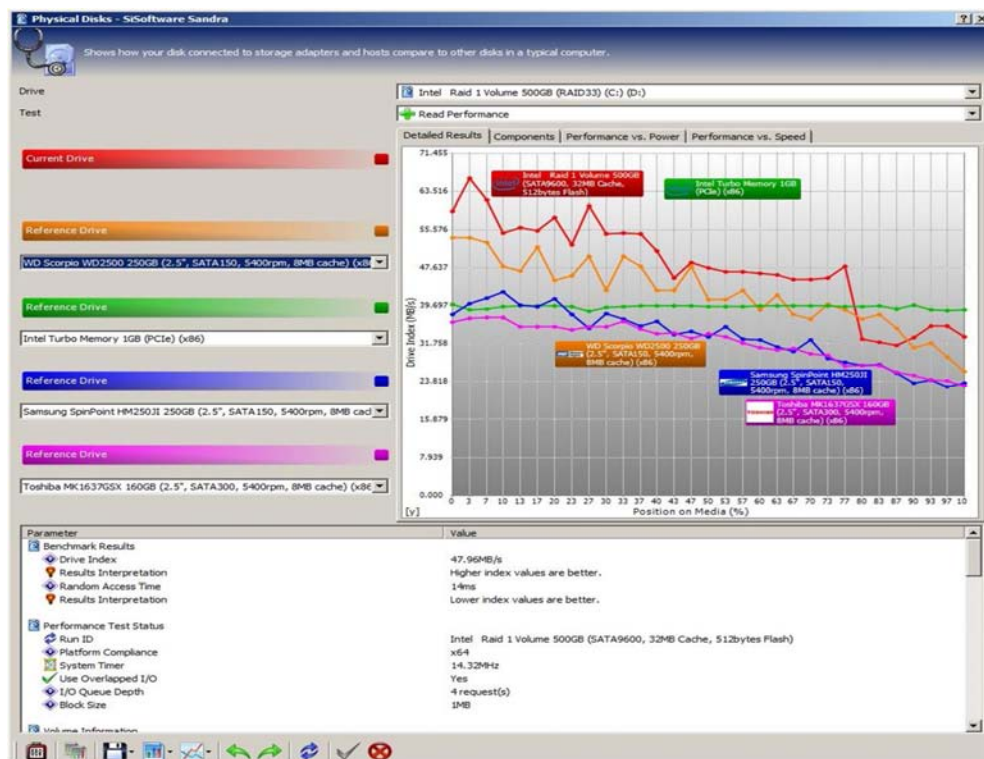
Slika 32: Virtualna mašina se jednim jezgrom i 512MB memorije, test multimedijalnih operacija



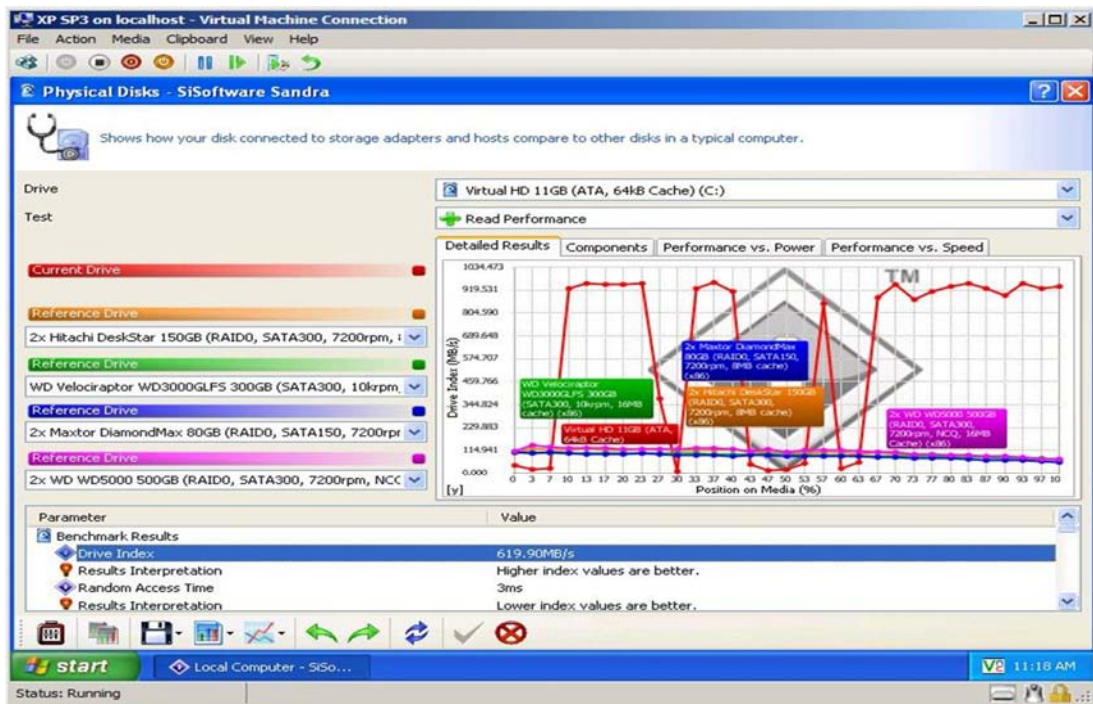
Slika 33: Fizički računar, memory latency/bandwidth test



