UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Matej Tekavčič

Nadgradnja informacijske infrastrukture

DIPLOMSKO DELO
NA VISOKOŠOLSKEM STROKOVNEM ŠTUDIJU

Mentor: doc. dr. Mira Trebar

Ljubljana, 2010

Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00494/2009
Datum: 15.12.2009

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **MATEJ TEKAVČIČ**

Naslov: **NADGRADNJA INFORMACIJSKE INFRASTRUKTURE**
INFORMATION INFRASTRUCTURE UPGRADE

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija

Tematika naloge:

V diplomski nalogi predstavite implementacijo nadgradnje informacijske infrastrukture na Mestni občini Ljubljana. Analizirajte obstoječi sistem in definirajte konfiguracijo strojne opreme z ustreznim številom strežnikov in podatkovnih modulov, tako da izpolnjujejo zahteve po visoki razpoložljivosti in zanesljivosti delovanja informacijskih storitev. Izberite primerno rešitev za izvedbo programske nadgradnje operacijskega sistema, storitev aktivnega imenika in poštnih storitev v programskem okolju Windows. Postopek nadgradnje implementirajte v realnem okolju pri končnem uporabniku in za zahtevano obdelavo poslovnih procesov z velikim številom uporabnikov ovrednotite predlagano rešitev.

Mentor:
doc. dr. Mira Trebar

Fakulteta za računalništvo in informatiko
2
UNIVERZA V LJUBLJANI

Dekan:
prof. dr. Franc Solina

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Namesto te strani **vstavite** original izdane teme diplomskega dela s podpisom mentorja in dekana ter žigom fakultete, ki ga diplomant dvigne v študentskem referatu, preden odda izdelek v vezavo!

IZJAVA O AVTORSTVU

diplomskega dela

Spodaj podpisani Matej Tekavčič,

z vpisno številko 63020165,

sem avtor diplomskega dela z naslovom:

Nadgradnja informacijske infrastrukture

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal/-a samostojno pod mentorstvom
  doc. dr. Mire Trebar
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki "Dela FRI".

V Ljubljani, dne 28.04.2010 Podpis avtorja/-ice:

Zahvala

Zahvaljujem se mentorici doc. dr. Miri Trebar za strokovno pomoč in usmerjanje pri izdelavi diplomske naloge. Zahvaljujem se tudi vsem, ki so me v času študija podpirali.

Kazalo

Seznam uporabljenih kratic in simbolov

AD	Active Directory
NAS	Network Area Storage
RAID	Redundant array of inexpensive disks
LUN	Logical unit number
FSMO	Flexible Single Master Operations
IP	Internet Protocol
WAN	Wide Area Network
DRC	Data Recovery Center
ISA	Internet Security and Acceleration Server
NLB	Network Load Balancing
LDAP	Lightweight Directory Access Protocol
DMZ	Demilitarized Zone
MAPI	Messaging Application Programming Interface
POP3	Post Office Protocol version 3
IMAP3	Internet Message Access Protocol 3
FSMO	Flexible single master operation

Povzetek

Analiza je pokazala, da informacijska infrastruktura ne Mestni občini Ljubljana ne izpolnjuje zahtev po visoki razpoložljivosti, varnosti in podpori sodobnim poslovnim procesom. Strojna oprema je zastarela in ni sposobna zagotoviti dovolj performančnih virov za izvajanje tekočih poslovnih procesov. Proizvajalec za programsko opremo ne nudi več podpore v obliki popravkov in odpravljanja napak.

Namen dela je analizirati obstoječe stanje informacijske infrastrukture in določiti ustrezno novo strojno in programsko opremo. Za nov operacijski sistem je najbolj primeren najnovejši Windows 2008 R2 Server v katerem je že Aktivni imenik, poštni sistem pa se bo nadgradil z Exchange 2010. Določiti je potrebno tudi zaporedne korake nadgradnje. Med postopkom nadgradnje ne sme priti do izpada katerekoli storitve v obstoječem sistemu.

Cilj posodobitve je zagotoviti sodobno informacijsko infrastrukturo, ki je dovolj hitra in zanesljiva. Izpolnjevati mora zahteve po visoki razpoložljivosti Aktivnega imenika in poštnih storitev, saj lahko le tako nudimo ustrezno podporo sodobnim poslovnim procesom.

Ključne besede:

informacijska infrastruktura, strežnik, Windows 2008 R2 Server, Exchange 2010, Aktivni imenik, VMWare

Abstract

The analysis showed that IT infrastructure at the Municipality of Ljubljana does not met requirements for high availability and security. It can no longer support modern business processes. Hardware is outdated and is unable to provide sufficient resources to run current business processes. The manufacturer does not provide support for software in the form of adjustments and troubleshooting.

The purpose is to analyze the current situation in IT infrastructure and determine appropriate new hardware and software. For the new operating system is the most suitable Windows 2008 R2 Server which also includes Active Directory, the postal system will be upgraded to Exchange 2010. It is also necessary to determine sequential upgrade steps. The upgrade process must not lead to any loss of service in existing system.

The update aims to provide a modern information infrastructure that is sufficiently fast and reliable. It must meet the requirements for high availability of Active Directory and postal services, only then we can offer appropriate support modern business processes.

Key words:

information technology infrastructure, server, Windows 2008 R2 Server, Exchange 2010, Active Directory, VMWare

Poglavje 1

Uvod

Sodobni informacijski sistem postaja splošna zahteva vsake uspešne organizacije. Uvajanje najnovejše tehnologije je nujno, če želimo pospešiti poslovne procese v podjetju in tako zagotoviti rast organizacije. Tega se zaveda tudi Mestna občina Ljubljana, ki se je odločila nadgraditi svojo informacijsko infrastrukturo. Zaradi zastarele strojne in programske opreme mestna občina ne more več slediti novim poslovnim procesom. Microsoft je za določeno programsko opremo, ki jo uporabljajo že ukinil podporo. Posodobitev informacijske infrastrukture je nujna za zagotavljanje varnosti, zanesljivosti in ustrezne podpore novim poslovnim procesom.

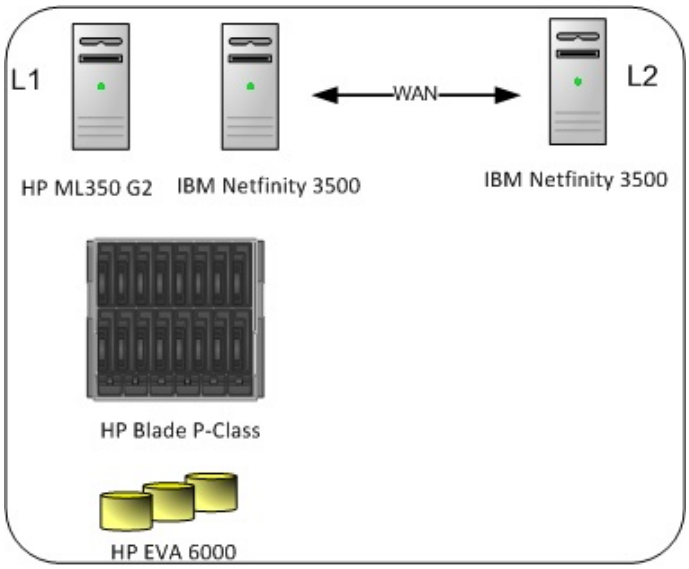
Potrebno je posodobiti operacijski sistem Windows 2000 Server in Windows 2003. Nadgraditi je potrebno tudi poštni strežnik Exchange 2003. Zaradi zastarele strojne opreme, ki ni sposobna poganjati najnovejše programske opreme je potrebno zamenjati tudi to. Nova informacijska infrastruktura mora zagotoviti visoko razpoložljivost Aktivnega imenika in poštnih stroritev ter varnost podatkov.

Operacijski sistem se bo zamenjal z najnovejšim Windows 2008 R2 Server, istočasno se bo posodobil tudi Aktivni imenik, poštni sistem pa se bo nadgradil z zadnjo verzijo Exchange 2010. Da se zagotovi varnost in visoka razpoložljivost storitev v primeru tehničnih okvar strežnikov, bo nova infrastruktura razdeljena na dve lokaciji. Nadgradnja se bo izvedla po korakih. Najprej se zamenja strojna oprema nato nadgradi operacijski sistem in Aktivni imenik, v zadnjem koraku pa se izvede nadgradnja poštnega sistema.

Poglavje 2

Strojna oprema

Informacijska infrastruktura na Mestni občini Ljubljana (MOL) je nameščena na dveh lokacijah. Primarna se nahaja na Streliški ulici (L1), sekundarna pa na Zarnikovi ulici (L2). Na lokaciji L1 teče Aktivni imenik in poštne storitve. Na lokaciji L2 teče le Aktivni imenik. Strojna oprema, na kateri teče omenjena programska oprema je postavljena tako, da ustreza zahtevam po visoki razpoložljivosti in zanesljivosti osnovnih informacijskih storitev. Fizična postavitev je predstavljena na sliki 2.1.



Slika 2.1: Fizična shema postavitve.

Strojno opremo sestavljajo:

- dva strežnika IBM Netfinity 3500
- strežnik Hewlet Packard ML350 G2
- strežniške rezine Hewlett Packard Blade P-Class
- mrežno diskovno polje Hewlett Packard Storage 6000 Enterprise Virtual Array

Lokaciji sta med sabo povezani s širokopasovno povezavo (WAN). Uporabniki na lokaciji L2 se prijavljajo na lokalni strežnik. Za dostop do elektronske pošte pa se odjemalci povežejo na poštni strežnik na lokaciji L1. Poštne storitve na lokaciji L1 tečejo na strežniških rezinah HP Blade P-Class.
Strežniška rezina je samostojna enota, ki vsebuje pomnilnik in procesno enoto. Več takih enot je nameščenih v posebno ohišje. Skupaj z ohišjem tvorijo zmogljiv računalniški sistem v katerem na vsaki enoti teče svoj operacijski sistem. Na ohišje je z optičnimi povezavami priključeno mrežno diskovno polje HP EVA 6000. Vsaka enota v ohišju ima svoj virtualni disk na mrežnem diskovnem polju.

2.1 Strežniki

Strežnik [5] je naprava, ki skupaj s programsko opremo, ki jo poganja, nudi določene storitve ostalim napravam oz. odjemalcem v omrežju. Fizično je strežnik zgrajen tako, da je čimbolj odporen na incidente, ki se lahko pripetijo v organizaciji. Diski na katerih teče operacijski sistem so zaradi zaščite podatkov povezani v RAID polje. Zaradi zaščite pred pregrevanjem komponent so strežniki nameščeni v posebnih sobah, hlajenih s klimatskimi napravami. Dodatno zaščito pred pregrevanjem nudi tudi veliko število ventilatorjev vgrajenih v strežniku med posameznimi komponentami. Praviloma imajo strežniki dva ali več napajalnikov, ki so priključeni na ločene vire napetosti. Prav tako imajo tudi več omrežnih kartic ravno tako priključenih na različna omrežna stikala. Vse to nam zagotavlja visoko razpoložljivost in zanesljivost storitev v organizaciji.

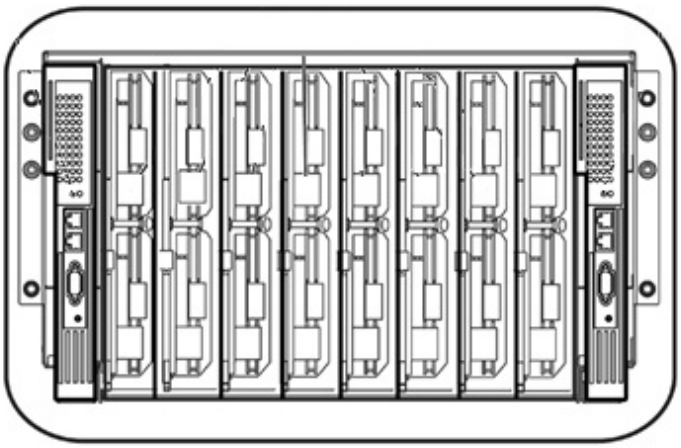
MOL razpolaga z dvema vrstama strežnikov:

- **Strežnik IBM Netfinity 3500**: Strežnik je oblike "Mini Tower" in je namenjen majhnim in srednje velikim organizacijam. Strežnik je že zastarel in ni več v proizvodnji. V njem je vgrajen Intelov procesor serije Pentium, ki lahko vsebuje do 1 GB pomnilnika. Primeren je za poganjanje operacijskega sistema Windows 2000 Sever ali, z vsemi strojnimi nadgradnjami, Windows 2003 Server [4].

- **Strežnik Hewlett Packard ML350 G2**: Strežnik je novejši kot IBM Netfinity 3500. Podpira dva procesorja družine Intel Pentium 3 in do 4GB pomnilnika. Vgrajeno ima ohišje za šest dodatnih fizičnih diskov, ki jih je možno povezati v RAID polje. Okvarjeni disk lahko zamenjamo brez izklopa strežnika. Priložena programska oprema omogoča boljši pregled delovanja posameznih komponent strežnika.

2.2 Strežniške rezine

Strežniške rezine [6] so kompaktni strežniki in so nameščeni v posebno za to namenjeno ohišje, ki pa je vgrajeno v standardno strežniško omaro (ang. rack). Vsaka strežniška rezina ima svojo procesno enoto in pomnilnik. Komponente, kot so omrežne kartice, napajalnik in diskovni prostor si deli z ostalimi rezinami v ohišju. Ohišje ima vgrajen modul za nadzor nad delovanjem posameznih komponent ohišja in strežniških rezin. Morebitne okvare ali nepričakovane dvige temperature pa ustrezno beleži in sporoča sistemskim administratorjem. Za usmerjanje omrežnega prometa med sistemi, ki tečejo v ohišju skrbi kar ohišje samo. Ohišje je zgrajeno tako, da ni odvisno le od enega električnega ali omrežnega vira. Električni viri in omrežne povezave so redundantne. Promet po omrežnih povezavah je ustrezno razporejen, da ne prihaja do preobremenitve le ene omrežne kartice. Primer ohišja z vsemi strežniškimi rezinami prikazuje slika 2.2.



