UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Jure Jereb

Vpeljava oddaljenega dostopa do namizij in aplikacij v podjetju

DIPLOMSKO DELO
NA VISOKOŠOLSKEM STROKOVNEM ŠTUDIJU

Mentor: doc. dr. Mojca Ciglarič

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: 00493/2009
Datum: 15.12.2009

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

Kandidat: **JURE JEREB**

Naslov: **VPELJAVA ODDALJENEGA DOSTOPA DO NAMIZIJ IN APLIKACIJ V PODJETJU**

REMOTE DESKTOP AND APPLICATIONS: IMPLEMENTATION IN THE ORGANIZATION

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija

Tematika naloge:

Opišite začetno stanje v izbranem podjetju in potrebe, ki so privedle do odločitve za vpeljavo oddaljenega dostopa do namizij in aplikacij. Preučite možne rešitve, ki so dostopne na trgu, komentirajte njihove prednosti in slabosti ter utemeljite izbiro. Opišite izvedbo in rezultate projekta vpeljave ter navedite prednosti in morebitne slabosti novega sistema.

Mentor:
M. Ciglarič
doc. dr. Mojca Ciglarič

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

Dekan:
prof. dr. Franc Solina

I Z J A V A O A V T O R S T V U

diplomskega dela

Spodaj podpisani/-a: **JURE JEREB**

z vpisno številko: **63030116**

sem avtor/-ica diplomskega dela z naslovom:

Vpeljava oddaljenega dostopa do namizij in aplikacij v podjetju

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal/-a samostojno pod mentorstvom (naziv, ime in priimek):

  doc. dr. Mojce Ciglarič

- 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 _____ Podpis avtorja/-ice: _____

---- original izdane teme diplomskega dela ----

Zahvala

Zahvaljujem se mentorici doc. dr. Mojci Ciglarič za pomoč, strokovne nasvete in usmeritve pri izdelavi diplomskega dela.

Hvala tudi izvršnemu direktorju informatike koncerna Kolektor Group, Bojanu Poženelu, ki mi je omogočil izvedbo projekta, opisanega v diplomskiem delu, in sistemskemu administratorju Boštjanu Berglezu, ki mi je pri izvedbi projekta pomagal.

Posebna zahvala pa tudi vsem domačim in ostalim, ki so mi tekom študija in pisanja diplomskega dela stali ob strani.

Kazalo vsebine

Seznam slik

Seznam tabel

Razlaga uporabljenih kratic in simbolov

Kratica	Angleški pomen	Slovenski pomen in razlaga
RD	Remote Desktop	Oddaljeno namizje.
RDS	Remote Desktop Services	Microsoftova tehnologija za oddaljeni dostop.
RDP	Remote Desktop Protocol	Protokol, ki se uporablja pri Microsoftovi tehnologiji za oddaljenih dostop.
RDC	Remote Desktop Connection	Povezava do oddaljenih namizij.
SSL	Secure Sockets Layer	Omrežni protokol, ki zagotavlja visoko stopnjo varnosti komunikacije.
VPN	Virtual Private Network	Navidezno zasebno omrežje.
PC	Personal Computer	Osebni računalnik.
RDS CALs	Remote Desktop Client Access Licenses	Microsoftove licence za oddaljeni dostop.
VDI	Virtual Destkop Infrastructure	Microsoftova infrastruktura za virtualna namizja.
HTTP	Hyper Text Transfer Protocol	Komunikacijski protokol za prenos informacij po spletu.
HTTPS	Hyper Text Transfer Protocol Secure	Zavarovana različica protokola HTTP, ki uporablja SSL/TLS.
DNS	Domain Name System	Sistem domenskih imen. Omogoča pretvorbo imen domen v IP naslove.
DHCP	Dynamic Host Configuration Protocol	Omrežni protokol za dinamično nastavitev gostitelja. Računalnikom v omrežju omogoča, da pridobijo svoje omrežne nastavitve od strežnika.
TCP/IP	Transmission Control Protocol/Internet Protocol	Protokol za nadzor prenosa in internetni protokol oziroma Internetni sklad protokolov (angleško: Internet protocol suite) je množica protokolov, ki izvaja protokolski sklad, prek katerega teče internet.
IPv4	Internet Protocol version 4	Internetni protokol verzije 4. Protokol omrežne plasti, ki je namenjen naslavljanju naprav v omrežju.
IPv6	Internet Protocol version 6	Internetni protokol verzije 6. Naslednik protokola IPv4.
IIS	Internet Information Services	Microsoftov spletni strežnik. Del operacijskega sistema Windows Server 2008.
AD	Active Directory	Aktivni imenik. Microsoftova tehnologija, ki omogoča številne omrežne storitve.

OU	Organizational Unit	Organizacijska enota znotraj aktivnega imenika.
GPO	Group Policy	Skupinske politike. Microsoftovo orodje, ki omogoča konfiguracijo uporabniških računov in računalnikov.
NLB	Network Load Balancing	Razporeditev obremenitve omrežja.
FQDN	Fully Qualified Domain Name	Polno domensko ime strežnika.
USB	Universal Serial Bus	Univerzalno serijsko vodilo.

Povzetek

Remote Desktop Services oziroma terminalske storitve predstavljajo Microsoftovo rešitev za večuporabniško okolje na Windows strežniku, ki omogoča uporabnikom dostop do oddaljenih podatkov in aplikacij, nameščenih na terminalskih strežnikih. S pomočjo terminalskih storitev lahko uporabniki dostopajo do terminalskih strežnikov iz omrežja podjetja ali pa preko interneta. Do uporabnika se prenaša samo zaslonska slika, zato za takšno delo ne potrebujemo zmogljivega računalnika. Uporaba terminalskih storitev pa poleg tega prinaša še veliko dodatnih prednosti. Med drugim tudi: zmanjšanje stroškov (ni potrebe po konstantni nadgradnji osebnih računalnikov, ugodno licenciranje), večjo zanesljivost in dostopnost (v omrežju postavimo farmo strežnikov, tako da so tudi ob izpadu enega izmed strežnikov uporabnikom vse storitve, programi in podatki še vedno na voljo), večjo varnost (vsi podatki so shranjeni na varni centralni lokaciji, kar zmanjšuje možnost izgube podatkov in poenostavi izdelovanje varnostnih kopij), enostavnejše vzdrževanje (zaradi strežniške farme so nadgradnje strežnikov enostavne, lažje je nadzorovanje in upravljanje s centralno nameščenimi aplikacijami in uporabniki, ki dostopajo do njih).

Cilji diplomske naloge so načrt in izvedba postavitve ter prehod na uporabo farme terminalskih strežnikov s pomočjo Microsoftovega strežniškega operacijskega sistema Windows Server 2008 R2 in njegove funkcionalnosti Remote Desktop Services. Po uspešni postavitvi farme pa sledi še njena vpeljava v produkcijsko omrežje in selitev uporabnikov na nov sistem.

V prvem delu diplomske naloge sem podal kratek opis projekta in zahtev, opis primernih rešitev oziroma produktov, ki so na voljo na trgu, in razloge, ki so vplivali na izbiro Microsoftove rešitve. Temu pa sledi še podrobnejši opis izbranega produkta oziroma rešitve.

Osrednji del diplomske naloge zavzema podroben opis izvedbe projekta v podjetju, ki vključuje vse postopke, ki jih je bilo tekom postavitve strežniške farme in njene vpeljave potrebno izvesti. Opisane so vse nadgradnje in namestitve strojne in programske opreme ter sistemske in varnostne nastavitve, na koncu pa še postopki selitve uporabniških profilov in uporabnikov na novi sistem.

Zaključek diplomske naloge je posvečen ugotovitvam in opisom prednosti in slabosti, ki sta jih prinesli postavitev in implementacija novega sistema tako za uporabnike kot tudi za skrbnike sistema.

Ključni pojmi:

Windows Server 2008, Remote Desktop Services, oddaljeni dostop, administracija, aplikacije, uporabniki

Abstract

Remote Desktop Services or terminal services present a Microsoft solution for multi-user environment in Windows server which allows its users an access to remote data and applications located on terminal servers. With the help of Remote Desktop Services users have access to terminal servers from a network of a company or through the Internet. Only the screen picture is transferred to its user, that is why such work does not demand a very efficient computer. The use of Remote Desktop Services also bring some advantages such as reduction of costs (there is not need for a constant upgrading of personal computers, favourable licensing), bigger reliability and accessibility (in the network we place a farm of servers so in case of problems with one of them users have access to all services, programmes and data), better security (all data are stored in a very safe central location – there is less possibility of losing data and on the other hand the creation of back-up copies is simplified), simpler maintenance (due to server farm upgrades of servers are simpler, it is easier to control and manage centrally located applications and users who have access to them).