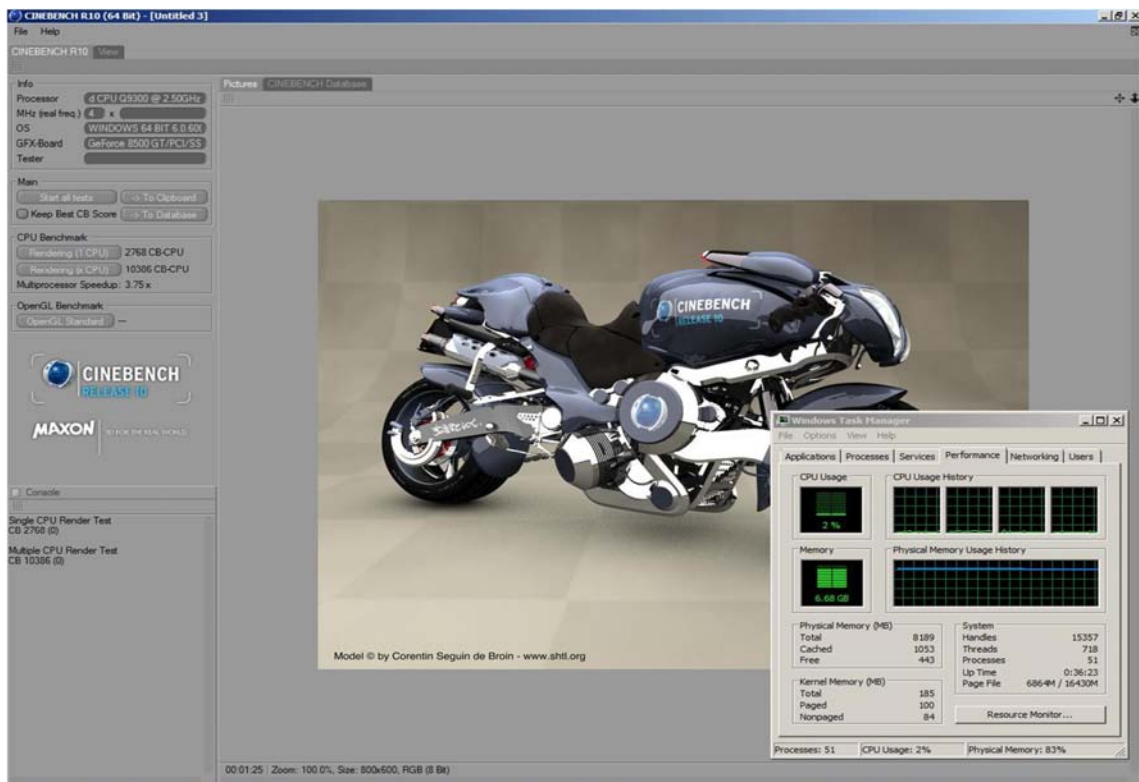
Slika 34: Virtualna mašina sa jednim procesorom i 512MB, memory latency/bendwith test