Slika 2.2: Strežniške rezine.

V ohišje je mogoče namesto strežniške rezine vgraditi tudi manjše diskovno polje v večini primerov pa se na ohišje priklopi zunanje diskovno polje. Polje se nato razdeli na več posameznih logičnih diskov, diski pa se nato povežejo na strežniško rezino na kateri teče operacijski sistem.
Strežniške rezine so primerne za poganjanje virtualnega okolja. Z uporabo takšne strežniške zasnove, prihranimo na prostoru in pridobimo na zmogljivosti. Sistem je tako konsolidiran in centralno upravljan.

MOL razpolaga z enim ohišjem Hewlett Packard Blade P-Class. Na njem teče virtualno okolje VMware ESX 3.5. V virtualnem okolje je postavljenih več virtualnih strežnikov. Dva izmed njih poganjata storitev elektronske pošte. Na ostalih strežnikih tečejo servisi za varnostno kopiranje, podatkovne baze in ostali servisi, ki niso del diplomske naloge.

2.3 Mrežno diskovno polje

Mrežno diskovno polje (ang. Network Area Storage) ali krajše NAS [7], je naprava v kateri se nahaja več enakih fizičnih diskov. Naprava je na strežnik priklopljena z eno ali več optičnimi povezavami, kar zagotavlja visoke hitrosti pri izmenjavi podatkov med strežnikom in NAS-om. NAS naprava služi za hranjenje velike količine datotek in podatkovnih baz, uporablja se tudi za izdelavo varnostnih kopij. Ob okvari enega izmed fizičnih diskov lahko le-tega zamenjamo brez izklopa naprave. Fizični diski so organizirani v RAID polja, ki jim pogosto rečemo tudi LUN (ang. Logical Unit Number). Na posameznem RAID polju lahko ustvarimo več logičnih diskov. Vsak logični disk je pripet svojemu strežniku. Fizične diske lahko povežemo v RAID polje na več različnih načinov. Vsak način ima svoje prednosti in slabosti.

Najbolj pogosti načini povezovanja fizičnih diskov v RAID polje:

- **RAID 0**: Za povezavo diskov v polje RAID 0 potrebujemo vsaj dva diska. Deluje tako, da podatke, ki jih vsebuje polje razdeli na vse diske v polju. Ta način odlikuje visoka hitrost zapisovanja in branja podatkov, saj vsak disk prevzame del dela. Slabost polja je, da ob okvari enega diska izgubimo podatke na vseh diskih v polju.

- **RAID 1**: Zahteva minimalno dva diska. Podatki na prvem disku so identični podatkom na drugem. V primeru okvare enega izmed obeh diskov ostanejo podatki nepoškodovani. Hitrost branja in zapisovanja je določena s hitrostjo posameznega fizičnega diska v polju.

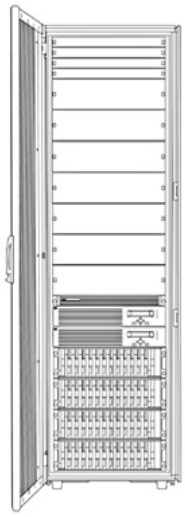
- **RAID 3 - 4**: Polje za delovanje potrebuje minimalno tri fizične diske. Prva dva vsebujeta podatke, na tretjem pa se hranijo paritetni podatki. Branje in zapisovanje je hitrejše kot pri polju RAID 1, saj se podatki zapisujejo izmenično na prva dva diska. V primeru okvare enega izmed njiju se podatki ponovno obnovijo s pomočjo tretjega diska. Med okvaro

enega diska so podatki nedosegljivi.

- **RAID 5**: Za delovanje potrebuje minimalno tri diske. V primeru okvare enega diska, so vsi podatki, za razliko od polja RAID 3- 4, dosegljivi, ker vsak disk hrani ustrezne paritetne podatke. Ta način se uporablja na MOL-u.

- **RAID 10**: Je kombinacija polja RAID 0 in RAID 1. Za delovanje potrebuje minimalno štiri fizične diske. Prva dva diska si delita podatke, kar pohitri pisanje in branje podatkov. Zaradi zaščite podatkov sta druga dva diska identična kopija prvih dveh.

Na MOL-u je v uporabi mrežno diskovno polje Hewlett Packard Storage 6000 Enterprise Virtual Array ali krajše HP EVA 6000. Diskovno polje HP EVA 6000 je namenjeno srednje velikim organizacijam. Zagotavlja visoko zmogljivost in razpoložljivost diskovnega polja. Izdelano je v "rack omari", ki je prikazana na sliki 2.2, kar omogoča modularno dodajanje novih komponent. Programska oprema, ki je priložena zelo olajša pot do želene konfiguracije diskovnega polja.

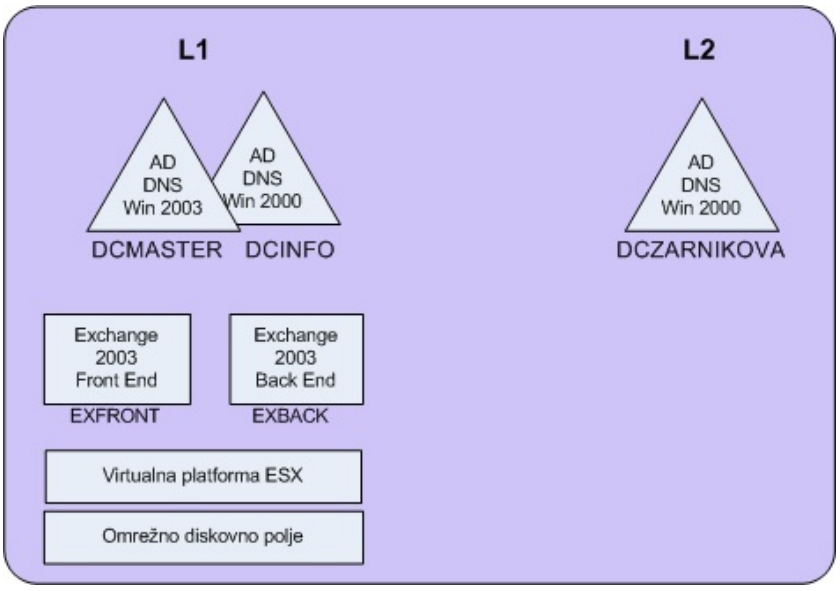


Slika 2.3: Diskovno polje HP EVA 6000.

Poglavje 3

Programska oprema

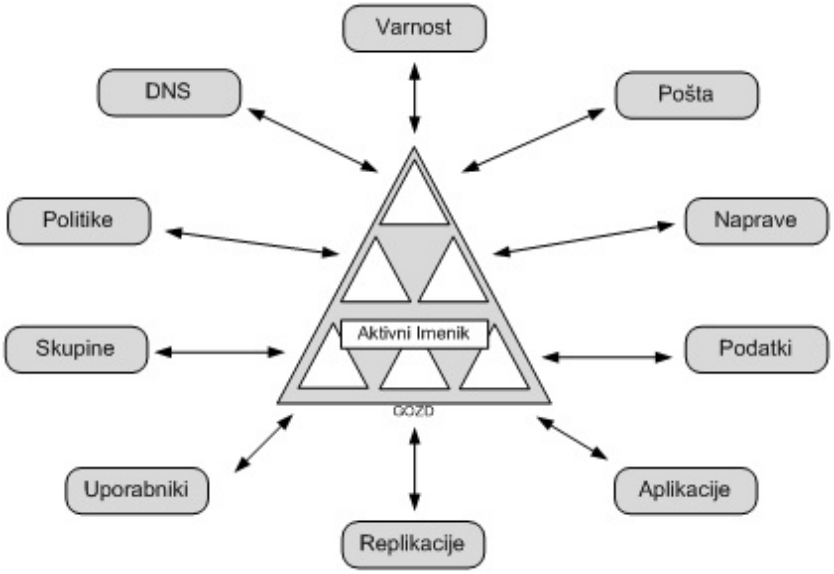
MOL uporablja programsko opremo Microsoft. Glede na to da je strojna oprema na dveh lokacijah je tudi programska oprema ustrezno postavljena na ločenih lokacijah. Strežniki na lokaciji L1 poganjajo Aktivni imenik in poštne storitve, strežnik na lokaciji L2 pa le Aktivni imenik. Poštni promet je iz lokacije L2 preusmerjen na lokacijo L1. Shemo programske infrastrukture prikazuje slika 3.1.



Slika 3.1: Logična shema postavitve.

3.1 Aktivni imenik

Aktivni imenik [11] poganja Microsoftov produkt Active Directory ali krajše AD (slika 3.2). Aktivni imenik v organizaciji hrani informacije o različnih identitetah in relacijah med njimi. Imenik je temeljna storitev v Windows okolju in je obvezen za vse storitve, ki jih nudijo ostali Microsoftovi produkti.



Slika 3.2: Aktivni imenik.

Aktivni imenik sestavljajo tri osnovne komponente:

- **Struktura Aktivnega imenika**: Zasnovana je na LDAP [10] protokolu. Je imenik vseh uporabnikov, strežnikov, delovnih postaj in aplikacij v organizaciji, ki so v strukturi predstavljeni kot objekti. Imenik omogoča centralni nadzor in upravljanje nad objekti. Posamezen objekt je lahko član skupine objektov. Na skupino ali posamezen objekt je mogoče dodeljevanje pravic ali različnih pravil, nameščanje aplikacij in popravkov.

- **Preverjanje identitete**: Zasnovano je na protokolu Kerberos [12], ki temelji na kriptografiji z uporabo skritega ključa. Uporabnik se mora za dostop do imeniških storitev in ostalih servisov na omrežju, prijaviti z ustreznim uporabniškim imenom in geslom. Aktivni imenik poskrbi, da so uporabniku posredovane ustrezne nastavitve programske opreme

in dostop do podatkov, ki jih potrebuje za svoje delo.

- **Sistem domenskih imen**: Je servis, krajše imenovan DNS (ang. Domain Name Service), ki preslika IP naslov v ime in obratno. Hrani vsa imena in njihove IP preslikave za vse delovne postaje, strežnike in storitve, ki se nahajajo v organizaciji.

3.2 Poštne storitve

Podporo poštnim storitvam nudi poštni strežnik Microsoft Exchange 2003 Server [9]. Gre za sporočilni sistem za prenos elektronske pošte. Poleg storitve elektronske pošte nudi uporabniku velik nabor najrazličnejših funkcionalnosti, ki mu olajšajo delo zlasti v poslovnih okoljih, kjer je potreba po hitri izmenjavi komunikacij nujna. Za uporabo vseh funkcionalnosti uporabnik potrebuje Microsoft Outlook, ki je direktni odjemalec Microsoft Exchange strežniku. Skupaj uporabniku nudita najrazličnejše storitve, ki jih potrebuje pri opravljanju poslovnih nalog.

3.2.1 Funkcionalnosti poštnega strežnika

- **Koledar**: Uporabnik lahko uporablja koledar za načrtovanje poslovnih sestankov, hkrati pa ga lahko da na vpogled ostalim uporabnikom. Omogoča jim, da lahko takoj ugotovijo medsebojno dosegljivost in tako lažje načrtujejo skupne aktivnosti.

- **Opravila**: Nadrejeni lahko s pomočjo opravil hitro in jasno posreduje nalogo delavcem, hkrati pa lahko spremlja kako delo napreduje.

- **Skupne mape**: V skupne mape lahko odložimo dokumente ali elektronska sporočila. Vsak, ki ima pravico do dostopa do posamezne skupne mape, lahko te dokumente vidi in ureja, kar je uporabno pri delu na skupnih projektih.

- **Rezervacije**: Skupaj z registrom resursov, kot so službeni avtomobili in sejne sobe, hrani informacije o njihovi zasedenosti, uporabnik pa jih lahko rezervira kar iz Microsoft Outlooka. Storitev imenika nudi uporabnikom dostop do kontaktnih podatkov ostalih uporabnikov hkrati pa lahko v imenik dodajajo tudi svoje kontakte.

Vse funkcionalnosti skupaj omogočajo, da uporabnik z enim postopkom pošlje vabilo na dogodek, rezervira potrebne resurse in vsem sodelujočim ustrezno posreduje potrebne podatke.
Microsoft Exchange se tesno integrira v Microsoftovo strežniško infrastrukturo. Za delovanje potrebuje Aktivni imenik iz katerega črpa podatke o uporabnikih in aplikacijah. Taka integracija uporabniku omogoča, da lahko z eno prijavo

na delovno postajo dostopa do vseh potrebnih storitev.

Microsoft Exchange dosledno sledi tako standardom za prenos elektronske pošte, kot tudi sodobnim varnostnim smernicam, ki jih narekujejo najboljše prakse. Poštni sistem je na MOL-u sestavljen iz dveh delov oz. vlog:

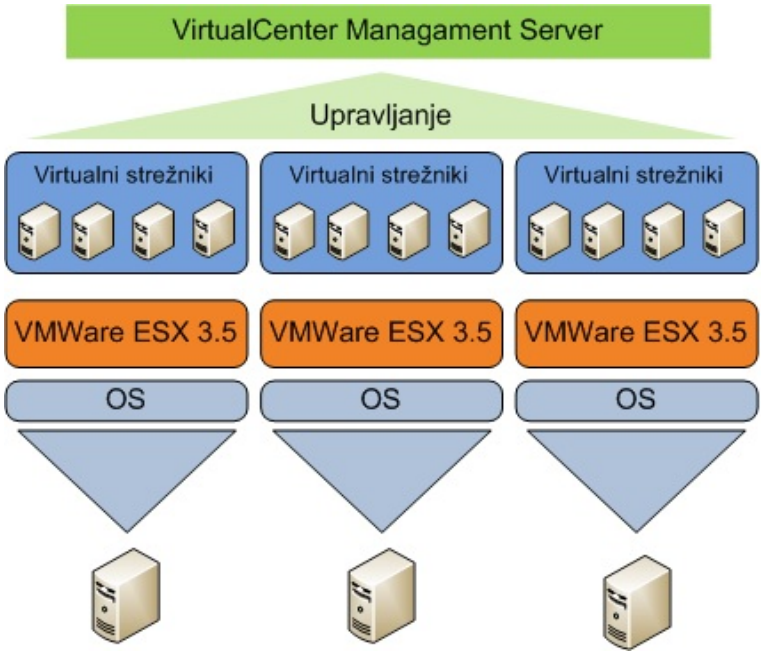
- **Vloga Back End**: skrbi za interno komunikacijo in je zaradi zaščite pred nezaželeno pošto ter zlonamerno kodo ločena od zunanjega sveta. Vloga hrani vse pošte predale uporabnikov in skrbi za ves notranji poštni promet.