The purposes of this diploma thesis are: planning and implementation of the installation as well as the transition to the use of terminal servers' farm with the help of Microsoft server operating system Windows Server 2008 R2 and its Remote Desktop Services role. What follows after a successful installation of the farm is its introduction into a production network and the migration of the users to a new system.

The first part of the thesis introduces a short presentation of the project and its demands, the description of suitable solutions or products that are available in the market and the reasons that had an influence on choosing the Microsoft solution. What follows is a detailed presentation of a chosen product or solution.

The main part of the thesis deals with the precise description of the project in the company which involves all the procedures that had to be done in the process of installing the server farm and its implementation. There are mentioned all the upgrades and installations of hardware and software, system and security configuration as well as all the procedures of migration of the users and their profiles into a new system.

The final part of the thesis is dedicated to the findings, advantages and disadvantages the installation and implementation of the new system have brought to its users and administators.

Key words:

Windows Server 2008, Remote Desktop Services, remote access, administration, applications, users

1. Uvod

Terminalske storitve so tehnologija, ki omogoča preprost in učinkovit način centralizacije poslovnih aplikacij. Predstavljajo preprost in učinkovit način dostopa do večuporabniškega okolja, ki omogoča uporabnikom dostop do oddaljenih podatkov in aplikacij, nameščenih na terminalskih strežnikih. Tako programske aplikacije delujejo na strežnikih, uporabniki pa do njih dostopajo s svojih delovnih postaj ali lahkih odjemalcev. V smeri od strežnika do uporabnika se prenaša samo slika, v obratni smeri pa samo uporabnikovi ukazi in njegova interakcija z aplikacijami, zato za takšno delo ne potrebujemo zmogljivega računalnika.

V podjetju, kjer smo izvajali projekt, so bile terminalske storitve že v uporabi. Postavljena je bila farma, sestavljena iz štirih tako imenovanih "blade" strežniških rezin (ang. Blade Server) v IBM Blade Centru z operacijskim sistemom Windows Server 2003, na katerih je bil nameščen produkt podjetja Citrix Systems, Citrix Presentation Server. To rešitev je vsakodnevno uporabljalo približno 100 uporabnikov. Ker pa je bila obstoječa farma postavljena že leta 2005, je bila potrebna prenove in posodobitve predvsem zaradi starega operacijskega sistema, premalo zmogljive strojne opreme in posledično počasnega delovanja in občasne nestabilnosti. To so bili tudi bistveni razlogi, na podlagi katerih smo se odločili za ta projekt.

Hkrati s prehodom na nove oziroma posodobljene terminalske storitve smo se odločili izvesti tudi prehod na novo verzijo operacijskih sistemov na terminalskih strežnikih. Zaradi prednosti, ki jih to prinaša, pa smo hkrati načrtovali tudi prehod na 64-bitno tehnologijo, saj je večina ostalih strežnikov v omrežju podjetja že tekla na Windows Server 2008 x64.

Poleg teh osnovnih pogojev pa smo pred začetkom projekta postavili še nekaj zahtevanih funkcionalnosti, ki jih mora izbrani produkt obvezno ponujati. Te funkcionalnosti so sledeče:

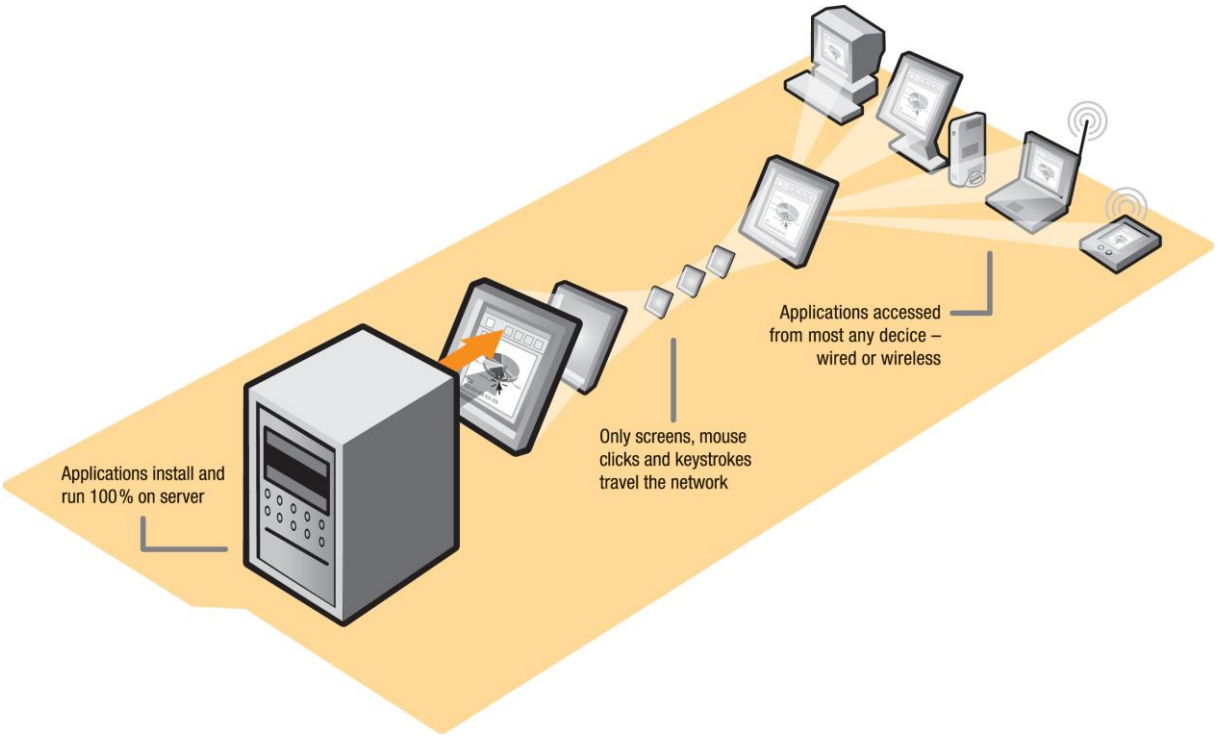
- **Združljivost aplikacij:** Vse obstoječe aplikacije morajo popolnoma funkcionirati tudi na novem sistemu.
- **Dostop do objavljenih namizij:** Nov sistem mora omogočati uporabnikom, da z oddaljenih lokacij dostopajo do objavljenih namizij na terminalskih strežnikih.
- **Dostop do posameznih objavljenih aplikacij preko spletnega vmesnika:** Nov sistem mora poleg dostopa do celotnih objavljenih namizij omogočati tudi dostop do posameznih objavljenih aplikacij preko spletnega vmesnika. Obvezno mora obstajati tudi možnost omejevanja dostopa do posameznih aplikacij za posamezne uporabnike oziroma skupine uporabnikov.
- **Možnost izgradnje strežniške farme:** Produkt mora omogočati možnost izgradnje farme, v katero je mogoče v prihodnosti dodajati dodatne strežnike in izklapljati oziroma odstranjevati obstoječe (na primer v primeru okvar ali nadgradenj). Prav tako mora farma omogočati vsaj enostavno razporeditev obremenitve (load balancing).
- **Centralizirano upravljanje in nadzor:** Produkt mora administratorjem omogočati nadzor in upravljanje sistema z enega mesta.

- **Čim boljša integracija z ostalimi Microsoftovimi produkti:** Večina ostalih strežnikov, servisov in storitev v omrežju podjetja teče na Microsoftovih tehnologijah in rešitvah, zato je pomembno, da se tudi terminalske storitve čim bolje integrirajo v celotno omrežje.
- **Ugodna cena:** Produkt in njegovo licenciranje naj bo čim bolj cenovno ugodno. Tovrstni produkti so namreč kljub ogromnim prihrankom, ki jih njihova uporaba prinese podjetju, še vedno precej dragi. Predvsem je lahko drago njihovo licenciranje, saj je le to po navadi izvedeno na nivoju uporabnika in ne na nivoju strežnikov. Prav zato se lahko ravno zaradi tega, ob velikem številu uporabnikov, stroški investicije precej povečajo.

2. Pregled tehnologij

2.1 Oddaljeni dostop

V računalništvu se izraz oddaljeni dostop (remote access) oziroma oddaljeno namizje (remote desktop) nanaša na programsko opremo ali funkcijo opreracijskega sistema, ki omogoča aplikacijam, da se izvajajo na odddaljenem strežniku oziroma gostitelju, medtem ko se rezultat njihove uporabe oziroma uporabnikova interakcija z njimi prikaže na lokalni ravni - pri odjemalcu.