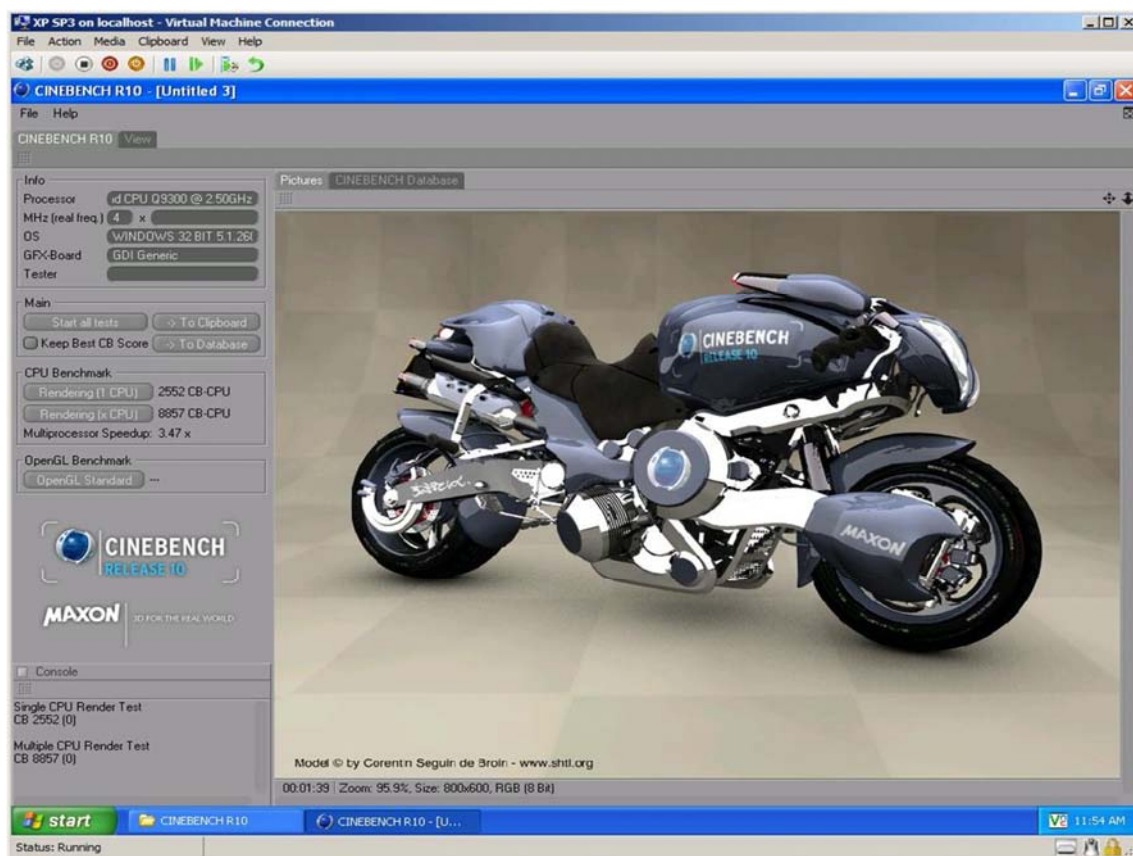
Slika 35: Fizički računar, Disk read/write test