- **Vloga Front End**: skrbi za komunikacijo z zunanjim svetom. Zaradi varnosti je postavljena izven internega okolja v DMZ (ang. Demilitarized Zone) coni omrežja. Nezaželeno pošto in zlonamerno kodo tako eliminira še preden uspe priti v interno omrežje. Ena izmed dodatnih storitev vloge "Front End" je tudi Outlook Web Access,spletni portal, ki omogoča uporabniku dostop do poštnih storitev od kjerkoli. Za uporabo portala uporabnik ne potrebuje Microsoft Outlooka, saj lahko do njega dostopa iz kateregakoli spletnega brskalnika ne glede na vrsto operacijskega sistema.

3.3 Virtualno okolje

Sistemski viri so v tradicionalni postavitvi fizične strežniške infrastrukture, po načelu en strežnik ena aplikacija, slabo izkoriščeni [8]. S številom aplikacij, ki jih potrebujemo v organizaciji, raste tudi potreba po številu fizičnih strežnikov, s tem pa tudi stroški. Takšna arhitektura je nujna, če želimo vnaprej eliminirati izpad delovanja večjega števila aplikacij, ker bi ena izmed njih povzročila neodzivnost ali izpad celotnega fizičnega strežnika. Do napake v takem primeru lahko pride tudi zaradi nekompatibilnosti med različnimi aplikacijami, ki bi v tem primeru tekle na istem fizičnem strežniku. Slabost take arhitekture pa je slaba izkoriščenost posameznega strežnika.

Virtualizacija močno poveča izkoriščenost fizične arhitekture, hkrati pa brez potrebe po dodatnih stroških omogoča ločevanje aplikacij na različne virtualne stroje. Uporaba virtualnega okolja zmanjša potrebo po prostoru in električni energiji, hkrati pa omogoča centralno upravljanje in boljšo konsolidacijo informacijske infrastrukture. Osnovno idejo virtualizacije prikazuje slika 3.3.



Slika 3.3: Virtualno ESX okolje.

MOL ima postavljene tri VMware ESX 3.5 strežnike, ki jih poganjajo tri strežniške rezine. Strežnikom sta dodeljena po dva virtualna diska iz dveh različnih diskovnih polj. Obe diskovni polji sta zgrajeni v načinu RAID 5. V virtualnem okolju teče več virtulanih strežnikov. Na dveh izmed njih tečeta vlogi "Back End" in "Front End". Ostali strežniki, ki tečejo v virtualnem okolju, so namenjeni arhiviranju in podatkovnim bazam. Sistemski diski virtualnih strežnikov se nahajajo na prvem polju, diski, na katerih se nahajajo podatkovne baze poštnega sistema pa se nahajajo na drugem polju. Tak način ločevanja sistemskih in podatkovnih diskov nam zagotavlja, da bo hitrost branja in pisanja optimalna. Zapisovanje in branje podatkov v podatkovno bazo je, prav tako, kot zapisovanje in branje podatkov med delovanjem operacijskega sistema zelo intenzivno. Z ločevanjem virtualnih diskov na različni diskovni polji dosežemo, da operacijski sistem in baza tečeta na različnih fizičnih diskih. Takšen način ločevanja operacijskega sistema in podatkovnih baz omogoča, da dosežemo najvišje možne performančne rezultate.

Poglavje 4

Nadgradnja informacijske infrastrukture

4.1 Načrt nadgradnje

Nadgradnja informacijske infrastrukture je bila v okviru projekta razdeljena na tri faze. V posamezni fazi definiramo izdelke. Faza je zaključena, ko so izdelani vsi izdelki. Koraki po fazah in izdelki posamezne faze so:

- **Faza 1**: Priprava obstoječe infrastrukture za nadgradnjo
  - **Izdelek A**: Delujoči trije strežniki z operacijskim sistemom Windows 2008 Server R2
  - **Izdelek B**: Razširjena shema Aktivnega imenika
  - **Izdelek C**: Verzija domene nastavljena na Windows 2003
- **Faza 2**: Nadgradnja imeniške infrastrukture
  - **Izdelek A**: Delujoči trije domenski Windows 2008 R2 Server strežniki
  - **Izdelek B**: Verzija domene nastavljena na Windows 2008 R2 Native
- **Faza 3**: Nadgradnja poštne infrastrukture
  - **Izdelek A**: Delujoč poštni sistem Microsoft Exchange 2010

4.2 Faza 1: Priprava obstoječe infrastrukture na nadgradnjo

4.2.1 Analiza stanja

Verzija domene na MOL-u je nastavljena na Windows 2000 Mixed in je drugo ime za verzijo Aktivnega imenika, ki teče v organizaciji. Različne verzije določajo kateri operacijski sistemi lahko tečejo na strežniku, ki je domenski kontroler. Starejša verzija domene ne dovoljuje priklopa novejših operacijskih sistemov in obratno. Verzija domene je vedno nastavljena tako, da jo lahko poganjajo vsi strežniki vključeni v domeno. Domena je na MOL-u nastavljena na verzijo Windows 2000 Mixed zato, ker so bili v preteklosti v organizacijo vključeni domenski strežniki z operacijskim sistemom Windows NT. Za pravilno delovanje sistema v katerem obstajajo domenski strežniki z Windows NT, Windows 2000 Server in Windows 2003 Server, mora biti verzija domene nastavljena na Windows 2000 Mixed [1]. Ta verzija domene ne omogoča vključitev domenskih strežnikov z operacijskim sistemom Windows 2008 R2 Server. Nivo domene je potrebno nastaviti na Windows 2003.

Za pravilno delovanje Aktivnega imenika skrbi pet vlog imenovanih "Flexible single master operation" [2]. Vse FSMO vloge obstajajo na strežniku DCINFO na katerem teče operacijski sistem Windows 2000. FSMO vloge so:

- **Glavna shema**: Krmilnik domene za glavno shemo nadzira vse posodobitve in spremembe v shemi. Pri posodabljanju sheme je potrebno imeti dostop do glavne sheme.

- **Glavno poimenovanje domene**: Krmilnik domene za glavno poimenovanje domene nadzira dodajanje domen v Gozd in odstranitev domen iz Gozda. V gozdu je mogoče imeti samo eno glavno poimenovanje domene. Gozd (ang. forest) [2] je skupek vseh domen in poddomen v organizaciji.

- **Glavna infrastruktura**: Infrastruktura je odgovorna za posodabljanje sklicevanj iz predmetov v njeni domeni na predmete v drugih domenah. Samo en krmilnik domene lahko kadar koli deluje kot glavna infrastruktura v posamezni domeni.

- **Glavni sorodni ID (RID)**: Glavni RID je odgovoren za obdelovanje zahtev iz zaloge RID iz vseh krmilnikov domen v neki domeni. Samo en krmilnik domene lahko kadar koli deluje kot glavni RID v domeni.

- **Primary Domain Controller Emulator (PDC)**: Emulator PDC je krmilnik domene, ki se delovnim postajam, članskim strežnikom in krmilnikom domen, ki uporabljajo starejše različice operacijskega sistema Windows, predstavlja kot primarni krmilnik domene (PDC). Če so na primer v domeni računalniki, v katerih se izvajajo odjemalski programi operacijskega sistema Microsoft Windows XP Professional ali Microsoft Windows 2000, ali če domena vsebuje varnostne krmilnike domene operacijskega sistema Microsoft Windows NT, deluje glavni emulator PDC kot primarni krmilnik domene operacijskega sistema Windows. Poleg tega je tudi glavni brskalnik domene in obravnava vse nedoslednosti pri geslih. Samo en krmilnik domene lahko kadar koli deluje kot glavni emulator PDC v posamezni domeni v gozdu.

Za uspešno nadgradnjo informacijske infrastrukture je potrebno vseh pet vlog prenesti na strežnik z novejšim operacijskim sistemom.
Obstoječa shema aktivnega imenika ni primerna za vključitev strežnikov z operacijskim sistemom Windows 2008 R2 Server in poštnega sistema Windows Exchange 2010. Z omenjenima produktoma je potrebno obstoječim objektom v aktivnem imeniku dodati nove politike in atribute. Shemo aktivnega imenika je zato potrebno ustrezno razširiti.

4.2.2 Priprava infrastrukture

Koraki priprave obstoječe infrastrukture:

- Prenos FSMO vlog iz strežnika DCINFO na strežnik DCMASTER, na katerem teče operacijski sistem Windows 2003
- Dvig verzije domene na Windows 2000 Native
- Razširitev sheme Aktivnega imenika
- Postavitev strežnikov z operacijskim sistemom Windows 2008 R2 Server

4.2.2.1 Prenos FSMO vlog

FSMO vloge prenesemo s pomočjo ukazne vrstice in orodja NTDSUTIL. Ukazi so navedeni na sliki 4.1.

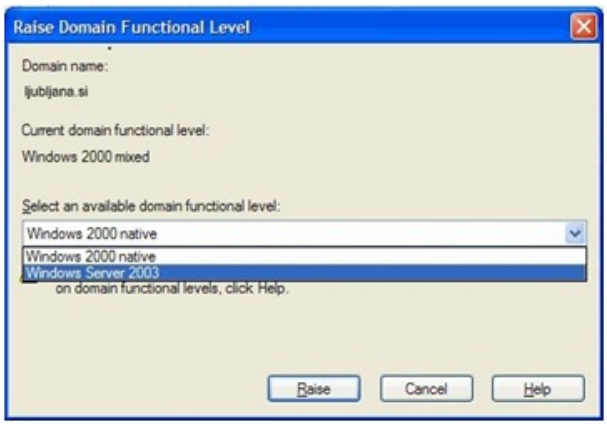
```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS>ntdsutil
ntdsutil:
ntdsutil: roles
fsmo maintenance:
fsmo maintenance: connections
server connections:
server connections: connect to server dcmaster
Binding to dcmaster ...
Connected to dcmaster using credentials of locally logged on user.
server connections:
Transfer domain naming master
Transfer infrastructure master
Transfer PDC
Transfer RID master
Transfer schema master
```

Slika 4.1: Prenos FSMO vlog.

4.2.2.2 Dvig verzije domene

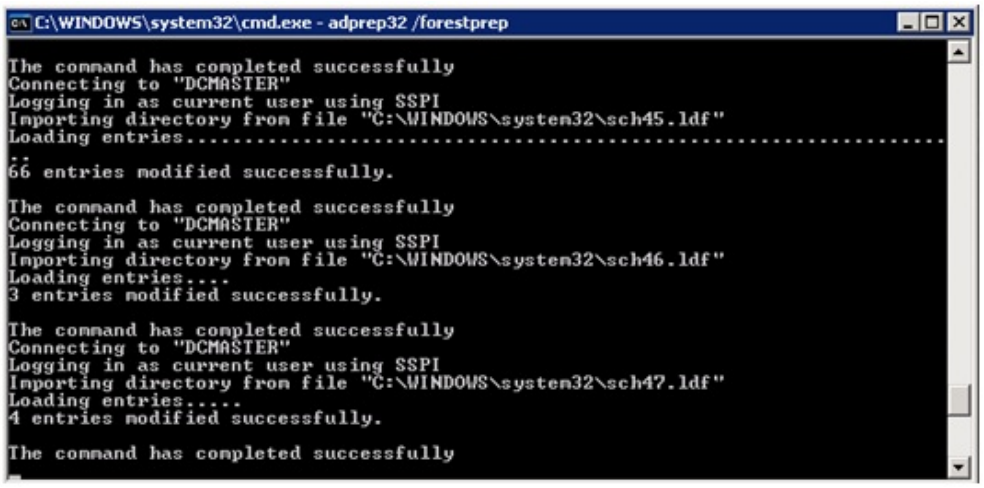
Zaženemo orodje "Active Directory Domains and Trusts" in z desno tipko kliknemo na ime domene ter izberemo "Raise Domain Functional Level". Na oknu izberemo Windows 2003 Server in to potrdimo s klikom na "Raise", kot kaže slika 4.2.



Slika 4.2: Dvig verzije domene.

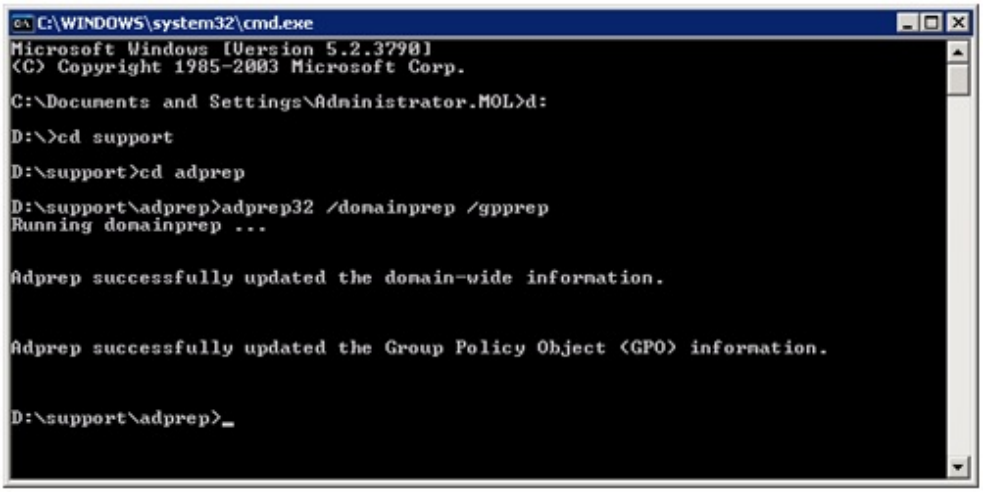
4.2.2.3 Razširitev sheme

1. Iz namestitvenega medija Windows 2008 Server R2 poženemo orodje adprep32, ki se nahaja na namestitvenem mediju v mapi sources adprep. Orodje zaženemo z ukazom *adprep32 forestprep* (slika 4.3).