Slika 1: Oddaljeni dostop

Oddaljeni dostop deluje tako, da odjemalčev računalnik prikazuje kopijo zaslonske slike gostiteljevega računalnika. Kopija je posodobljena na določen časovni interval oziroma ko pride do spremebe na gostiteljevem zaslonu, ki jo opazi programska oprema za oddaljeni dostop. Programska oprema na odjemalčevem računalniku prenaša aktivnost iz odjemalčeve tipkovnice in miške na gostiteljev računalnik, kjer programska oprema za oddaljeni dostop izvede aktivnosti, ki jih je zahteval odjemalec. Gostiteljev računalnik pa se nato obnaša, kot da bi bile aktivnosti izvedene lokalno. Odvisno od implementacije se lahko na gostiteljevem zaslonu prikazujejo aktivnosti odjemalca, lahko pa je zaslon onemogočen in zaklenjen, tako da so odjemalčeve aktivnosti skrite.

Oddaljena namizja in aplikacije imajo različne lastnosti. Nekatere omogočajo tudi vklop v obstoječo uporabnikovo sejo in oddaljeni nadzor oziroma pomoč uporabniku. Ta način imenujemo tudi oddaljena administracija (remote administration) in "daljinsko" je pred očmi uporabnika. Prevzem namizja na daljavo je oblika daljinskega upravljanja. Tipični komercialni programi, uporabljeni za oddaljeno upravljanje z Windows računalniki, vključujejo Radmin, Netop Remote Control, NetSupport Manager, pcAnywhere, I'm InTouch in Laplink. Za računalnike Macintosh obstaja Apple Remote Desktop in Timbuktu (Timbuktu deluje tudi na Windows sistemih). Na voljo so tudi odprtokodne rešitve, na primer VNC (Virtual Network Computing) in FreeNX.

Drugi način je oddaljeni dostop do drugega računalnika preko omrežja in uporaba na njem nameščenih aplikacij. Ta metoda je zelo razširjena pri velikih proizvajalcih računalnikov, ki jo uporabljajo kot metodo za pomoč svojim strankam, in tudi v mnogih drugih velikih podjetjih. Microsoftovi operacijski sistemi že vključujejo Redmote Desktop Services, Apple vključuje deljenje zaslona v operacijskem sistemu Mac OS X in za doplačilo ponuja Apple Remote Desktop. Poleg tega pa obstaja še ogromno profesionalnih orodij za oddaljeni dostop drugih proizvajalcev, tako odprtokodnih kot brezplačnih, takih, ki delujejo na operacijskih Windows, Mac, Unix/Linux/BSD, ali pa celo na vseh naenkrat. Naj omenimo samo najbolj razširjene: Citrix Presentation Server, podjetja Citrix Systems, Ericom Software, TQuest Software vWorkspace, PowerTerm WebConnect in še mnogi drugi.

2.2 Opis možnih rešitev

2.2.1 Citrix Delivery Center

Citrix je vodilna družba na področju programske opreme in storitev za navidezna delovna okolja, ki omogočajo dostop do aplikacij, informacij, procesov in ljudi z uporabo različnih računalniških naprav prek kakršnegakoli omrežja, kjerkoli in kadarkoli. Citrix poskrbi, da današnje digitalne pisarne postanejo popolnoma navidezne. Namesto da bi morali vi v pisarno, pisarna sledi vam.

V sodelovanju z vodilnimi partnerji na področju brezžičnih rešitev, integracije in svetovanja Citrix ponuja rešitve za poslovanje, ki odgovarjajo na poslovne izzive, med katerimi so tudi uvajanje aplikacij, povezovanje oddaljenih pisarn, mobilnost delovne sile in poslovanje brez prekinitev.

Citrix Delivery Center je sistem za zagotavljanje aplikacij, ki omogoča virtualizacijo aplikacij in namizij, centralizirano upravljanje, povečanje zmogljivosti in varno zagotavljanje aplikacij uporabnikom, kjerkoli že so. Citrix Delivery Center optimizira zagotavljanje aplikacij iz podatkovnega središča za namizja ter izboljša način, kako podjetje svojim strankam, partnerjem in zaposlenim zagotavlja za poslovanje ključno programsko opremo, operacijske sisteme in orodja za večjo storilnost. Gre za rešitev, ki statična podatkovna središča spreminja v dinamična središča za zagotavljanje aplikacij.

Družino izdelkov Citrix Delivery Center sestavljajo izdelki za virtualizacijo in omrežja, ki omogočajo celovit sistem za virtualizacijo strežnikov, aplikacij in namizij, centraliziranje le-teh v podatkovnem središču in zagotavljanje uporabnikom prek vsakega omrežja kot storitev na zahtevo.

- Citrix XenDesktop je sistem za virtualizacijo namizij, ki centralizira in zagotavlja namizja kot storitev za uporabnike, kjerkoli že so, poveča varnost in zniža skupne stroške lastništva namiznih sistemov.

- Citrix XenApp je sistem za zagotavljanje aplikacij za Windows, ki virtualizira aplikacije, jih upravlja v podatkovnem središču in kot storitev na zahtevo zagotavlja uporabnikom kjerkoli že so.

- Citrix XenServer je odprta, po meri velikih poslovnih okolij in s podporo za računalništvo v oblakih zasnovana platforma za virtualizacijo z naprednimi zmožnostmi upravljanja virtualizacije in avtomatizacije, ki spremeni podatkovna središča v dinamična središča za zagotavljanje.

- Citrix Netscaler je krmilnik za zagotavljanje spletnih aplikacij, ki izboljša zmogljivosti, zniža stroške in poveča varnost spletnih aplikacij.

- Citrix Access Gateway je navidezno zasebno omrežje (VPN), ki zagotavlja varen dostop do aplikacij, ki uporabnikom prinaša preprosto možnost dostopa vedno in povsod, skrbnikom pa najboljše možnosti nadzora na ravni aplikacij.

- Citrix Branch Repeater je rešitev za optimiziranje podružnic, namenjena pospeševanju in izboljšanju zmogljivosti aplikacij za uporabnike, ki svoje delo opravljajo na oddaljenih lokacijah.

- Citrix Receiver je lahek programski odjemalec, ki uporabnikom omogoča, da izberejo svoje poslovne aplikacije in namizja ter jih iz središča Citrix Delivery Center na zahtevo prejmejo na katero koli napravo.

Slika 2: Citrix Delivery Center

Za naš projekt sta najpomembnejša dva gradnika Citrix Delivery Centra, in sicer:

Citrix XenApp™

Citrix XenApp (prej se je izdelek imenoval Citrix Presentation Server) je nesporno standardna rešitev za zagotavljanje aplikacij za Windows/Linux z najnižjimi stroški, za vse uporabnike, z uporabo vseh naprav in pri dostopu prek vsakega omrežja.

Z uporabo varne aplikacijske arhitekture organizacije pridobijo:

- centralizirane aplikacije in podatke v varnih podatkovnih središčih,
- nižje stroške upravljanja in podpore,
- povečano varnost podatkov,
- povečano uporabniško zadovoljstvo in produktivnost,
- hitro in enostavno namestitev popravkov, nadgradenj, novih aplikacij.

Citrix XenDesktop™

Zagotavljanje namizij z Windows iz gruče terminalskih strežnikov. Namizja z Windows je zdaj mogoče zagotavljati varneje, zanesljiveje in z nižjimi stroški, neposredno iz podatkovnega središča. To omogoča Citrix XenDesktop.

Tveganje, da bi prišlo do izgube poslovnih podatkov, je zdaj manjše, upravljanje porazdeljenih PC-jev je preprostejše in bolj prilagodljivo, skupni stroški lastništva pa so nižji tudi do 40 odstotkov.

Globalizacija, prilagodljivi načini dela, poslovanje brez prekinitev, združitve in prevzemi podjetij pomenijo, da zaposleni zdaj svoje delo opravljajo na novih lokacijah, to pa zahteva nove načine varnega zagotavljanja namizij in to takoj.

Virtualizacija namizij pomeni ločitev fizične lokacije, kjer so namizni PC-ji, od mesta, kjer uporabniki dostopajo do PC-jev. Z uporabo rešitve Citrix XenDesktop sta gostovanje in upravljanje namizij centralizirana v podatkovnem središču, zagotavljanje namizij končnim uporabnikom pa je centralizirano. To je najboljši in najučinkovitejši način zagotavljanja namizij z Windows za uporabnike v pisarnah, podružničnih pisarnah in uporabnike pri zunanjih izvajalcih, saj omogoča poslovne pobude, kot so širitve podružnic, oddajanje del zunanjim izvajalcem, doseganje skladnosti z veljavnimi zakoni in poslovanje brez prekinitev.