Slika 36: Virtualna mašina sa jednim procesorom i 512MB, Disk read/write test

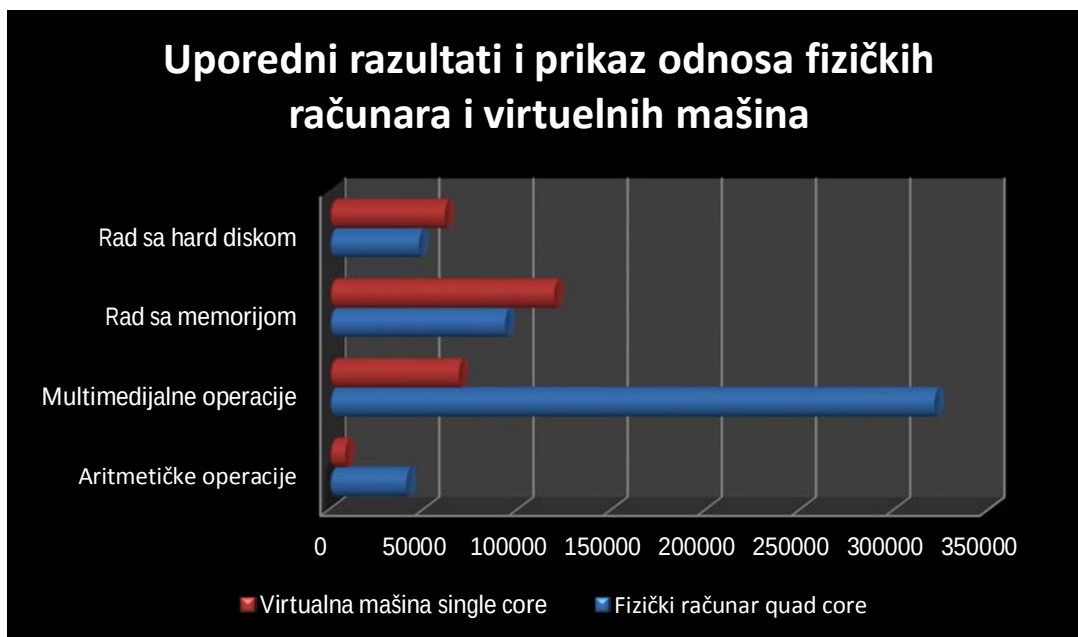


Slika 37: Fizički računar, Procesor rendering test (single and multi core)

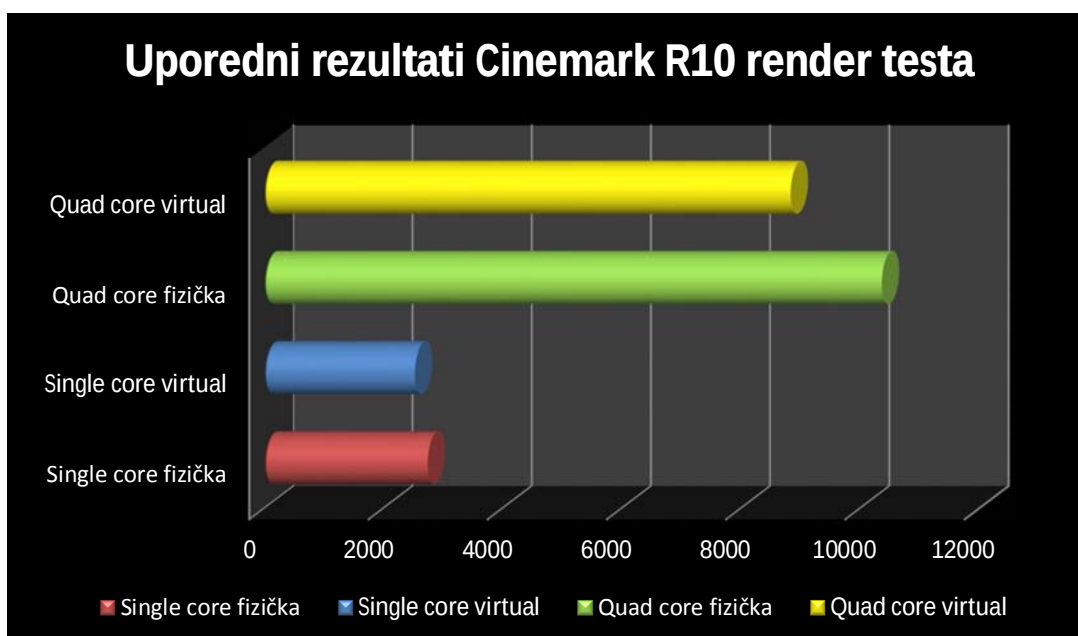


Slika 38: Virtualna mašina sa četiri jezgra i 1024MB, Procesor rendering test

Na sledećim graficima su grafički predstavljeni uporedni prikazi i odnosi rada fizičkih računara naspram virtualnih mašina u radu sa memorijom, hard diskovima, multimedijalnim aplikacijama kao i sa aritmetičkim operacijama. Treba obratiti pažnju pri analizi rezultata u slučaju virtualnih mašina rezultati su zasnovani na jednom jezgru dok je test fizičkog računara rađen sa četiri jezgra.