Slika 4.3: Korak 1: Priprava Gozda.

2. Poženemo ukaz *adprep32 domainprep gpprep* (slika 4.4).

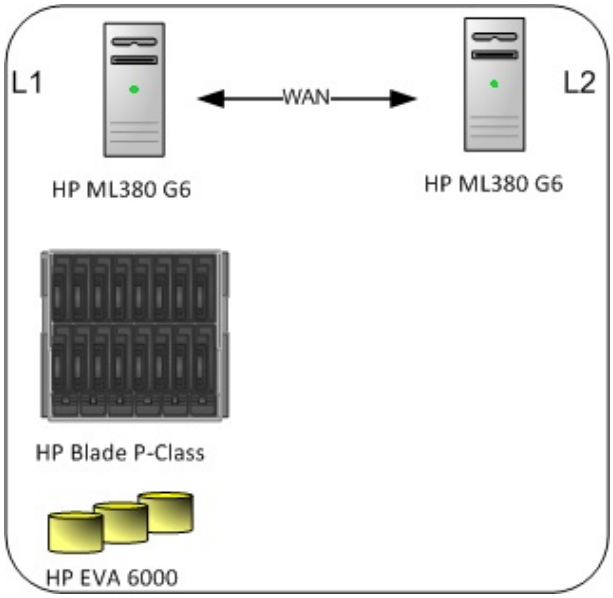


Slika 4.4: Korak 2: Priprava domene.

3. Shema je pripravljena za vključitev novih domenskih strežnikov

4.2.2.4 Postavitev strežnikov

Na lokaciji L1 postavimo en fizični in en virtualni strežnik, na lokaciji L2 fizični strežnik. Osnovna namestitev operacijskega sistema Windows 2008 R2 Server je enostavna [1], in hitra. Po namestitvi sistema na vse tri strežnike namestimo zadnje popravke in jim dodelimo ustrezne IP naslove ter jih vključimo v domeno, kot navadne strežnike. Shema strežnikov v novi infrastrukturi je predstavljena na sliki 4.5. Sestavljata jo dva strežnika Hewlet Packard ML380 G6 in en strežnik, ki teče v virtualnem ESX 3.5 okolju [8].



Slika 4.5: Korak 3: Nova infrastruktura.

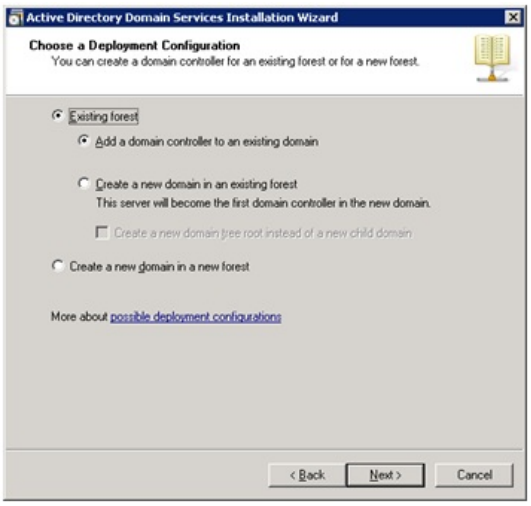
4.3 Faza 2: Nadgradnja imeniške infrastrukture

Vsi trije strežniki se postavijo v domenske strežnike na enak način, zato bom samo enkrat opisal postopek dodajanja novega domenskega strežnika, kakor tudi odstranitev starih domenskih strežnikov.
Vključitev novega strežnika v domeni povzroči, da se le ta replicira z ostalimi domenskimi strežniki v organizaciji. V podpoglavju 4.3.4 bom bolj podrobno predstavil delovanje replikacije in zakaj je pomembna.

4.3.1 Vključitev novega strežnika v domeno

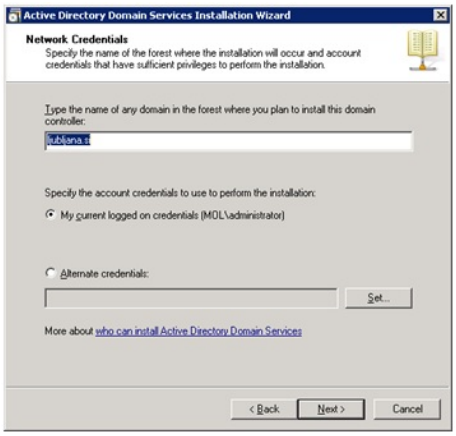
V zagonsko vrstico operacijskega sistema vpišemo ukaz *dcpromo*, ki nam zažene postopek za dodajanje novega domenskega strežnika. Med postopkom vključevanja moramo posredovati ustrezne podatke.

1. V pogovornem oknu, ki je prikazan na sliki 4.6, izberemo možnosti "Existing forest" in nato "Add a domain controller to an existing domain", kot kaže slika 4.6.



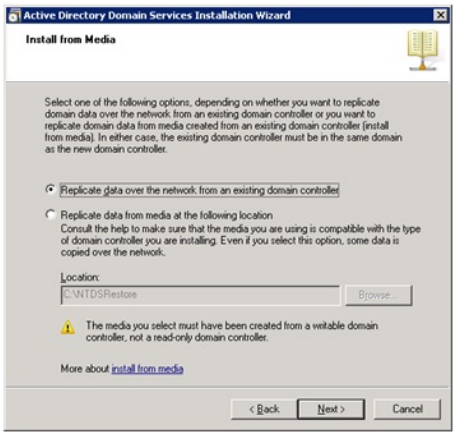
Slika 4.6: Strežnik dodamo v obstoječo domeno.

2. V nadaljevanju (slika 4.7) vpišemo ime domene, ki se v primeru MOL-a glasi ljubljana.si.



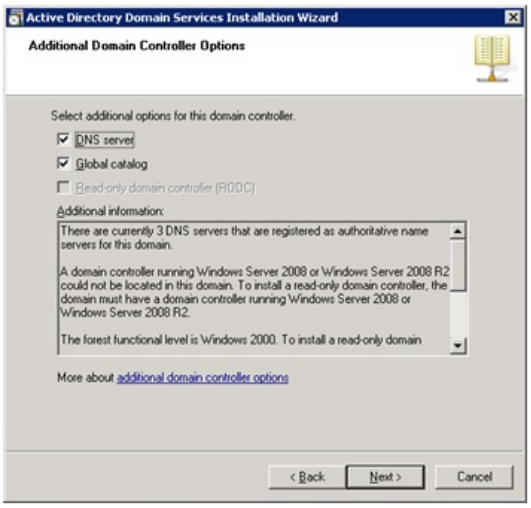
Slika 4.7: Vpis domene.

3. V naslednjem koraku (slika 4.8) določimo način replikacije. Na voljo imamo dve možnosti. Strežnik lahko repliciramo iz določenega medija ali pa kar iz obstoječega domenskega strežnika. Izberemo drugo možnost "Replicate data over the network from an existing domain controller".



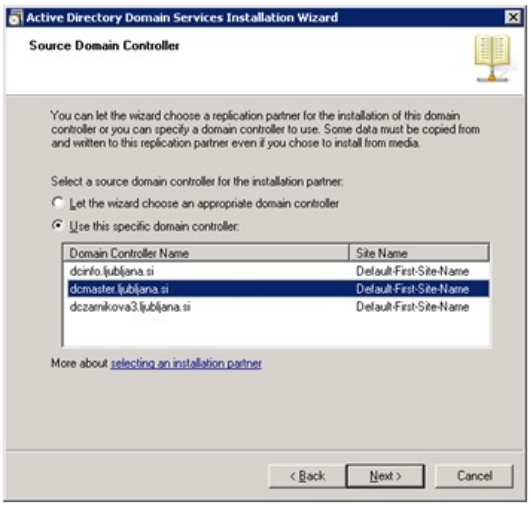
Slika 4.8: Nastavitev prve replikacije.

4. Ker bomo vse servise selili na novo informacijsko infrastrukturo, v tem koraku (slika 4.9) namestimo tudi DNS vlogo in Global Catalog.



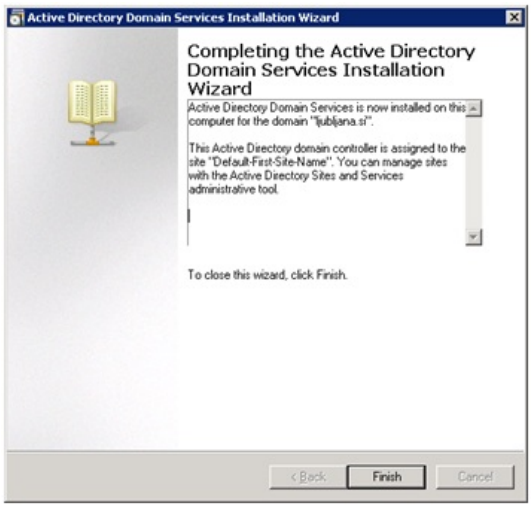
Slika 4.9: Namestitev DNS in Global Catalog.

5. Ker smo v koraku, ki ga prikazuje slika 4.9, izbrali replikacijo iz drugega domenskega strežnika, moramo v tem koraku (slika 4.10) izbrati iz katerega strežnika bomo naredilii prvo replikacijo. Izberem najbližji in najbolj zmogljiv strežnik, to je DCMASTER.



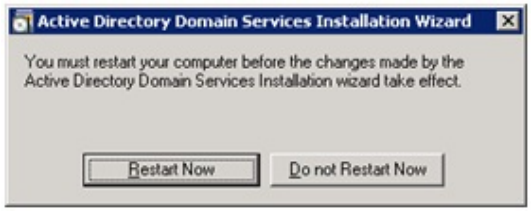
Slika 4.10: Izberemo strežnik za replikacijo.

6. Postopku smo podali vse potrebne informacije za vključitev novega strežnika v domeno, na zadnjem pogovornem oknu (slika 4.11) kliknemo "Finish".



Slika 4.11: Zaključek vključevanja strežnika v domeno.

7. In ponovno zaženemo računalnik (slika 4.12).

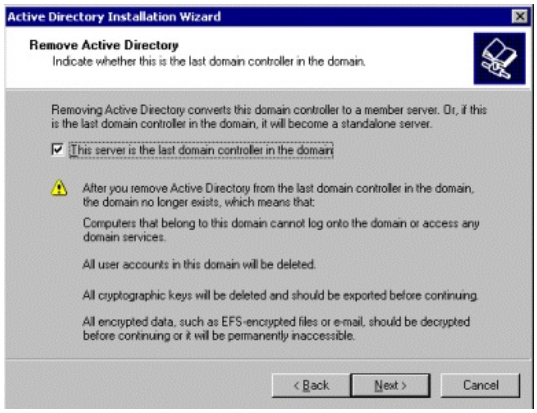


Slika 4.12: Ponovni zagon strežnika.

Po ponovnem zagonu pustimo, da strežnik teče en dan, brez dodatnega posega-nja v nastavitve. S tem zagotovimo, da bo replikacija, ki poteka v določenem intervalu pravilna in popolna. Isti postopek izvedemo tudi na ostalih dveh strežnikih.

4.3.2 Odstranitev starega strežnika iz domene

Postopek za odstranitev starega domenskega strežnika je enostaven. V ukazni vrstici strežnika, ki ga želimo odstraniti poženemo ukaz *dcpromo*, kar nam ponudi pogovorno okno za odstranitev domenskega strežnika (slika 4.13).

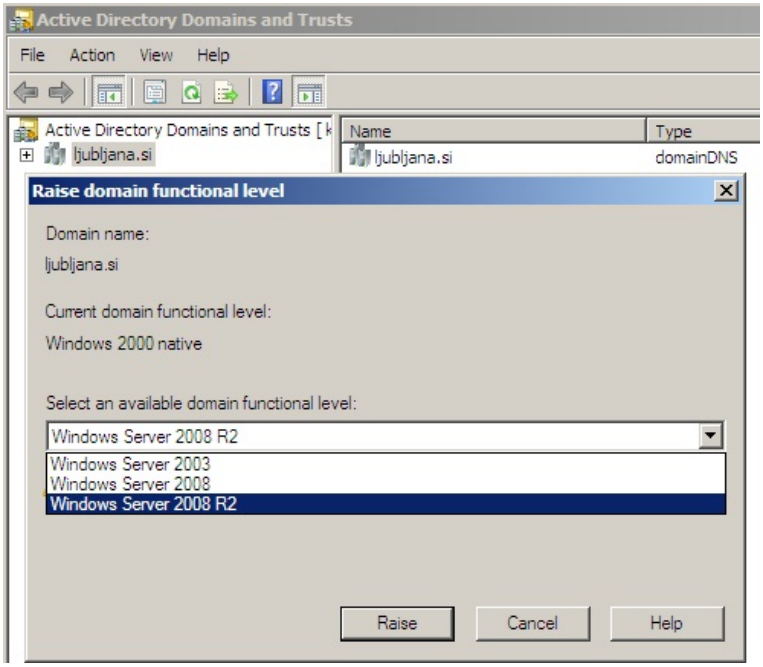


Slika 4.13: Odstranitev domenskega strežnika iz domene.

Ker strežnik ni zadnji domenski strežnik v domeni, odstranimo kljukico pred "This sever is the last domain contoler in the domain" in kliknemo "Next". Izvedel se bo postopek odstranitve domenskega strežnika. Po zaključku postopka, je strežnik član domene kot vsak drug strežnik ali delovna postaja. Za popolno odstranitev strežnika iz organizacije ga moramo odstraniti iz domene in izklopiti.