Glavne prednosti rešitve:

- Nižji stroški
- Centralizirana administracija
- Kvalitetno in enostavno vzdrževanje
- Izboljšana varnost ...

2.2.2 Microsoft Remote Desktop Services 2008

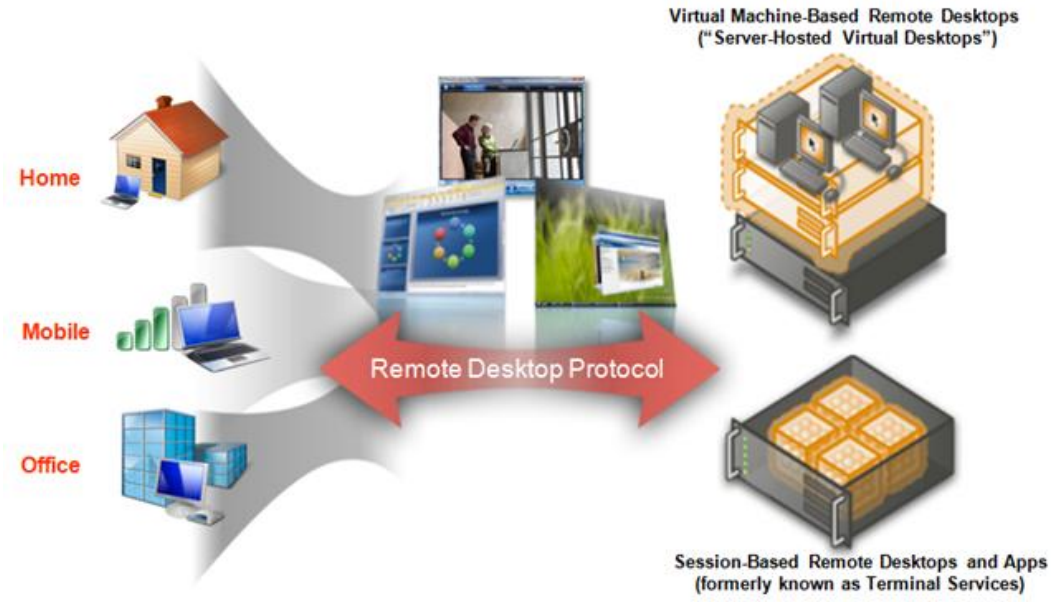
Z Remote Desktop Services (RDS), ki predstavlja eno izmed glavnih virtualizacijskih tehnologij na voljo v Windows Server 2008 R2, Microsoft napreduje v svoji viziji zagotavljanja najboljše virtualizacijske platforme za pospeševanje in razširjanje namizij in aplikacij iz podatkovnih centrov za vse vrste odjemalcev. Poleg tradicionalne virtualizacije sej, poznane že iz prejšnjih različic, imenovanih Terminal Services, Remote Desktop Services razširja svojo vlogo in tako nudi tudi razširljivo platformo za tako imenovano Virtual Desktop Infrastructure (VDI).

Remote Desktop Services v Windows Server 2008 R2 ponuja tehnologije, ki omogočajo uporabnikom dostop do Windows programov, ki so nameščenih na Remote Desktop Session Host (RD Session Host) strežnikih, ali dostop do celotnega Windows namizja. S pomočjo Remote Desktop Services lahko uporabniki dostopajo do RD Session Host strežnikov iz omrežja podjetja ali pa kar preko interneta.

Remote Desktop Services omogoča administratorjem učinkovito postavitev in vzdrževanje programske opreme v okolju podjetja. Programe je mogoče enostavno nameščati in vzdrževati s centralne lokacije. Ker so programi nameščeni samo na strežniku, a ne na računalnikih uporabnikov, jih je veliko enostavneje nadgrajevati in vzdrževati.

Ko uporabnik dostopa do programa na RD Session Host strežniku, se vse izvajanje le tega dogaja na strežniku. Samo ukazi tipkovnice, miške in prikaz informacij se prenašajo preko

omrežja na uporabnikov računalnik. Vsak uporabnik vidi samo svojo individualno sejo. Sejo, ki je povsem neodvisna od sej ostalih uporabnikov, povsem transparento upravlja strežnikov operacijski sistem.



Slika 3: Delovanje Remote Desktop Services

Remote Desktop Services je ena izmed strežniških vlog (server role), ki jih lahko namestimo na strežnik z operacijskim sistemom Windows Server in je sestavljena iz več komponent oziroma storitvenih vlog (role services). V operacijskem sistemu Windows 2008 R2 je Remote Desktop Services sestavljen iz sledečih storitvenih vlog:

- RD Session Host je gostitelj seje oddaljenega namizja in omogoča strežniku, da gosti Windows programe oziroma celotna Windows namizja. Uporabniki se lahko povežejo na RD Session Host strežnik in poganjajo programe, shranjujejo datoteke ali pa uporabljajo omrežne vire na strežniku.

- RD Web Access je storitvena vloga, ki omogoča uporabnikom, da dostopajo do RemoteApp programov in do orodja Remote Desktop Connection preko spletnega vmesnika.

- RDS Licensing je storitvena vloga, ki upravlja z Remote Desktop Services client access licenses (RDS CALs) licencami, ki so potrebne za vsakega odjemalca oziroma uporabnika, ki se povezuje na strežnik. S pomočjo RD Licensing-a nameščamo, dodeljujemo in nadziramo razpoložljivost uporabniških licenc na licenčnem strežniku.

- RD Gateway služi kot omrežni prehod in omogoča pooblaščenim oddaljenim uporabnikom povezovanje na vire znotraj omrežja podjetja, s kateregakoli odjemalca, povezanega na internet, ki lahko poganja Remote Desktop Connection odjemalca.

- RD Connection Broker je storitvena vloga, ki upravlja s povezavami in sejami uporabnikov in na ta način omogoča razporeditev obremenitve na nivoju uporabniških

sej in ponovne povezave uporabnikov v svoje obstoječe seje, med strežniki znotraj strežniške farme, ki podpira razporeditev obremenitve.

Uporaba Remote Desktop Services oziroma namestitev programa na RD Session Host strežnik namesto na vsakega posameznega odjemalca ima veliko koristi. Med njimi so tudi sledeče:

- Z uporabo Remote Desktop Services lahko hitro omogočite dostop do programov uporabnikom v celotnem omrežju podjetja. Še posebej je uporaben če imate v podjetju programe, ki potrebujejo pogoste posodobitve, so redko uporabljeni ali pa je njihovo vzdrževanje zahtevno.
- Uporaba Remote Desktop Services lahko bistveno zmanjša pasovno širino omrežja, ki je potrebna za dostop do oddaljenih aplikacij.
- Remote Desktop Services pomaga pri produktivnosti uporabnikov. Uporabniki lahko dostopajo do programov, ki so nameščeni na terminalskih strežnikih z naprav, kot so domači računalniki, kioski, lahki odjemalci, in tudi iz drugih operacijskih sistemov.
- Remote Desktop Services zagotavlja boljše delovanje programov za uporabnike na oddaljenih lokacijah, ki potrebujejo dostop do centralno shranjenih podatkov. Podatkovno intenzivni programi po navadi nimajo protokolov odjemalec/strežnik, optimiziranih za nizke hitrosti povezave.
- Programi te vrste zato pogosto delujejo bolje preko Remote Desktop Services, kot pa preko navadnih širokopasovnih povezav.

2.2.3 Ostale rešitve

Na trgu je še precej podobnih rešitev drugih proizvajalcev. Naj omenim samo nekatere: Na Windows platformi poleg Citrixa in Microsofta, ki zavzemata večino trga, prednjačijo še: Ericom Software, TQuest Software vWorkspace in PowerTerm WebConnect. Produkt Win4Lin Virtual Desktop Server podjetja Virtual Bridges ponuja podobne funkcionalnosti na Linux platformi, medtem ko Sun-ov produkt za virtualizacijo aplikacij, the Sun Secure Global Desktop, ponuja celovito rešitev tako za Windows kot tudi Unix aplikacije na vseh večjih platformah. Vendar pa nobena od teh rešitev v našem primeru ni prišla v ožji izbor, bodisi ker ne izpolnjuje vseh zahtevanih funkcionalnosti, bodisi cenovno ni konkurenčna.