Grafik 1: Uporedni rezultati i prikaz odnosa fizičkih računara i virtualnih mašina



Grafik 2: Uporedni rezultati i prikaz odnosa fizičkih računara i virtualnih mašina u Cinemark R10 rendering testu

Po završetku testiranja uverili smo se da je virtuelizacija PC računara ušla u zrele godine i da je spremna da zauzme svoje mesto u datacentru Univerziteta Singidunum.

Windows Server 2008 x64 Enterprise edition pokrenuli smo na sledećoj konfiguraci:

Matična ploča	Intel VSA5000
Procesori	2 x Intel Xeon 5410
Memorija	8 X 2 GB Kingstone DDR3
Grafička karta	Integrisana ATI
Hard disk	2x WD Caviar 1Tb/WD10000AAKS, 7200rpm, 32MB
Opički uređaj	Pioneer 116D
Napajanje	Chieftec 750W

Iako malo skuplji i jači delovi nego ona koju smo koristili pri testiranju i ovi delovi uspevaju da opravdaju svoju cenu. Na pomenutom računaru trenutno je pokrenuto sedam virtuelnih mašina od kojih se četiri koriste u nastavi, jedna za računovodstvo a dve za eksperimentalne svrhe. U većini slučajeva korisnici nisu ni svesni da rade na virtualizovanim delovima koji već tri meseca bez greške obavljaju i najsloženije operacije.

ZAKLJUČAK

U radu smo predstavili koncept već standardnog Windows Server 2003 domen okruženje i ukazali na prednosti koje ovaj sistem ima u odnosu na druge mrežne operativne sisteme. Opisali smo i pokazli sve elemente koje čine jedan fizički data centar da bi u drugom delu rada fizičke elemente preneli i testirali u virtualnom okruženje koje sa sobom nosi Windows Server 2008.

U radu smo predstavili gotovo sve trenutno aktuelne proizvode namenjenih virtualizaciji, objasnili kako se uključuje virtualizacija u Windows Serveru 2008 i kako se pravi i pokreće virtualna mašina pod Windows Serverom 2008. Uradili smo testove zasnovane na aritmetičkim i multimedijalnim operacijama, kao i testove rada memorije i hard diska, takođe smo uradili i testove 3D renderinga, a rezultati su predstavljeni preko grafikona i tabela. Nakon svih sprovedenih testova i instalacija došli smo do zaključka da je virtualizacija opravdana u svakom pogledu:

- Cena nabavke jednog "jakog" računara sličnog onom kojeg smo koristili za test je daleko manja nego cena četiri slabija računara koji bi obavljali funkcije ovog računara, takođe nabavka i instalacija jednog računara traje vremenski mnogo kraće nego nabavka i instalacija četiri ili više nezavisnih računara
- Potrebno je četiri puta manje izvora struje (UPSeva) za servere nego u slučaju ne virtualizovanih računara
- Potrebno je četiri puta manje prostora nego u slučaju ne virtualizovanih računara
- Makimalno je olakšana manipulacija i rad sa serverima, pogotovo korišćenjem opcije Snapshot
- Korišćenjem virtualnih mašina otvara se mogućnost testiranja na živom sistemu što često nije moguće u poslovnom okruženju i sa fizičkim mašinama

Da zaključimo: virtualizacija je koncept i skup zrelih proizvoda koji su danas na dohvat ruke (rešenja Hiper-V, Vmware, Xen, itd.), koji uspešno rešava brojne probleme u datacentru, i koji će u godinama koje slede iz temelja izmeniti arhitekturu datacentra, operativnih sistema, modela licenciranja softvera i najzad samog koncepta IT servisa. Virtualizacija je IT megatrend koji preduzeća i njihov IT mogu ignorisati samo na sopstvenu štetu.