4.3.3 Dvig verzije domene na 2008 R2 Native

Zadnji korak v Fazi 2 je dvig verzije domene na zadnjo trenutno verzijo, Windows 2008 R2 Native. To lahko naredimo, saj smo do sedaj odstranili vse strežnike s starim operacijskim sistemom. V organizaciji imamo sedaj samo tri domenske strežnike z operacijskim sistemom Windows 2008 R2 Server. Verzijo domene dvignemo na podoben način, kot smo to storili v Fazi 1 (poglavje 4.2) ob dvigu domene na Windows 2000 Native.
Zaženemo orodje "Active Directory Domains and Trusts", z desno tipko miške kliknemo na ime domene in izberemo "Raise Domain Functional Level". V oknu, ki se nam odpre (slika 4.14) izberemo Windows 2008 R2 in to potrdimo s klikom na "Raise".



Slika 4.14: Dvig domene na Windows 2008 R2.

4.3.4 Replikacija Aktivnega Imenika

Vsak domenski strežnik mora vzdrževati bazo objektov aktivnega imenika. Replikacija zagotavlja da je baza objektov ves čas konsistentna z bazami ostalih domenskih strežnikov v organizaciji.

4.3.4.1 Pomen replikacije

Vse informacije, ki so shranjene v Aktivnem imeniku morajo biti ves čas dostopne tudi ostalim domenskim strežnikom. To nam zagotavlja dejstvo, da se informacija nahaja na več lokacijah, kar pomeni, da je informacija redundantna.

Glavni razlogi za zagotavljanje redundantnosti informacije so:

- **Hitrost dostopa do informacije**: Vsak odjemalec bo iskal informacijo na strežniku, ki je njemu najbližje, kar pomeni, da bo dobil informacijo kar se da najhitreje.
- **Razporejanje obremenitve**: V primeru večjega števila zahtev po informacijah iz aktivnega imenika, se zahteve razporedijo tudi na ostale domenske strežnike. Obremenjenost se tako razporedi med vse domenske strežnike v organizaciji.
- **Zaščita pred izpadom strežnika**: V primeru okvare enega izmed strežnikov, je informacija dostopna na drugem. Informacija bo dostopna dokler bo delujoč vsaj en domenski strežnik v organizaciji.

4.3.4.2 Delovanje replikacije

Določena informacija na različnih domenskih strežnikih v danem trenutku ni nujno konsistentna. Konsistentna pa zagotovo bo, če se nekaj časa ne bo spreminjala. To pomeni, da bodo vsi domenski strežniki hranili enako informacijo o nekem predmetu v aktivnem imeniku. Da lahko zagotovimo čim boljšo konsistentnost informacije, moramo zagotoviti, da se vsaka sprememba replicira iz enega domenskega strežnika na drugega. Vsak domenski strežnik beleži vsako ustvarjanje, spreminjane ali brisanje predmeta. Vsako tako spremembo pa posreduje naprej ostalim domenskim strežnikom oz. replikacijskim partnerjem. Replikacija seveda povzroča promet, v primeru MOL-a, lokalnih

povezavah, lahko pa tudi na WAN povezavah, če ima organizacija takšno informacijsko infrastrukturo.

V povezavi z ustvarjanjem prometa se pojavljata dve nasprotni si situaciji:

- Pogosteje kot se izvaja replikacija, večja je obremenjenost omrežja in strežnikov, kar povzroči zakasnitev, saj je pri visoki obremenjenosti težko zagotoviti konsistentno informacijo v vsakem trenutku.
- Redkeje, kot se izvaja replikacija starejšo informacijo bodo domenski strežniki hranili, kar prav tako povzroča zakasnitev.

Oba dejavnika sta odvisna od tega kako pogosto se informacija spreminja. Če se spreminja le redko, potem ta zakasnitev ni zelo pomembna.

Aktivni imenik uporablja dva načina replikacije:

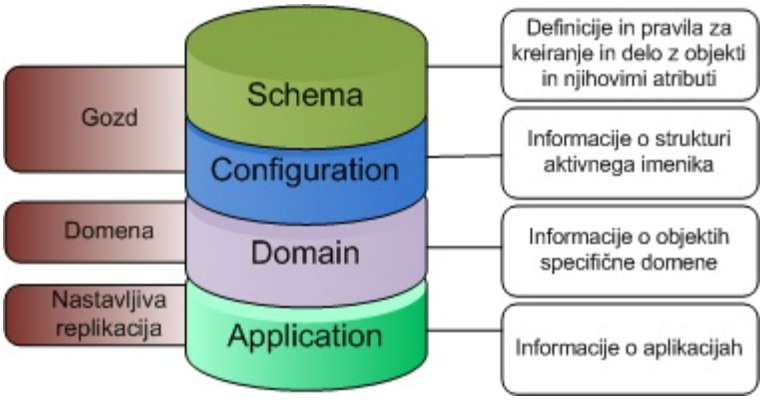
- **Replikacija Single Master**: Spremembe se lahko izvajajo le na enem domenskem strežniku, ki se imenuje PDC. Spremembe se iz PDC strežnika replicirajo na ostale. Tak način replikacije je uporabljal operacijski sistem Windows NT. Njena uporaba se opušča, ker izpad PDC strežnika pomeni, da spremembe v domeni niso mogoče.
- **Replikacija Multi-Master**: Spremembe se lahko izvajajo na kateremkoli domenskem strežniku, le-ta pa jih bo posredoval ostalim replikacijskim partnerjem. Tak način replikacije se uporablja tudi na MOL-u.

4.3.4.3 Particije in replike

Pri replikaciji se pojavljata še dva pojma. To sta:

- **Particije**: narekujejo kaj je lahko replicirano na kateri domenski strežnik.
- **Replike**: so kopije particije na različnih domenskih strežnikih.

Domenske particije (slika 4.15) se nahajajo znotraj domen in poddomen, kar pomeni, da je vsaka informacija replicirana le med strežniki ene domene ali poddomene. V domenskem gozdu obstajata dve globalni particiji, to sta "Schema" in "Configuration". Informacije v omenjenih particijah se replicirajo med vsemi strežniki v gozdu. Obstaja tudi particija "Application", ki je namenjena hranjenju informacij določene aplikacije.



Slika 4.15: Baza aktivnega imenika.

4.3.4.4 Replikacijski procesi

Aktivni imenik ne replicira celotnih predmetov ampak le posamezne informacije. Zaradi tega je manj podatkov, ki jih je potrebno replicirati in konfliktov, ki bi morebiti nastali pri spreminjanju različnih podatkov istega predmeta. Za reševanje konfliktov se uporablja ura. Če je informacija spremenjena na različnih lokacijah, je pomembno, da je na obeh lokacijah pravilno nastavljen čas, da lahko v aktivnem imeniku obstane prava informacija. Za sinhronizacijo časa se uporablja "Time Service".

4.4 Faza 3: Nadgradnja poštne infrastrukture

Ker sem bistvo Microsoft Exchange poštnega sistema že opisal v poglavju 3.2, bom v prvem delu tega poglavja predstavil glavne novosti Microsoft Exchange 2010 [3] verzije v primerjavi z obstoječo MS Exchange 2003 verzijo, v drugem delu pa opisal potek nadgradnje iz stare verzije na novo.

4.4.1 Microsoft Exchange 2010

MS Exchange 2010 je razdeljen na pet vlog, ki nudijo podporo komunikaciji in poslovnim procesom v organizaciji:

- **Vloga "MailBox" (MBX)**: Je jedro poštnega sistema, ki vzdržuje in hrani bazo vseh poštnih predalov in javnih map.
- **Vloga "Edge Transport" (EDGE)**: Se zaradi ločevanja zunanje in interne pošte, namesti izven internega omrežja v t.i. DMZ cono omrežja. Filtriranje nezaželene in okužene pošte se tako vrši izven interne infrastrukture. Pošta je naprej preusmerjena na HUB vlogo, ki jo potem posreduje do poštnih predalov MBX vlogi. EDGE vloga ni del projekta in ne bo nameščena.
- **Vloga "Hub Transport" (HUB)**: Skrbi za usmerjanje interne pošte, lahko pa se jo nastavi tudi za sprejemanje in oddajanje zunanje pošte. V tem primeru ta vloga tudi filtrira nezaželeno in okuženo pošto.
- **Vloga "Client Access Server" (CAS)**: Vsak odjemalec, ki želi vzpostaviti povezavo s poštnim sistemom jo mora narediti s CAS vlogo. CAS vloga upravlja z vsemi povezavami ne glede na vrsto povezujoče se naprave. Povezavo lahko vzpostavijo odjemalci kot so Outlook 2003 in Outlook 2010 in vse ostale naprave, ki podpirajo MAPI, POP3 in IMAP3 protokol.
- **Vloga "Unified Messaging" (UM)**: Namenjena je postavitvi glasovne pošte in povezovanju poštnega sistema s telefonskim omrežjem. UM vloga ni del projekta in ne bo nameščena.

Bistvene izboljšave v primerjavi z MS Exchange 2003:

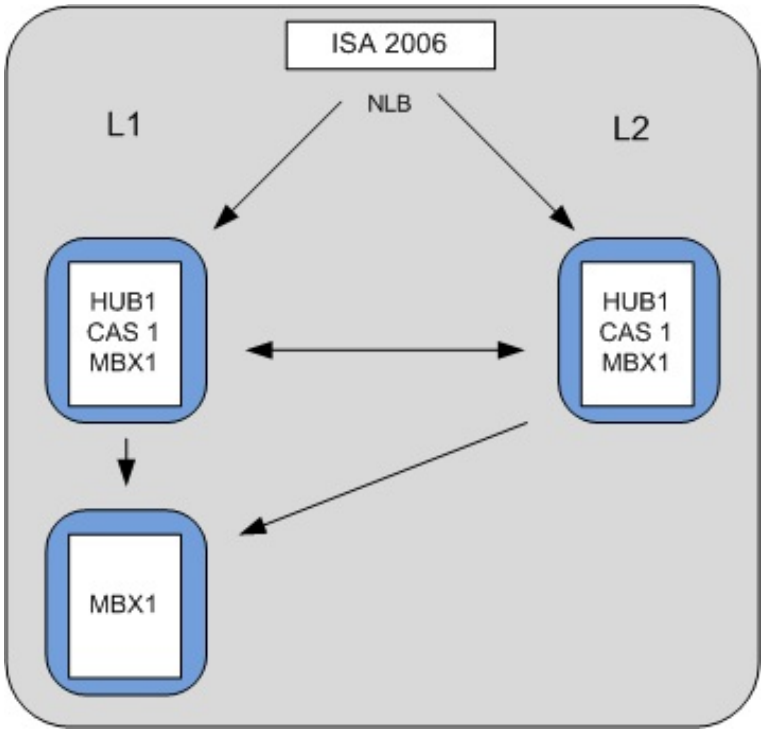
- Boljša protivirusna zaščita
- Boljša zaščita pred nezaželeno pošto
- Združljivost s 64 bitno strojno opremo
- Ločevanje vlog, kar omogoča, da procesorsko zahtevne vloge razdelimo na več različnih strežnikov
- Podpira poštne baze do velikosti 16TB
- PowerShell podpora, ki omogoča avtomatizirano in skriptirano izvrševanje ukazov
- Boljši grafični vmesnik za upravljanje celotnega poštenga sistema

4.4.2 Izvedba nadgradnje poštnega sistema

Izvedba nadgradnje bo potekala v petih korakih:

- Priprava obstoječe infrastrukture
- Namestitev poštnega strežnika Microsoft Exchange 2010
- Nastavitev novega strežnik
- Selitev uporabnikov na nov poštni sistem
- Ukinitev stare poštne infrastrukture

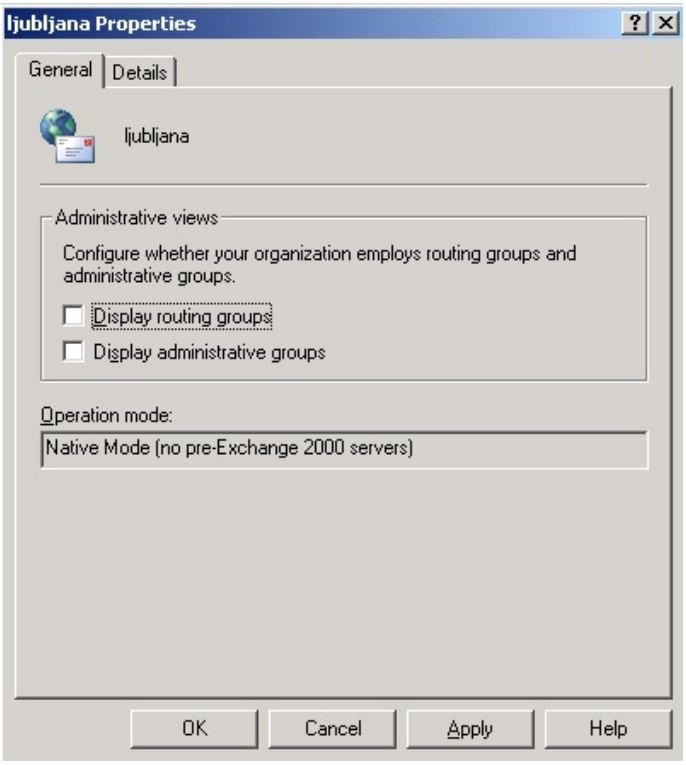
Po zaključeni nadgradnji bo poštni sistem postavljen kot prikazuje slika 4.16. V sistemu se bosta nahajala dva strežnika z vlogami MBX, CAS in HUB. Dva strežnika bosta na lokaciji L1 drugi pa na lokaciji L2. Na tretjem strežniku bo tekla le MBX vloga in opravljala funkcijo DRC-ja v primeru, da pride do okvare katerega izmed ostlaih dveh strežnikov. Vse tri MBX vloge bodo hranile vse poštne predale in javne mape v organizaciji. Vsa poštna infrastruktura bo tekla na virtualnih strežnikih, ki jih poganja VMware ESX 3.5 predstavljen v poglavju 3.3. HUB vloga bo opravljala tudi vlogo sprejemanja in oddajanje ter filtriranja zunanje pošte. Ves odhodni in dohodni promet bo nadziral strežnik ISA 2006, ki ga je MOL ustrezno nastavila. ISA strežnik bo opravljal tudi funkcijo NLB-ja, kar pomeni, da bo s prihajajočo dohodno pošto enakomerno obremenil oba strežnika s HUB vlogo.