2.3 Izbor najprimernejše rešitve

Kot je razvidno že iz prejšnjih poglavij, sta v ožji izbor prišla dva produkta. Tako Citrix Delivery Center kot Microsoft Remote Desktop Services sta izpolnjevala vse zahtevane funkcionalnosti, ki smo jih zastavili pred začetkom projekta. Citrix-ov produkt sicer ponuja še

veliko dodatnih funkcionalnosti, ki pa jih v našem primeru nismo nujno potrebovali, tako da je bil tudi Microsoftov produkt, ki je izpolnjeval le obvezne zahteve, enakovredna konkurenca.

Glede na to, da sta bila produkta po zahtevanih funkcionalnostih izenačena, je bila naslednja postavka za primerjanje cena. Tukaj se je pokazala bistvena prednost Remote Desktop Services. Kot ena izmed Roles v Windows Server 2008 R2 je Remote Desktop Services integriran v sam operacijski sistem. Licenciranje je tako izvedeno na nivoju operacijskega sistema s pomočjo tako imenovanih Remote Desktop Client Access Licenses (RDS CALs). Ob vzpostavljanju povezave RDP na enega izmed terminalskih strežnikov se terminalski strežnik najprej poveže z licenčnim strežnikom, ki uporabniku, ki se povezuje, dodeli njegovo licenco (RDS CAL). Za vsakega uporabnika, ki se želi povezati na terminalske strežnike, moramo zato imeti na voljo licenco. Torej moramo kupiti toliko licenc, kot imamo RDS uporabnikov. Po drugi strani pa je Citrix Delivery Center programska oprema, ki jo je potrebno dodatno namestiti na strežnike z Windows Server operacijskim sistemom, kar seveda vključuje nakup še dodatnih Citrix uporabniških licenc, prav tako za vsakega uporabnika, ki se poveže na strežnik in dostopa do Citrix storitev. Ker bi to pomenilo najmanj dvojne stroške, smo se posledično odločili za uporabo Microsoftove rešitve Remote Desktop Services.

Zahtevane funkcionalnosti	**Obstoječe stanje**	**Citrix Delivery Center**	**Microsoft Remote Desktop Services**
Združljivost aplikacij	DA	DA	DA
Dostop do objavljenih namizij	DA	DA	DA
Dostop do posameznih objavljenih aplikacij preko spletnega vmesnika	DA	DA	DA
Možnost izgradnje strežniške farme	DA	DA	DA
Centralizirano upravljanje in nadzor	DA	DA	DA
Čim boljša integracija z ostalimi Microsoftovimi produkti	SLABA	SLABA	ODLIČNA
Ugodna cena	NE, potrebno podaljšanje vzdrževalne pogodbe	NE, potreben je nakup dodatnih Citrix licenc	DA, potrebujemo samo licence za operacijski sistem

Tabela 1: Primerjava obstoječega stanja in novih rešitev

Naši izbiri je še dodatno botrovalo to, da je Microsoftova rešitev, kot že rečeno, integrirana v sam strežniški operacijski sistem, kar poenostavi tako namestitev in nastavitve kot tudi upravljanje, nadgrajevanje in administracijo. Podjetje ima z Microsoftom podpisano tudi tako imenovano License Agreement pogodbo, ki sam nakup Microsoftove programske opreme in licenc samo še poenostavi in na dolgi rok tudi poceni. Poleg tega pa se, ker gre za Microsoftovo tehnologijo, tudi bolje integrira v celotno omrežje in informacijsko infrastrukturo podjetja, ki je zgrajena iz večinoma Microsoftovih rešitev.

2.4 Izbrana rešitev

2.4.1 Microsoft Windows Server 2008

Windows Server 2008 je zadnji produkt iz Microsoftove serije strežniških operacijskih sistemov. Izdan je bil februarja 2008 in je naslednik sistema Windows Server 2003, ki je bil izdan pet let prej. Prav tako kot zadnji Microsoftov namizni operacijski sistem Windows Vista je tudi Server 2008 zgrajen na Windows NT 6.0 SP1 kernelu.

Ker je, kot že rečeno, zgrajen na isti osnovi kot Windows Vista, si z njo deli precejšnji del arhitekture in funkcionalnosti. Glede na to, da je osnovna koda skupna, je enaka ali zelo podobna tudi večina tehničnih, varnostnih, upravljalnih in administrativnih novosti. Kot na primer na novo napisan omrežni sklad (native IPv6, native wireless, izboljšana hitrost in varnost), izboljšana namestitev, recovery, diagnostika, nadzorni center ... ; z novimi varnostnimi funkcionalnosti (BitLocker, ASLR), izboljšan je Windows Firewall požarni zid, z varno privzeto konfiguracijo, sledi podpora .NET 3.0 tehnologijam in izboljšave samega jedra, ravnanja s pomnilnikom in datotečnim sistemom.

Windows Server 2008 vključuje tudi možnost tako imenovane Server Core namestitve. Server Core je precej okleščena verzija namestitve strežnika, ki ne vsebuje Windows Explorer lupine. Vsa konfiguracija in vzdrževanje takega strežnika se izvaja s pomočjo vmesnika z ukazno vrstico ali s povezavo z drugega računalnika s pomočjo Microsoft Managment Console. Na voljo je edino Beležnica in pa nekaj nastavitev iz Nadzorne plošče. Server Core ne vključuje .NET frameworka, Internet Explorerja, Windows Power Shella in mnogih drugih za Core verzijo nepomembnih funkcionalnosti. Server Core strežnik je lahko konfiguriran za nekaj osnovnih vlog: Domenski strežnik, DNS strežnik, DHCP strežnik, datotečni strežnik, tiskalniški strežnik, Windows Media strežnik, IIS7 spletni strežnik in Hyper-V virtualni strežnik. Prav tako pa se ga lahko uporabi za izdelavo strežniške gruče z visoko dosegljivostjo, s pomočjo Failover Clusteringa ali Network Load Balancinga. Glavna motivacija za razvoj Core verzije Windows Serverja 2008 je bilo zmanjšanje možnosti napadov na operacijski sistem, saj bi se lahko z uporabo Server Core verzije izognili 70 % varnostnim pomanjkljivostim v Microsoftovih sistemih v zadnjih 5 letih.

Active Directory vloga, ki je v Windows Server 2003 omogočala centralni nadzor in upravljanje s povezanimi računalniki, nastavljanje politik za skupine in uporabnike ter

nameščanje aplikacij na skupine računalnikov, je v Windows Server 2008 razširjena s tako imenovano Identity, Certificate and Rights Managment storitvijo in preimenovana v Active Directory Domain Services. Dodano pa je bilo še nekaj dodatnih storitev kot na primer: Active Directory Federation Services, Active Directory Lightweight Directory Services, (prej poznano kot Active Directory Application Mode), Active Directory Certificate Services in Active Directory Rights Management Services. Identity and Certificate Services omogoča administratorjem upravljanje z uporabniškimi računi in digitalnimi potrdili, ki omogočajo dostop do določenih storitev in sistemov. Federation Managment Services omogoča podjetjem deljenje uporabniških imen in gesel svojim zaupanja vrednim partnerjem in kupcem, kar jim omogoča tesnejše sodelovanje.

Veliko nadgradnjo so v Windows Server 2008 doživele storitve Terminal Services. Le-te zdaj podpirajo Remote Desktop protokol verzije 6.0. Najbolj opazno izboljšanje je zmožnost deljenja posamezne aplikacije preko povezave z oddaljenim namizjem, namesto deljenja celotnega namizja kot v prejšnjih verzijah. Ta funkcionalnost se imenuje Terminal Services RemoteApp. Druge novosti vključujejo Terminal Services Gateway in Terminal Services Web Access. S Terminal Services Gateway se lahko avtorizirani računalniki varno povežejo s terminalskim strežnikom ali oddaljenim namizjem iz interneta, z uporabo RDC-ja s HTTPS protokolom brez predhodne vzpostavitve VPN seje. Tako ni potrebno odpiranje nobenih dodatnih vrat na požarnem zidu. Terminal Services Web Access omogoča administratorjem, da omogočijo uporabnikom dostop do Terminal Services sej preko spletnega vmesnika. Uporaba RD Gateway in RD RemoteApp poteka preko HTTP(S) protokola in uporaba oddaljenih aplikacij je za uporabnika povsem transparentna, kot da bi jih poganjal lokalno na svojem računalniku. Več aplikacij teče v isti seji, tako da ni potrebe po dodatnih licencah za posameznega uporabnika. Terminal Services Easy Print zagotavlja redirekcijo odjemalčevih tiskalnikov in dosegljivost vseh tiskalniških vmesnikov ter lastnosti za uporabo v oddaljenih sejah. Terminal Services seje se kreirajo paralaleno, namesto serijskega delovanja – nov model sej lahko začne vsaj štiri seje paralelno oziroma še več, če ima strežnik več ko štiri procesorje.