Na samom kraju rada napomenuo bih da smo pisajući ovaj rad stekli mnogo praktičnih iskustava koja se sada primenjuju u datacentru Univerziteta Singidunum. Ovde navodimo samo neka od njih:

- Microsoft ILM 2007 server je podignut i radi kao virtuelna mašina, server se koristio i koristi se za otvaranje studentskih mail naloga, preko ovog servera otvoreno je 1600 naloga za brucoše Univerziteta Singidunum. Server se koristio i preko RDC protokola i Shareview konekcije sa članovima Microsofta iz Nemačke i pritom sa pomenutim serverom nikada nije bilo problema ili bilo kakvih intervencija na istom, UP time ovog virtualnog računara je nešto više od 63 dana.
- TLS server koji se koristi za testiranje studenata pomoću programa TLS je uspešno konvertovan iz fizičkog računara u virtuelnu mašinu i kao takav se već tri ispitna roka koristi za testiranje studenata. Na serveru su podignuti SQL baza i sam server, sa ovim serverom se javilo par poteškoća ali su sve uspešno prevaziđene i od tada server ima UP time od 30 dana.
- Server JIN je takođe konvertovan iz fizičkog računara u virtuelnu mašinu. Server se koristi za knjigovodstvene programe i bazu podataka pravnih regulativa. Server nikada nije pravio probleme, a korisnici nisu ni primetili prelazak niti su svesni da rade na virtuelnom serveru. UP time ovog servera je 80 dana bez ikakvih problema.
- Microsoft SharePoint Server 2007 podignut je na virtuelnoj mašini i uspešno se koristi za potrebe Računskog centra Univerziteta Singidunum već dva meseca.

LITERATURA

- (1) Uvod u računarske mreže – Prof. dr Mladen Veinović i Mr. Aleksandar Jevremović
- (2) Implementiranje, upravljanje i održavanje mrežne infrastrukture Microsoft Windows 2003: udžbenik za pripremu ispita individualnim tempom - J.C. Mackin, Ian McLean
- (3) Windows Server 2003 Security Infrastructures: Core Security Features - Clerq, Jan De, Elsevier
- (4) Windows Server 2003 Networking Recipes: A Problem-solution Approach - Allen, Robbie; Dinerman, Bradley J.; Hunter, Laura E.
- (5) Informaciona tehnologija za menadžment: transformisanje poslovanja u digitalnu ekonomiju – Efraim Turban, Ephraim McLean, James Wherterbe
- (6) Network+:studijski priručnik – David Groth, Tobz Skandier
- (7) Security+:studijski priručnik – Mike Pastore, Emmett Dulaney
- (8) Windows Server 2003 Biblija – Jeffrey R. Shapiro, Jim Boyce, Marcin Policht
- (9) CCNP BCMSN: priprema za CCNP ispit: zvanični udžbenik za polaganje ispita – David Hucaby
- (10) Windows® Administration at the Command Line for Windows Vista™, Windows® 2003, Windows® XP, and Windows® 2000 - Mueller, John Paul

- (11) Microsoft Windows Server 2003 TCP/IP Protocols and Services Technical Reference, Joseph Davies and Thomas Lee
- (12) How to Cheat at Designing Security for a Windows Server 2003 Network: The Windows Server 2003 Security Guide - Ruston, Neil; Peiris, Chris
- (13) Windows Server 2008 Unleashed, Rand Morimoto , Michael Noel, Omar Droubi , Ross Mistry , Chris Amaris
- (14) Windows Server 2008 Inside Out, William R. Stanek
- (15) Microsoft Windows Server 2008 Administration - Seguis, Steve
- (16) Windows Server 2008 Administrator's Pocket Consultant , William R. Stanek
- (17) Microsoft Windows Server 2008: Implementation and Administration, Barrie Sosinsky
- (18) Windows Server 2008 Hyper-V Unleashed, Rand Morimoto, Jeff Guillet

Internet izvori:

- (1) <http://www.microsoft.com>
- (2) <http://www.hp.com>
- (3) <http://www.sisoftware.net>
- (4) <http://www.microsoft.com/isaserver/default.mspix>
- (5) <http://www.microsoft.com/windowsserver2003/iis/default.mspix>
- (6) <http://www.eset.com/>
- (7) <http://www.microsoft.co.yu>
- (8) <http://www.coming.co.yu>
- (9) <https://www.mssinergija.net/>