Slika 4.16: Shema poštne infrastrukture.

4.4.2.1 Priprava obstoječe infrastrukture

Pred nadgradnjo moramo preveriti ali je obstoječa poštna infrastruktura nastavljena na "Native mode". To pomeni, da v poštni infrastrukturi ne obstajajo poštni strežniki starejši od Windows Exchange 2000. To preverimo tako, da odpremo Exchange konzolo z desno tipko miške kliknemo na organizacijo in v oknu, ki se nam odpre (Slika 4.17) preverimo ali je polje "Operation Mode" nastavljeno na "Native mode". Verzija domene mora biti nastavljena vsaj na Windows 2000 ali več, kar pa je, saj smo jo v poglavju 4.3.3 nastavili na Windows 2008 R2.



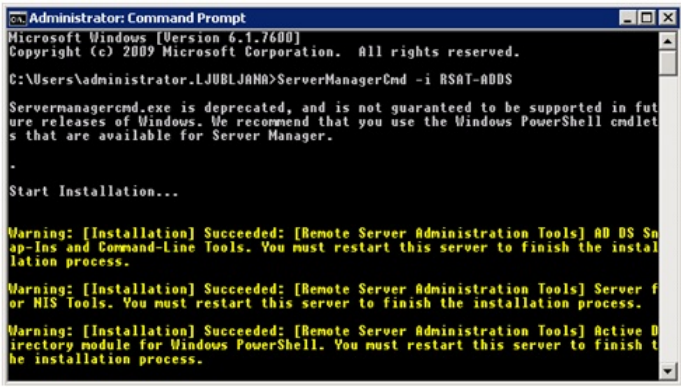
Slika 4.17: Exchange 2003 Operation mode.

V postopku priprave na nadgradnjo je potrebno ustrezno pripraviti tudi:

- Orodja za namestitev strežnika Exchange
- Podporo za pravice starega strežnika Exchange
- Shemo
- Aktivni imenik

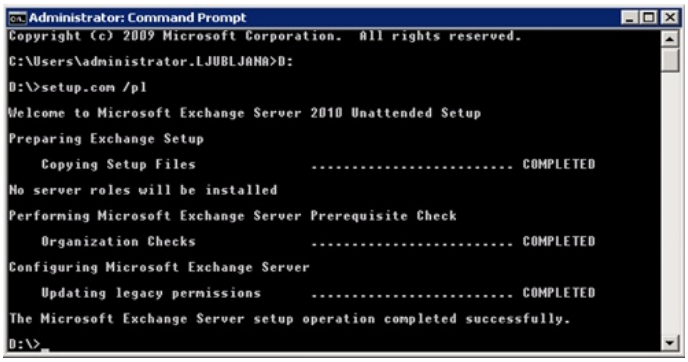
Vse to naredimo iz ukazne vrstice tako, da poženemo ukaz Setup.com z ustreznimi parametri. Orodje Setup.com se nahaja v mapi z namestitvenimi datotekami Exchange.

1. Namestimo potrebna orodja z ukazom *s*erverManagerCmd -i RSAT-ADDS (Slika 4.18).



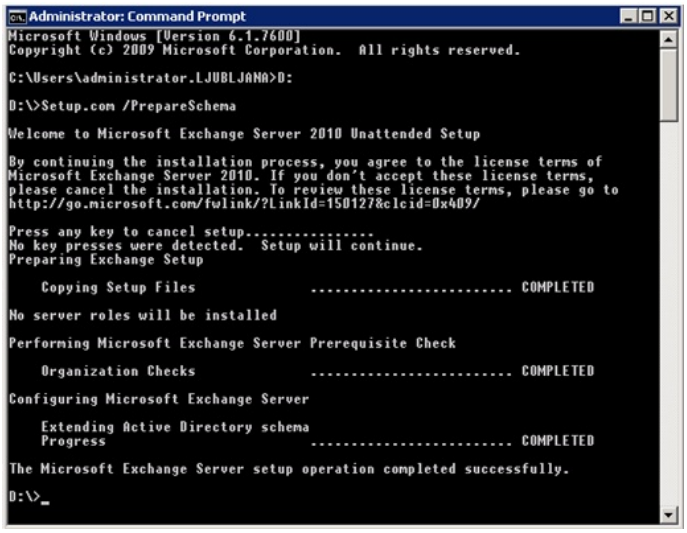
Slika 4.18: Orodja za namestitev strežnika.

2. Podporo za pravice starega strežnika Exchange vklopimo z ukazom *s*etup.com /PrepareLegacyExchangePermissions (Slika 4.19).



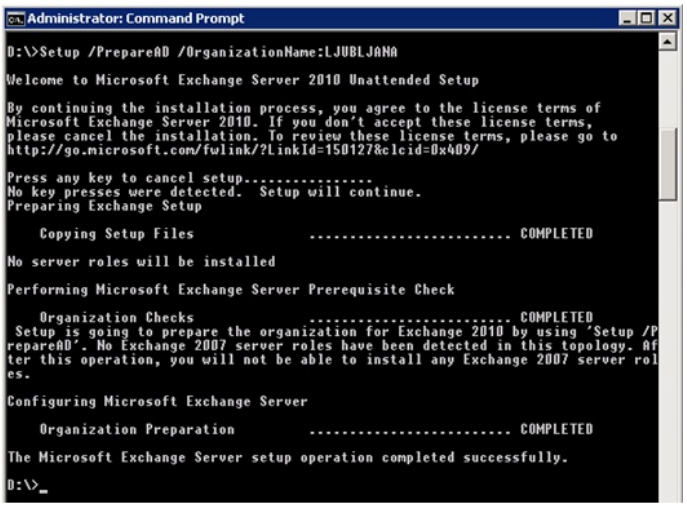
Slika 4.19: Pravice starega strežnika Exchange.

3. Shemo aktivnega imenika razširimo z ukazom *s*etup.com /PrepareSchema (Slika 4.20).



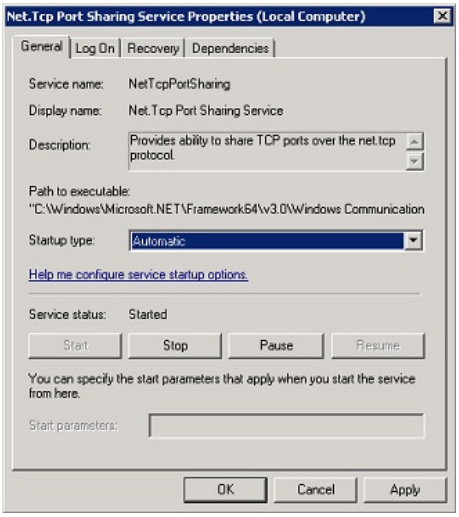
Slika 4.20: Priprava sheme aktivnega imenika.

4. Aktivni imenik pripravimo z ukazom *s*etup /PrepareAD /Organization-Name:LJUBLJANA (Slika 4.21).



Slika 4.21: Priprava aktivnega imenika.

5. Namestitev zahteva, da je zagon servisa "Net.Tcp Port Sharing Service" nastavljen na "Automatic". To nastavimo z orodjem "services.msc" (Slika 4.22).



Slika 4.22: Net.Tcp Port Sharing Service.

4.4.2.2 Namestitev poštnega strežnika Microsoft Exchange 2010

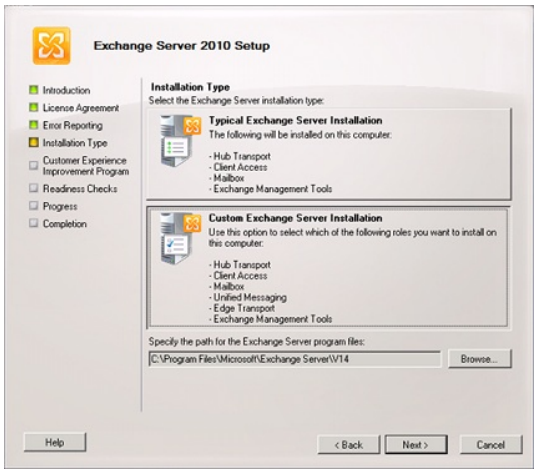
Vsi trije poštni strežniki se namestijo na enak način le, da pri strežniku, ki opravlja vlogo DRC-ja namestimo le vlogo "mailbox".

Koraki namestitve novega strežnika:

1. Iz namestitvenega medija zaženemo datoteko Setup.exe in odpre se nam namestitevno okno (Slika 4.23). Kliknemo na "Install Microsoft Exchange".

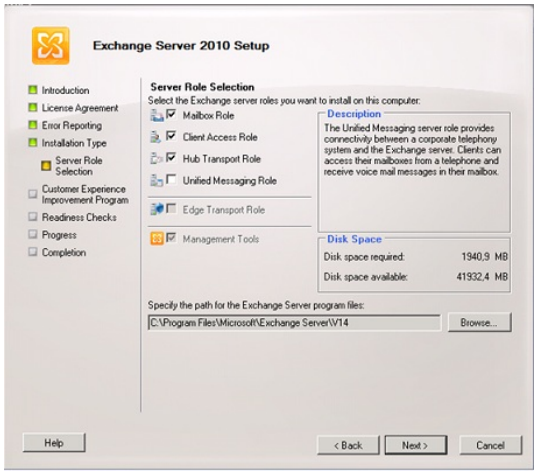
Slika 4.23: Namestitveno okno.

2. V naslednjih treh korakih kliknemo "Next", da pridemo do okna, ki ga prikazuje slika 4.24 na katerem izberemo "Custom Exchange Server Installation".



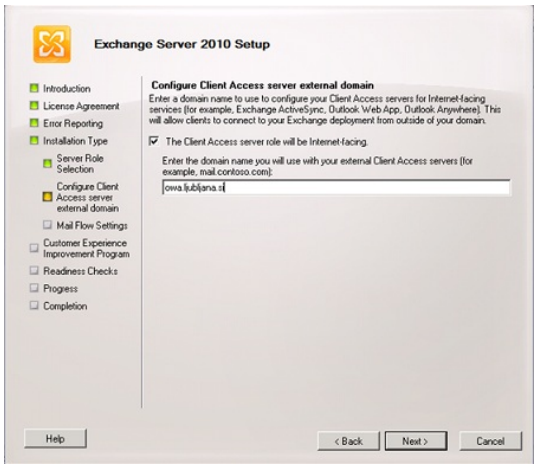
Slika 4.24: Izbira namestitve.

3. V tem koraku (Slika 4.25) izberemo vloge, ki jih želimo namestiti na strežnik. V dveh primerih izberemo vloge "Hub Transport Role", "Client Access Role" in "Mailbox Role". Pri namestitvi tretjega strežnika, ki opravlja funkcijo DRC-ja izberemo le vlogo "Mailbox Role". Kliknemo "Next".



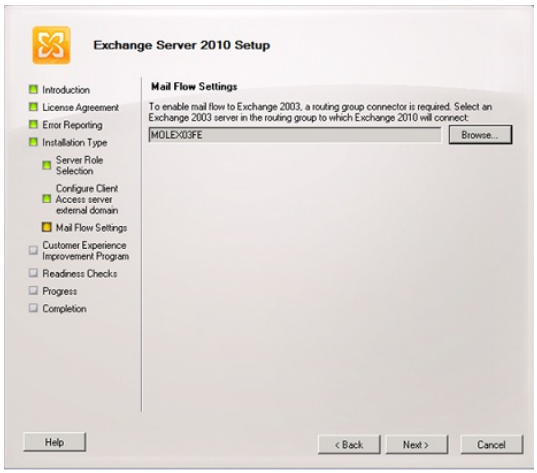
Slika 4.25: Izbira vlog.

4. Poštni sistem bo odprt tudi za uporabnike, ki potrebujejo dostop do elektronske pošte tudi, ko so doma ali na službenem potovanju. V tem koraku (Slika 4.26) vpišemo naslov na katerem bo poštni strežnik dosegljiv za odjemalce zunaj omrežja in kliknemo Next.



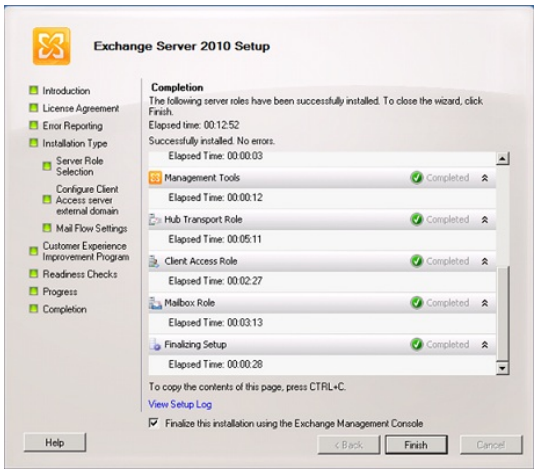
Slika 4.26: Zunanji naslov strežnika.

5. Da zagotovimo nemoteno delovanje elektronske pošte moramo star in nov poštni sistem ustrezno povezati. Ob namestitvi izberemo s katerim obstoječim strežnikom naj se novi poveže. Izberemo strežnik, na katerem teče vloga "Front End".



Slika 4.27: Povezava z obstoječim sistemom.

6. Na naslednjem oknu kliknemo Next in nato Finish. S tem smo dokončali namestitev strežnika (Slika 4.28).

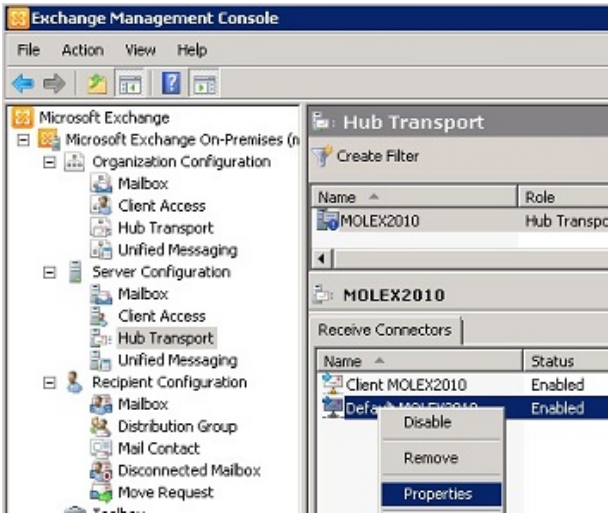


Slika 4.28: Zaključek namestitve.