Windows Server 2008 je prvi operacijski sistem, ki vsebuje tako imenovan Windows PowerShell, Microsoftovo novo razširjeno lupino z ukazno vrstico in skriptno tehnologijo. PowerShell je zasnovan na konceptu objektno usmerjenega programiranja in verziji 2.0 Microsoftovega .NET framework-a ter vključuje več kot 120 orodij za sistemsko administracijo, consistentno sintakso in vgrajene možnosti za delo z registrom, certifikati ali Windows Managment instrumentacijo. PowerShell skriptni jezik je bil razvit posebej za IT administracijo in se lahko uporabi namesto cmd.exe in Windows Script Host-a.

Še ena lastnost, ki je skupna z Windows Visto, je tako imenovani Self-healing NTFS. V prejšnjih verzijah je operacijski sistem ob ugotovitvi okvar v datotečnem sistemu NTFS zvezka označil le-tega kot »umazanega« (»dirty«). Za odpravo napak na zvezku ga je bilo treba odklopiti. Pri uporabi self-healing NTFS v ozadju teče nit, ki izvaja lokalna popravila na okvarjenih podatkovnih strukturah, tako da so tisti trenutek nedosegljive samo datoteke oziroma mape, ki se popravljajo, in ni potrebe po izklapljanju celotnega zvezka oziroma izklopa strežnika. Operacijski sistem uporablja tudi tako imenovane S.M.A.R.T. tehnike za

zaznavanje, za lažje ugotavljanje okvar diskov. V Windows Server 2008 je vključen tudi Windows System Resource Manager (WSRM). WSRM omogoča upravljanje z viri, in je uporaben za nadzor in določanje količine virov za posamezne procese ali uporabnike na osnovi poslovnih prioritet.

Server Manager je novo upravljalsko orodje za Windows Server 2008. Je kombinacija orodij Manage your server in Security configuration wizard iz Windows Server 2003. Server Manager je izboljšava orodja Configure my server, ki se privzeto zažene na Windows Server 2003 strežnikih. Poleg tega, da služi kot začetna točka za konfiguriranje novih vlog strežnika, vključuje še vse ostale operacije, ki jih uporabnik potrebuje pri konfiguraciji strežnika.

Z najnovejšo posodobitvijo Windows Server 2008 R2 Microsoft razširja obstoječe tehnologije in dodaja nove funkcionalnosti, kar omogoča IT strokovnjakom povečati zanesljivost in fleksibilnost njihove strežniške infrastrukture. Nova virtualizacijska orodja, spletni viri, izboljšave za upravljanje in integracija z operacijskim sistemom Windows 7 pomagajo prihraniti čas, zmanjšati stroške in zagotoviti platformo za dinamično in učinkovito upravljanje podatkovnih centrov.

Najpomembnejše spremembe so vidne na naslednjih področjih:

- Izboljšava platforme za spletne aplikacije: Nadgrajen spletni strežnik Internet Information Services (IIS) 7.5, boljša podporo za .NET tehnologije na Core verziji.

- Virtualizacija strežnikov in namizij: Nova verzija Hyper-V vključuje izboljšave na več ključnih področijih za ustvarjanje virtualnih dinamičnih podatkovnih centrov, vključno z omogočanjem večje razpoložljivosti in zmogljivosti, boljšega upravljanja, poenostavljene metode za uvajanje in nove funkcije, predvsem tako imenovan live migration. Remote Desktop Services, prej imenovani Terminal Services, ponuja uporabnikom in administratorjem funkcije in fleksibilnost, potrebno za izgradnjo najbolj robustnih scenarijev za dostop do in razširjanje programske opreme. Poleg tega pa prinaša še novo funkcionalnost Virtual Desktop Infrastructure (VDI), ki omogoča poganjanje in upravljanje Windows in ostalih namiznih okolij v virtualnih računalnikih na centraliziranem strežniku.

- Izboljšan nadzor porabe in racionalizacija upravljanja strežnikov: Kompatibilnost z najnovejšimi standardi, izboljšan nadzor porabe energije v podatkovnem centru, izboljšani mehanizmi oddaljene administracije, upravljanja preko ukazne vrstice in avtomatizacije upravljanja s pomočjo PowerShell 2.0.

- Še večja razširljivost in zanesljivost: Podpora za nove, sofisticirane CPU arhitekture, izboljšane zmogljivosti in razširljivosti za aplikacije in storitve, boljše rešitve za shranjevanje podatkov, izboljšana zaščita intranetnih virov.

- Izboljšanje uporabniške izkušnje skupaj z operacijskim sistemom Windows 7: poenostavljeno oddaljeno povezovanje s pomočjo funkcionalnosti DireckAccess, izboljšane zmogljivosti, varnost, integracija virtualiziranih namizij ...

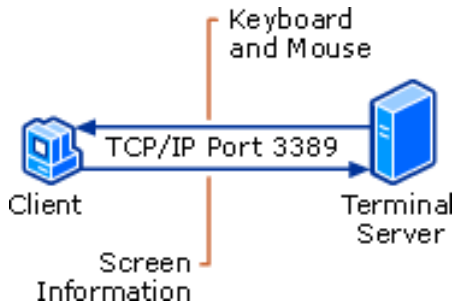
2.4.2 Microsoft Remote Desktop Services 2008

Kaj so Remote Desktop Services?
Remote Desktop Services je strežniška vloga v Windows Server 2008 R2, ki nudi tehnologije, ki omogočajo uporabnikom dostop do programov, ki so nameščeni na terminalskem strežniku (Remote Desktop Session Host), ali pa dostop do celotnega Windows namizja. Z uporabo Remote Desktop Services lahko uporabniki dostopajo do terminalskega strežnika iz omrežja podjetja ali pa iz interneta.

Kaj je terminalski strežnik?
Terminalski strežnik oziroma Remote Desktop Session Host je strežnik, ki gosti Windows aplikacije oziroma celotno Windows namizje za Remote Desktop Services odjemalce. Uporabniki se lahko povezujejo na terminalski strežnik in tako dostopajo do programov, shranjujejo datoteke in uporabljajo omrežne vire na tem strežniku. Uporabniki lahko dostopajo do terminalskega strežnika z uporabo Remote Desktop odjemalca, kjer dostopajo do celotnega namizja ali pa z uporabo RemoteApp programov, kjer s pomočjo lokalne bližnjice oziroma spletnega vmesnika poganjajo posamezen program, ki teče na terminalskem strežniku.

Remote Desktop Services omogočajo učinkovito razširjanje in vzdrževanje programske opreme v okolju podjetja. Enostavno lahko omogočamo uporabnikom dostop do aplikacij nameščenih na centralni lokaciji. Ker so aplikacije nameščene na terminalskem strežniku in ne na računalnikih uporabnikov, je nadgrajevanje in vzdrževanje bistveno lažje, hitrejše in zanesljivejše.

Ko uporabnik dostopa do aplikacije na terminalskem strežniku, se program zažene na strežniku. Preko omrežja se prenašajo samo informacije o aktivnosti tipkovnice in miške in dogajanju na zaslonu. Vsak uporabnik vidi le svojo individualno sejo. Sejo povsem transparentno upravlja operacijski sistem strežnika in je neodvisna od ostalih sej odjemalca.



Slika 4: RDP povezava

Prednosti uporabe Remote Desktop Services
Z namestitvijo aplikacij na RD Session Host strežnik, namesto na vse računalnike v omrežju, pridobimo veliko ugodnosti:

- Hitro lahko distribuiramo aplikacije na računalnike v podjetju. Remote Desktop Services so še posebej uporabne za programe, ki se pogosto nadgrajujejo, so malo v uporabi ali jih je težko upravljati.
- Uporaba Remote Desktop Services lahko precej zmanjša obremenitve omrežja, ki nastajajo ob dostopanju do oddaljenih aplikacij.
- Uporaba Remote Desktop Services poveča produktivnost uporabnikov, saj lahko dostopajo do aplikacij, nameščenih na terminalskem strežniku, s katerega koli računalnika, z raznih lahkih odjemalcev, od doma, preko interneta ...
- Remote Desktop Services ponujajo boljše performanse za uporabnike, ki dostopajo do centraliziranih skladišč podatkov. Aplikacije, ki uporabljajo velike količine podatkov, pogosto delujejo bolje z uporabo Remote Desktop Services povezave kot pa preko navadne WAN povezave.