4.4.2.3 Nastavitev novega strežnika

Namestitev večino nastavitev strežnika prevzame iz Aktivnega imenika, kjer se nahajajo nastavitve stare poštne infrastrukture. Vsa interna komunikacija novega poštnega sistema deluje že takoj po namestitvi. Vseeno pa je potrebno pred selitvijo uporabnikov na nov poštni sistem potrebno še dodatno nastaviti.

1. Da bo poštni sistem lahko sprejemal pošto iz zunanjega sveta moramo nastaviti vtič za dohodno pošto (ang. Receive Connector). Odpremo Exchnage konzolo in z desno tipko miške kliknemo na privzeti vtič za dohodno pošto in nato kliknemo "Properties", kot kaže slika 4.29.

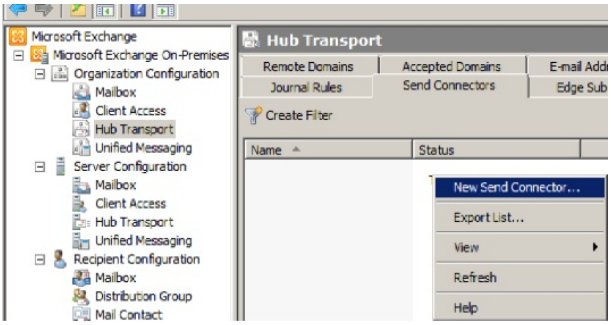


Slika 4.29: Dohodna pošta.

V oknu, ki se nam odpre izberemo zavihek "Permissions Groups" in označimo skupine od katerih želimo prejemati pošto (Slika 4.30).

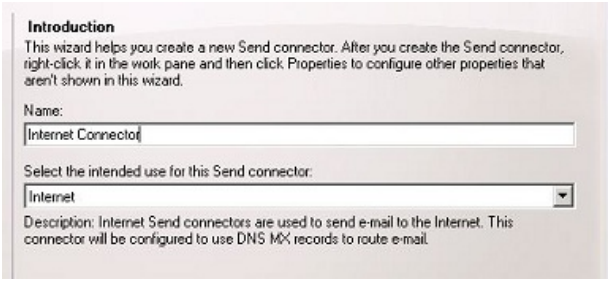
Slika 4.30: Skupine.

2. Za pošiljanje pošte moramo nastaviti vtič za odhodno pošto (ang. Send Connector). Izberemo "New Send Connector", kot kaže slika 4.31.



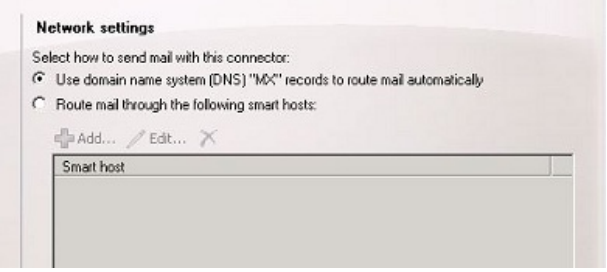
Slika 4.31: Odhodna pošta.

Vpišemo ime vtiča in izberemo, da bo pošiljal pošto, ki je namenjena zunanjemu svetu (Slika 4.32).



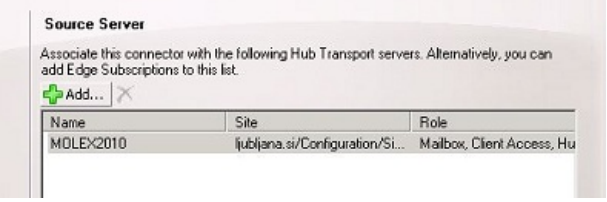
Slika 4.32: Ime vtiča za odhodno pošto.

Izberemo prvo možnost (Slika 4.33), kar pomeni, da bo za usmerjanje pošte uporabil zapise na DNS strežniku.



Slika 4.33: Zapisi na DNS strežniku.

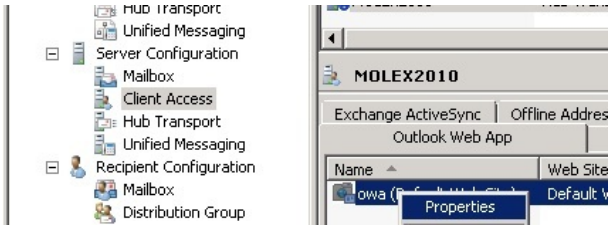
V naslednjem oknu izberemo strežnik iz katerega se bo odpošiljala pošta (Slika 4.34).



Slika 4.34: Strežnik odhodne pošte.

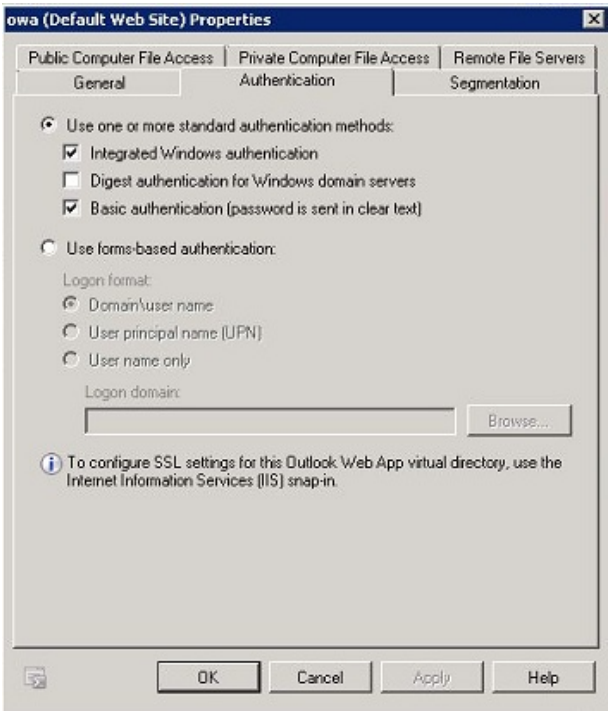
Na zadnjem oknu kliknemo "Next" in nato "Finish".

3. Potrebno je nastaviti tudi spletni portal, ki omogoča dostop do elektronske pošte iz spletnega brskalnika (eng. Outlook Web Access). Z desno tipko miške kliknemo na "owa" in izberemo "Properties", kot kaže slika 4.35.



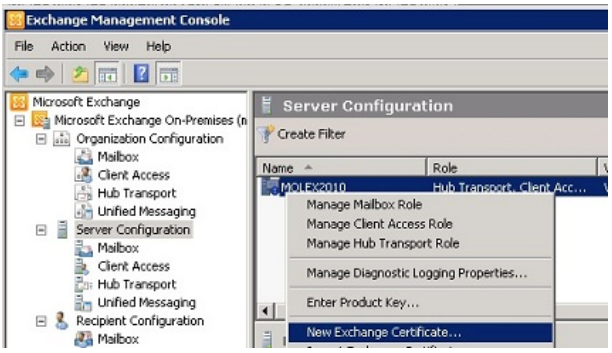
Slika 4.35: Spletni dostop.

V oknu, ki se nam odpre izberemo zavihek "Authentication" in ga nastavimo kot kaže slika 4.36



Slika 4.36: Avtentikacija.

4. Da je uporaba poštnih storitev varna je potrebno strežniku dodati ustrezen certifikat. Zahtevo za certifikat ustarimo tako, da izberemo "New Exchange Certificate", kot je prikazano na sliki 4.37.

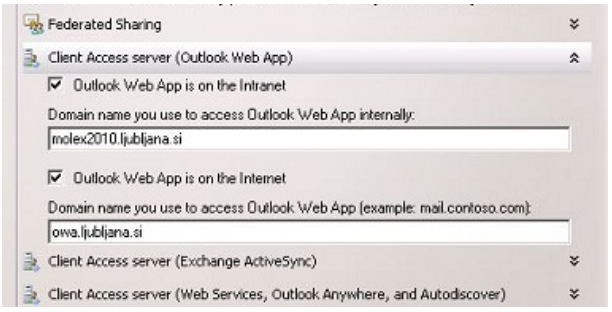


Slika 4.37: Zahteva za certifikat.

Vpišemo ime certifikata (Slika 4.38).

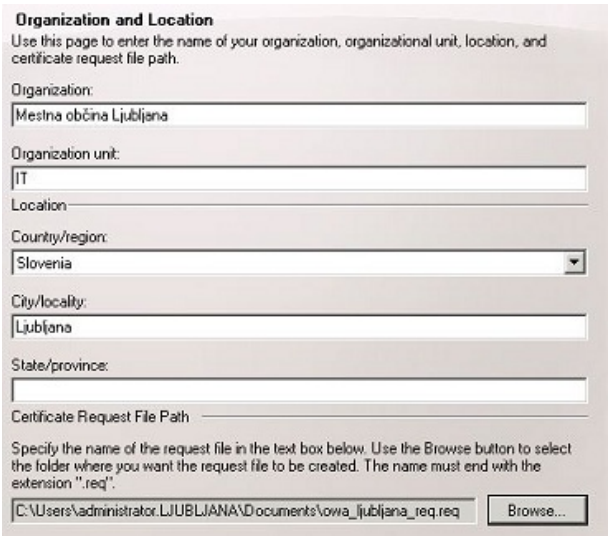
Slika 4.38: Ime certifikata.

Izberemo servise za katere bomo certifikat uporabili. V našem primeru se bo certifikat uporabljal le za spletni dostop do elektronske pošte (Slika 4.39).



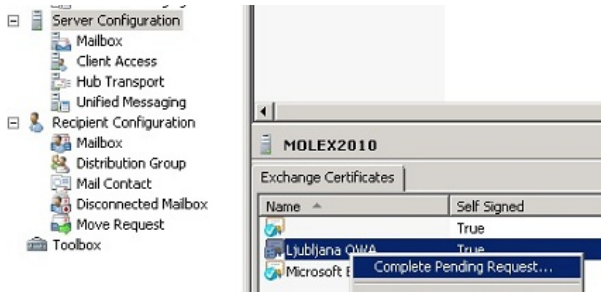
Slika 4.39: Servisi, ki uporabljajo certifikat.

V naslednjem oknu (Slika 4.40) vnesemo podatke organizacije in izberemo pot kamor želimo odložiti zahtevo za certifikat.



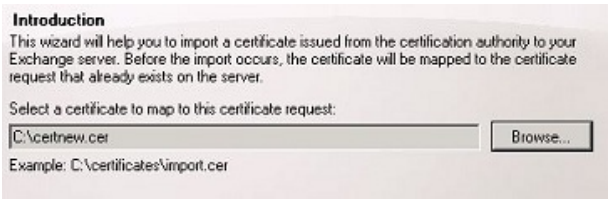
Slika 4.40: Podatki organizacije.

Kliknemo "Next" in "Finish". Zahtevo za certifikat pošljemo javnemu izdaljatelju certifikatov kot sta PostarCA ali Tawte. Izdajatelj nam izda certifikat, ki ga nato nastavimo na poštnem strežniku. Izberemo "Complete Pending Request" (Slika 4.41).



Slika 4.41: Zaključek prošnje za izdajo certifikata.

In izberemo datoteko, ki nam jo je poslal izdajatelj certifikatov (Slika 4.42).



Slika 4.42: Uvoz certifikata.

Kliknemo "Next" in nato "Finish".

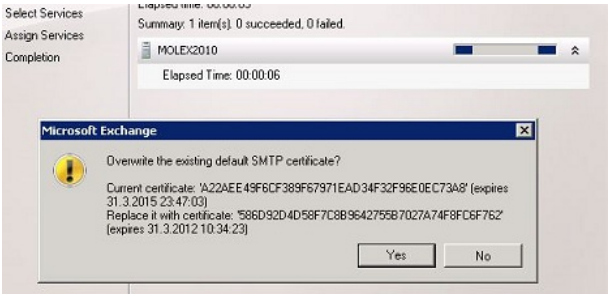
Certifikat je potrebno povezati še z ustreznimi protokoli. To naredimo tako, da z desno tipko miške kliknemo na "Assign Services to Certificate" (Slika 4.43).

Slika 4.43: Povezava certifikata s protokoli.

Kliknemo "Next" in izberemo protokole, za katere želimo, da se cetifikat uporablja (Slika 4.44).

Slika 4.44: Protokoli.

Kliknemo "Assign" in potrdimo prepis certifikata z novim, kot kaže slika 4.45.



Slika 4.45: Zaključek uvoza certifikata.

Za konec moramo ponovno zagnati vse servise, to naredimo tako, da v ukazni vrstici zaporedno izvedemo ukaze:

1. IISReset /NoForce
2. Net Stop MSExchangeIS
3. Net Start MSExchangeIS

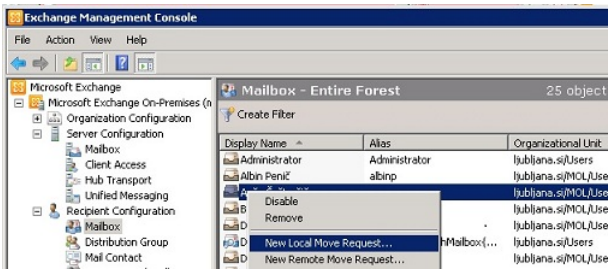
Pošni strežnik je sedaj pripravljen, da sprejme poštne predale starega poštnega strežnika.

4.4.2.4 Selitev uporabnikov na nov poštni sistem

Microsoft Exchange 2010 Server, uporablja nov način migracije poštnih predalov. Če želimo preseliti poštni predal moramo uporabiti t.i. prošnjo za premik poštnega predala (ang. Move Mailbox Request). Za določen predal naredimo prošnjo za premik predala v novo poštno bazo. Strežnik izvede premik, ko je to mogoče. Ta funkcionalnost je zelo dobrodošla, saj lahko označimo za premik vse poštne predale, strežnik pa jih bo premaknil, ko bo to mogoče. V preteklosti je bilo potrebno ob prehodu na nov poštni strežnik migrirati posamezne predale enega po enega. Pri migraciji poštnih predalov iz Exchange 2003 na Exchange 2010 poštni sistem so poštni predali med migracijo nedosegljivi. Čas migracije je odvisen od velikosti poštnega predala in lahko traja od ene do deset minut.

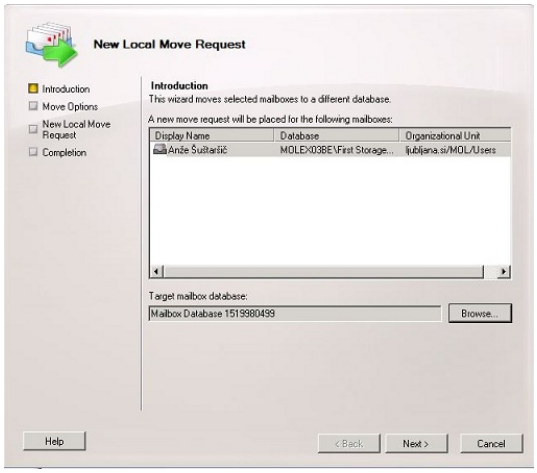
Koraki migracije enega poštnega predala:

1. Zaženemo konzolo strežnika Exchange 2010 in pod "Recipient Configuration" izberemo polje "Mailbox". V srednjem oknu z desno miškino tipko kliknemo na uporabnika(e), ki jih želimo seliti na nov poštni sistem in izberemo "New Local Move Request", kot kaže slika 4.46.



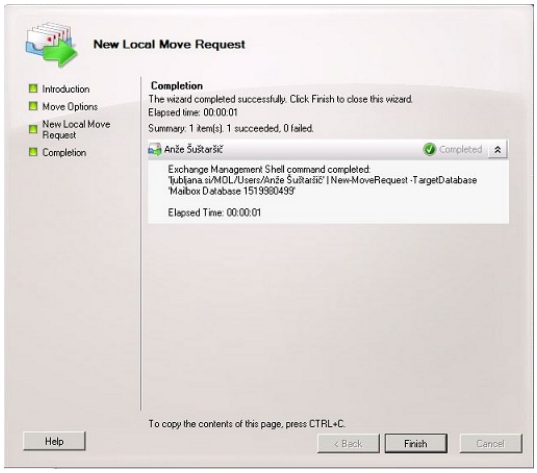
Slika 4.46: Izbira poštnega predala.

2. V naslednjem oknu v polju "Target mailbox database" izberemo bazo na novem poštnem sistemu in kliknemo Next (Slika 4.47).



Slika 4.47: Izbira baze.

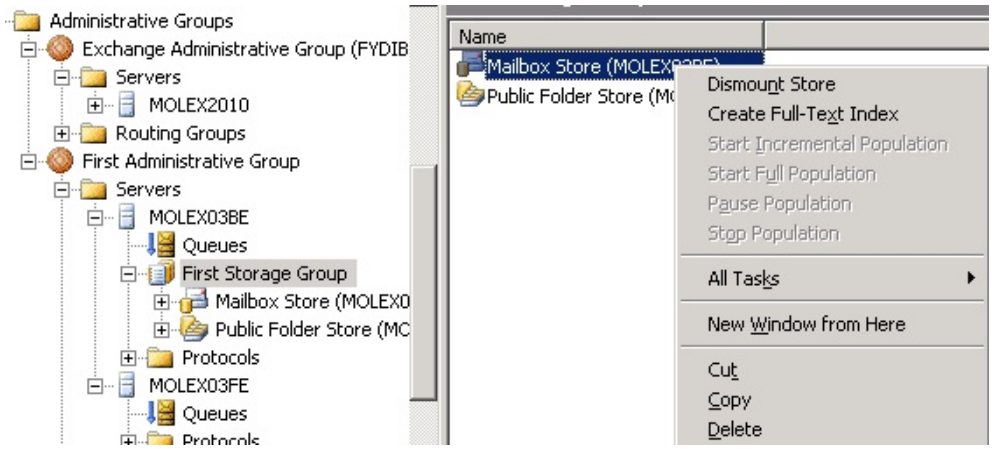
3. V naslednjem oknu kliknem Next in nato Finish. Prošnjo za premik poštenga predala smo naredili. Strežnik bo naredil premik takoj, ko bo to mogoče (Slika 4.48).



Slika 4.48: Selitev poštnega predala.

4.4.2.5 Ukinitev stare poštne infrastrukture

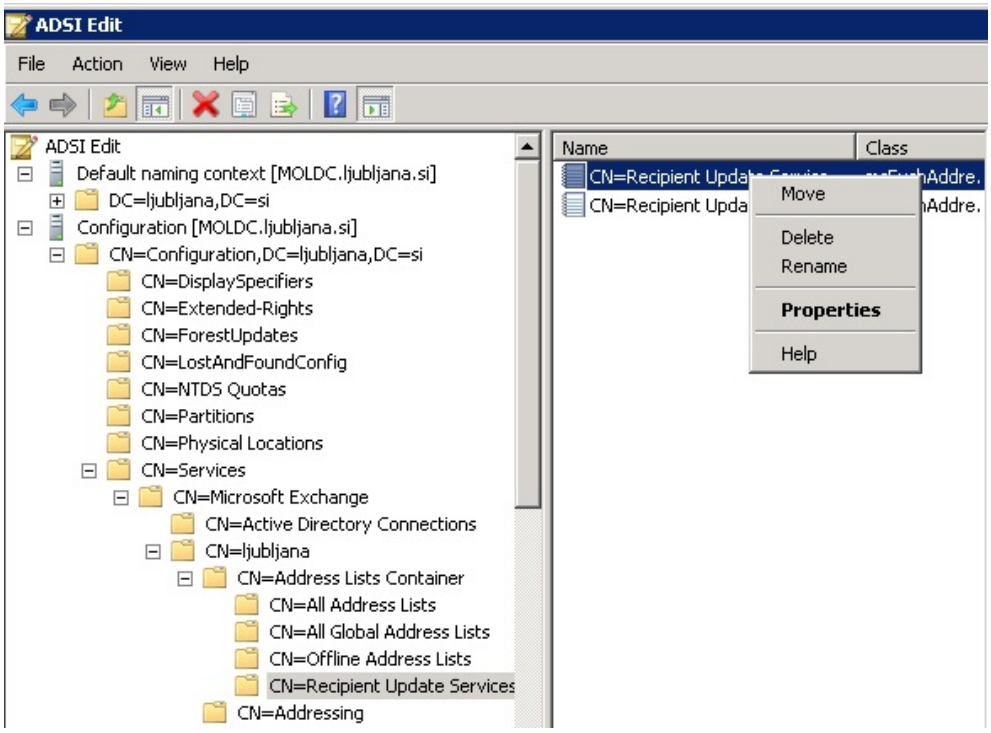
Preden odstranimo stare poštne strežnike je priporočljivo, da jih za nekaj dni le ugasnemo in spremljamo ali vse poštne storitve delujejo normalno samo z novimi poštnimi strežniki. Če je vse v redu lahko pričnemo z odstranjevanjem starih strežnikov. Na starih strežnikih najprej pobrišemo staro poštno bazo in javne mape (Slika 4.49).



Slika 4.49: Brisanje baze in javnih map.

Naslednji korak je, da z ukazom *Get-RoutingGroupConnector — Remove-RoutingGroupConnector -confirm:$false* odstranimo povezavo med starim in novim poštnim sistemom.

Iz aktivnega imenika je potrebno ročno z orodjem ADSEDIT pobrisati zapis "Recipient Update Service", ker ga ne potrebujemo več (Slika 4.50).

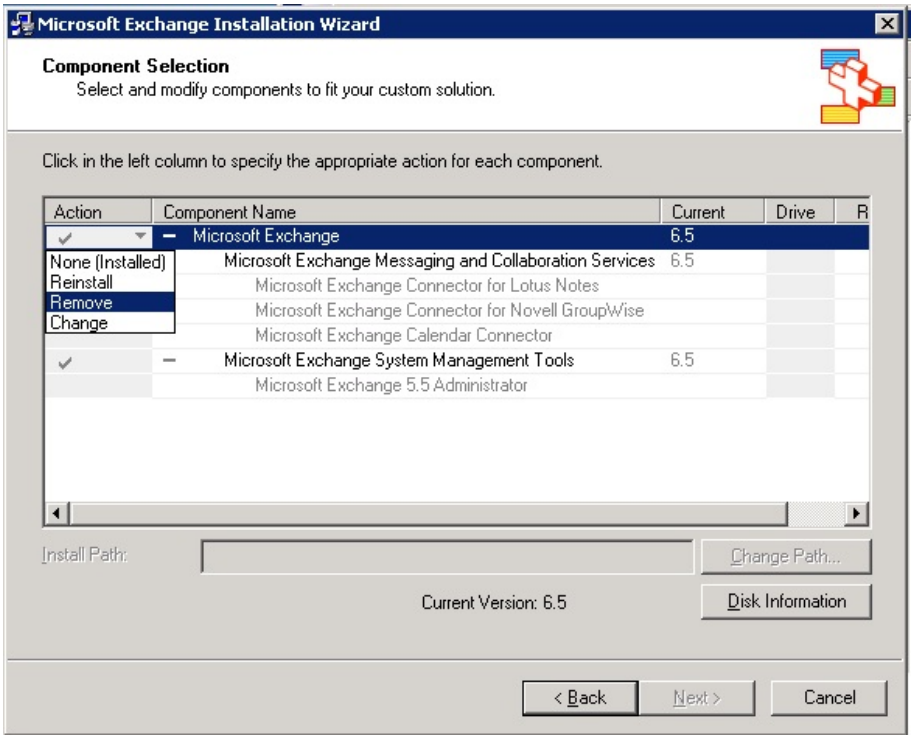


Slika 4.50: Brisanje Recipient Update Service.

Zadnji korak je odstranitev Microsoft Exchange iz strežnikov. Odpremo orodje "Add Remove Programs", izberemo Microsoft Exchange in kliknemo na "Remove" (Slika 4.51).

Slika 4.51: Odstranitev starega poštnega sistema.

Za vse tri komponente izberemo možnost "Remove" in potrdimo s klikom na "Next", kot kaže slika 4.52.



Slika 4.52: Zaključek odstranitve.

Po zaključku odstranitve imamo v organizaciji delujoč nov poštni sistem, ki temelji na najnovejšem poštnem strežniku Microsoft Exchange 2010.

Poglavje 5

Zaključek

Sodobna informacijska infrastruktura nam omogoča lažje in hitrejše upravljanje polovnih procesov. V diplomski nalogi sem predstavil postopek nadgradnje poštnega strežnika in Aktivnega imenika, ki v vsaki organizaciji predstavljata osnovni komponenti informacijske infrastrukture. Nadgradnja je pokazala, da je potrebno dosledno slediti korakom, ki so potrebni za izvedbo posamezne faze. Vsekakor je pomembno, da se na prehod na novo infrastrukturo dobro pripravimo. Pri izvedbi projekta nisem imel večjih težav, saj sem se na nadgradnjo dobro pripravil v testnem okolju, ki ga imamo v podjetju. Vedno je priporočljivo, da se nadgradnja opravi v ekvivalentno postavljenem testnem okolju, kjer se odkrijejo možne težave, hkrati pa se lahko nanje pripravimo in se jim pri dejanski nadgradnji izognemo. Težave, na katere sem naletel pri nadgradnji v testnem okolju so bile povezane z napačnimi nastavitvami in nepravilmin zaporedjem korakov, ki so potrebni za uspešno nadgradnjo.
Med izvedbo projekta sem največ časa porabil za načrtovanje nove infrastrukture. Izdelana je tako, da lahko uporabniki kljub odpovedi enega izmed strežnikov nemoteno opravljajo svoje delo. Ker je infrastruktura postavljena na dveh lokacijah se podatki v primeru hujših nesreč, kot je recimo požar, ne izgubijo, saj so dostopni na drugi lokaciji.
Z novo informacijsko infrastrukturo je mestna občina poenostavila upravljanje informacijskega sistema in izboljšala varnost in zaščito podatkov. MOL mora poskrbeti še za posodobitev delovnih postaj na operacijski sistem Windows 7 in pisarniški paket Microsoft Office 2010. Z namestitvijo novejših aplikacij bodo uporabniki lahko izkoriščali vse prednosti nove informacijske infrastukture. Ta del posodobitve ni bil del projekta in ga bo mestna občina izvedla sama.

Slike

Literatura

[1] William R. Stanek, *Windows Server 2008 Administrator's Pocket Consultant, Second Edition [Updated for R2]*, Redmond, Washington: Microsoft Press, 2009.

[2] Stan Reimer, *Active Directory for Microsoft Windows Server 2003 Technical Reference*, Redmond, Washington: Microsoft Press, 2003.

[3] William R. Stanek, *Microsoft Exchange Server 2010 Administrator's Pocket Consultant*, Redmond, Washington: Microsoft Press, 2009.

[4] William R. Stanek, *Windows Server 2003 Inside-Out*, Redmond, Washington: Microsoft Press, 2004.

[5] Rene J. Chevance, *Server Architectures*,Burlington, Elsevier Digital Press, 2005.

[6] Kiran Mani, *On the Edge: A Comprehensive Guide to Blade Server Technology*, Singapore, John Wiley and Sons, 2007.

[7] Jon William Toigo, *The Holy Grail of Data Storage Management*, New Jersey, A Person Education Company, 1999.

[8] (2010) Virtualizacija Dostopno na: http://www.vmware.com/virtualization/what-is-virtualization.html

[9] (2010) Microsoft Exchange Server Dostopno na: http://en.wikipedia.org/wiki/Microsoft_Exchange_Server

[10] (2010) Lightweight Directory Access Protocol Dostopno na: http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

[11] (2010) Aktivni Imenik. Dostopno na: http://en.wikipedia.org/wiki/Active_Directory

[12] (2010) Kerberos. Dostopno na:
http://en.wikipedia.org/wiki/Kerberos_*protocol*