Remote Desktop Services storitvene vloge
Remote Desktop Services je strežniška vloga (role), ki je sestavljena iz nekaj komponent oziroma storitvenih vlog. V Windows Server 2008 R2 je Remote Desktop Services sestavljene iz sledečih storitvenih vlog:

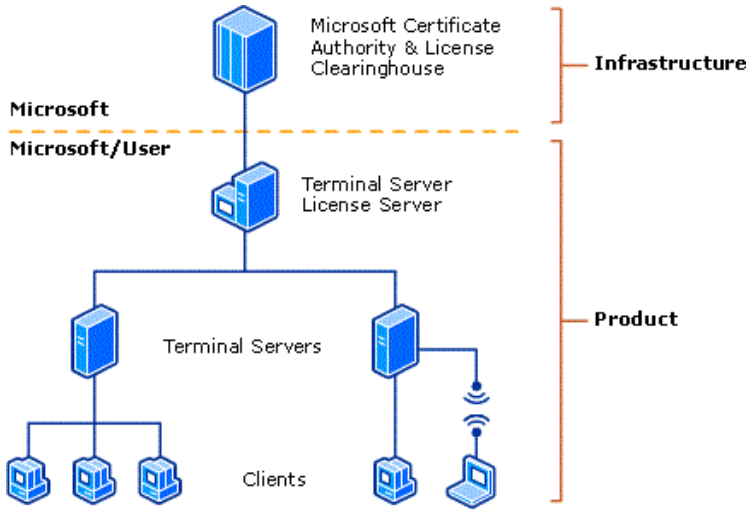
Remote Desktop Session Host
RD Session Host, prej znani kot Terminal Server, je storitvena vloga, ki omogoča strežniku, da gosti Windows programe oziroma celotna Windows namizja za Remote Desktop Services odjemalce. Uporabniki se lahko povežejo na RD Session Host strežnik in poganjajo programe, shranjujejo datoteke ali pa uporabljajo omrežne vire na strežniku. Uporabniki lahko dostopajo do RD Session Host strežnika s pomočjo Remote Desktop Connection odjemalca ali pa z uporabo RemoteApp programov. RemoteApp programi so programi, do katerih dostopamo s pomočjo Remote Desktop Services. Nameščeni so na RD Session Host strežniku, ob poganjanju pa se obnašajo, kot da bi jih poganjali uporabniki lokalno, na svojih računalnikih. Uporabniki jih lahko poganjajo vzporedno s svojimi lokalnimi programi. Če uporabnik poganja več RemoteApp programov z istega RD Session Host strežnika, si programi delijo isto Remote Desktop Services sejo. Ta funkcionalnost omogoča hitrejšo povezavo do vsakega dodatnega RemoteApp programa, ki je nameščen na istem strežniku. S pomočjo RD RemoteApp Managerja lahko izdelamo Installer pakete (.msi pakete) ali pa .rdp datoteke, ki jih nato distribuiramo na računalnike v omrežju, ki te programe potrebujejo. Če pa bi radi, da uporabniki do RemoteApp programov dostopajo preko spleta, jih preprosto objavimo na spletni strani s pomočjo RD Web Accessa.

Remote Desktop Web Access
RD Web Access omogoča, da RemoteApp programe in Remote Desktop Connection ponudite uporabnikom preko spleta. S pomočjo RD Web Accessa uporabniki lahko obiščejo spletno stran (na internetu ali intranetu) in tako dostopajo do spiska programov, ki so na voljo.

Ko uporabnik zažene program, se ustvari RDS seja na RD Session Host strežniku, ki gosti zagnano aplikacijo. Ob namestitvi RD Web Accessa določimo, kateri RD Session Host strežnik se bo uporabljal kot vir za RemoteApp programe, ki bodo dostopni preko spleta. V RD Web Access je vključen tudi tako imenovani Remote Desktop Web Connection. S tem orodjem lahko uporabnik izbere računalnik, na katerega bi se rad povezal, nato pa zažene polno Remote Desktop sejo na ta računalnik. Za uspešno povezavo mora uporabnik seveda imeti omogočen Remote Desktop dostop na ciljnem računalniku.

Remote Desktop Licensing

RD Licensing je strežnik za licenciranje, ki upravlja z RDS CALs (Remote Desktop Services Client Access Licenses), ki so potrebni za vsakega uporabnika ali napravo, ki se želi povezati na terminalske strežnike. Strežnik za licenciranje uporabljamo za namestitev, dodeljevanje in nadzor nad dostopnostjo RD licenc (RD CALs). Za uporabo Remote Desktop Services je potrebno imeti vsaj en strežnik za licenciranje. Za manjše projekte lahko namestite tako terminalski strežnik kot tudi strežnik za licenciranje na isti strežnik. Za velike projekte pa je priporočljivo, da se strežnik za licenciranje namesti posebej. Storitvena vloga RD Licensing mora biti pravilno nameščena in nastavljena, preden lahko terminalski strežnik začne sprejemati povezave s strani odjemalcev.



Slika 5: Potek licenciranja

Remote Desktop Gateway

RD Gateway je omrežni prehod, ki omogoča avtoriziranim oddaljenim uporabnikom dostop do virov znotraj omrežja podjetja s katerekoli naprave, ki ima povezavo z internetom in lahko poganja Remote Desktop Connection odjemalca. Omrežni viri so lahko terminalski strežniki, terminalski strežniki, ki poganjajo RemoteApp programe, ali pa računalniki, ki imajo omogočen Remote Desktop. RD Gateway vsebuje Remote Desktop protokol znotraj protokola RPC, znotraj protokola http, preko Secure Socket Layer (SSL) povezave. Na ta način RD Gateway pomaga pri izboljšanju varnosti, z vzpostavitvijo šifrirane povezave med oddaljenimi uporabniki na internetu in notranjimi viri v omrežju, na katerih tečejo aplikacije, do katerih uporabniki dostopajo.

Remote Desktop Connection Broker

RD Session Broker je storitvena vloga, ki skrbi in upravlja z uporabniškimi povezavami in sejami v strežniški farmi terminalskih strežnikov z razporeditvijo obremenitve (load-balancing). V svoji podatkovni bazi shranjuje podatke o stanju uporabniških sej, ki vključujejo ID sej, imena uporabnikov za posamezne seje in imena strežnikov, kjer seje potekajo. Ko se uporabnik, ki že ima obstoječo sejo, poveže na terminalski strežnik v strežniški farmi, RD Session Broker preusmeri uporabnika na terminalski strežnik, kjer že obstaja njegova seja. To prepreči, da bi se uporabniki v takem primeru povezovali na druge terminalske strežnike in tam zaganjali nove seje. Če je omogočena RD Session Broker funkcija za razporeditev obremenitve, RD Session Broker sledi tudi številom uporabniških sej na vsakem terminalskem strežniku v strežniški farmi in preusmeri uporabnike, ki še nimajo obstoječe seje, na strežnik z najmanj sejami. Ta funkcionalnost omogoča, da se seje enakomerno porazdelijo na strežnike v load-balanced farmi terminalskih strežnikov.

3. Izvedba projekta

3.1 Načrt prehoda

Pred samo izvedbo projekta smo sestavili načrt, kako naj bi izvedba projekta potekala. Projekt smo razdelili na več zaporednih faz oziroma korakov:

- Analiza obstoječega stanja in morebitne potrebne nadgradnje
- Priprava testnega okolja in testiranje
- Priprava selitve uporabniških profilov
- Postavitev novega tiskalniškega strežnika
- Nadgradnja odjemalcev
- Izvedba pilotskega projekta
- Postavitev produkcijskih strežnikov
- Prehod na novi sistem

3.2 Analiza obstoječega stanja strojne in programske opreme in nadgradnja

Kot je že bilo omenjeno v uvodu diplomske naloge, so bili v podjetju že v uporabi terminalski strežniki, na katerih je bil nameščen Citrix Presentation Server, a so bili potrebni prenove. Deloma je bila prenova potrebna zaradi zastarele programske opreme Citrix, deloma pa zaradi strojne opreme, ki je komaj še zmogla obvladovati vedno večje število uporabnikov terminalskih storitev.

Obstoječa farma terminalskih strežnikov je bila sestavljena iz štirih produkcijskih terminalskih strežnikov, ki so bili nameščeni na štirih tako imenovanih "blade" strežniških rezinah (ang. Blade Server) IBM Blade Centra. Ker se v podjetju uporablja večinoma IBM strežniška oprema, smo se na podlagi dobrih izkušenj iz preteklosti, tudi za namestitev Remote Desktop Services farme, odločili uporabiti enako strojno opremo. Tako smo za nove terminalske strežnike prav tako izbrali štiri nove strežniške rezine v istem Blade Centru. Vendar s to razliko, da smo nove rezine nadgradili. Vsaka izmed novih rezin tako vsebuje po dva Intel Xeon 3.4GHz procesorja in 8 GB pomnilnika.

Da bi čim bolje izkoristili izbrano strojno opremo, ki smo jo imeli na voljo (večje količine pomnilnika, večprocesorska arhitektura), in omogočili vse potrebne funkcionalnosti zadnje

verzije Remote Desktop Services, smo na vse strežnike namestili 64-bitni operacijski sistem Windows Server 2008, in sicer zadnjo različico z oznako R2.

3.3 Priprava testnega okolja in testiranje aplikacij

V tem koraku smo namestili in nastavili testno farmo terminalskih strežnikov. Testna farma je vsebovala vse komponente in funkcionalnosti, potrebne za delovanje, a je bila za razliko od produkcijske sestavljena samo iz dveh terminalskih strežnikov, kar pa je bilo dovolj za uspešno testiranje vseh željenih funkcionalnosti. Po namestitvi in konfiguraciji smo na oba terminalska strežnika namestili še vse potrebne aplikacije, ki jih bodo uporabniki potrebovali pri svojem delu. Po namestitvi smo vse aplikacije preizkusili tako na administrativnem kot tudi na uporabniškem nivoju. Tu so se že pojavili prvi zapleti. Z večino aplikacij sicer ni bilo problemov, nekatere (Time&Space, Apis IQ-FMEA PRO, 7zip …) pa na 64-bitnem operacijskem sistemu niso delovale. To nam je uspelo rešiti s posodobitvijo aplikacij na najnovejše verzije ali pa s ponovno namestitvijo 64-bitnih verzij aplikacij. S tem korakom smo potrdili, da je Remote Desktop Services primerna rešitev tudi na nivoju uporabniških aplikacij, saj so po zaključku testov vse nameščene aplikacije pravilno delovale.

3.4 Priprava na selitev uporabniških profilov

Uporabniški profili v operacijskih sistemih Windows XP in Windows Server 2003 zaradi svoje zgradbe niso združljivi z uporabniškimi profili v novejših verzijah operacijskih sistemov, kot so Windows Vista, Windows 7 in Windows Server 2008. Ko se uporabnik prijavi na računalnik, na katerem teče novejši operacijski sistem, se kreira nova mapa z imenom `uporabnisko_ime.V2`, ki vsebuje novo verzijo (Version 2) uporabniškega profila.

Vendar pa je vseeno mogoče uporabljati uporabniške profile, narejene v starejših operacijskih sistemih, tudi v Windows Vista, Windows 7 in Windows Server 2008. Obstajata dve metodi za selitev podatkov iz uporabniških profilov na novo V2 verzijo, ki se uporablja v novejših Microsoftovih operacijskih sistemih.

3.4.1 Uporaba orodja User State Migration Tool

Uporaba orodja User State Migration Tool je priporočljiva v primeru, ko v svojem Active Directory okolju ne uporabljamo tako imenovanih roaming profilov oziroma funkcionalnosti Folder Redirection. Roaming uporabniški profil je Microsoftov koncept, ki ga najdemo v družini Microsoft Windows NT operacijskih sistemov. Uporabniku z računalnikom, ki je pridružen Windows Server domeni omogoča, da se prijavi na kateremkoli računalniku v istem omrežju in dostopa do svojih dokumentov in uporablja enake nastavitve aplikacij in namizja

kot na svojem računalniku. Prav tako je uporaba tega orodja priporočljiva, ko želimo preseliti več podatkov, ker orodje ne preseli samo uporabnikovih datotek, ampak tudi uporabnikove nastavitve registra, nastavitve aplikacij ter ostale sistemske nastavitve in nastavitve namizja, ki ne bodo avtomatsko preseljene ob uporabi funkcionalnosti Folder Redirection. Slaba lastnost orodja User State Migration Tool pa je, da lahko z njim preselimo samo uporabniške profile, ki so shranjeni na lokalnem računalniku. V primeru, da imamo profile shranjene centralno na strežniku, uporaba tega orodja ni mogoča. Orodje pa prav tako ne deluje na Windows Server 2008.

3.4.2 Uporaba funkcionalnosti Folder Redirection

V primeru, da imamo uporabniške profile shranjene centralno na strežniku in uporabljamo tako imenovane roaming profile, moramo za selitev profilov uporabiti funkcionalnost Folder Redirection. Slaba stran te metode pa je, da preseli samo uporabnikove podatke, ne pa tudi njegovih sistemskih nastavitev in nastavitev namizja zaradi razlik v operacijskem sistemu.

Funkcionalnost Folder Redirection za selitev roaming uporabniških profilov iz verzije 1 v verzijo 2 nastavimo po sledečem postopku:

1. Najprej se prepričamo, da je v aktivnem imeniku (AD) v lastnostih uporabniškega računa vpisana pot do uporabnikovega roaming profila. To storimo tako, da v aktivnem imeniku z desnim miškinim gumbom kliknemo na uporabniški račun, izberemo Properties in v oknu, ki se nam odpre, izberemo zavihek Profile, kjer preverimo, če je pot vpisana.

2. Konfiguriramo funkcionalnost Folder redirection na Windows Xp/Windows Server 2003 računalniku, ki je del Active Directory (AD) okolja, s pomočjo skupinskih politik (GPO), z orodjem Group Policy Managment Console (GPMC), s katerim kreiramo oziroma uredimo določene Group policy objekte.

3. Konfiguriramo Group policy objekt, ki se nahaja na lokaciji `User Configuration\Windows Settings\Folder Redirection`, tako da preusmerimo mape, ki bi jih radi selili med profili, na lokacijo, ki je različna od trenutne lokacije roaming profilov. Poleg tega se moramo še prepričati, da v lastnostih map, ki jih bomo selili, opcija Grant the user exclusive rights to <Redirected Folder Name> NI obkljukana.

4. Shranimo spremembe, ki smo jih izvedli v GPO.

5. GPMC poženemo še na Windows Vista/Windows7/Windows Server 2008 računalniku in uredimo Group Policy objekt, ki smo ga kreirali oziroma urejali v korakih 2 in 3.

6. Preverimo nastavitve funkcionalnosti Folder Redirection, ki so definirane za preusmerjene mape v GPO. Prepričati se moramo še, da v lastnostih map, ki jih bomo selili, opcija Grant the user exclusive rights to <Redirected Folder Name> NI obkljukana. Izberemo pa še

opcijo Also apply redirection policy to Windows 2000, Windows 2000 Server, Windows XP, and Windows Server 2003 operating systems.

7. Ko shranimo nastavitve iz koraka 6, se bodo datoteke iz originalnega uporabniškega profila pojavile v novem V2 uporabniškem profilu.

3.5 Postavitev novega tiskalniškega strežnika

Zaradi prehoda na nove operacijske sisteme in 64-bitno tehnologijo je bilo potrebno postaviti tudi nov tiskalniški strežnik. Tudi to nalogo bo opravljal strežnik, na katerem bo nameščen operacijski sistem Windows Server 2008 R2 z nameščeno vlogo Print and Document Services. Ker so v podjetju v uporabi samo omrežni tiskalniki, bodo na tiskalniškem strežniku nameščeni vsi omrežni tiskalniki, ki so v uporabi na glavni lokaciji podjetja, ter tudi na nekaterih oddaljenih lokacijah. Namestili bomo tako 32- kot tudi 64-bitne gonilnike, tako da bo strežnik uporabnikom omogočal enostavno izbiro, namestitev in uporabo tiskalnikov v skupni rabi, ne glede na operacijski sistem, ki ga uporabljajo, administratorjem pa centralizirano upravljanje in nadzor vseh tiskalnikov.

Vlogo Print and Document Services namestimo po sledečem postopku:

1. Kliknemo Start, pokažemo na Administrative Tools in izberemo Server Manager.
2. Na levi strani z desnim miškinim gumbom kliknemo na Roles in nato na Add Roles.
3. V koraku Select Server Roles, v čarovniku Add Rolest, obkljukamo Print and Document Services.
4. V koraku Add Role Services obkljukamo vlogo Print server. To nam bo namestilo Print Server role service in Print Managment snap-in ter skonfiguriralo strežnik za vlogo tiskalniškega strežnika.
5. Če želimo omogočiti uporabnikom omejeno upravljanje s tiskalniki in tiskanjem, lahko obkljukamo še opcijo Internet Printing, kar namesti spletni vmesnik, ki teče s pomočjo Internet Information Services, do katerega lahko uporabniki dostopajo s spletnim brskalnikom.
6. Če želimo omogočiti dostop do tiskalnikov in tiskanje tudi uporabnikom, ki uporabljajo druge operacijske sisteme, moramo obljukati še opcijo LDP Service.
7. Ko izberemo željene opcije, kliknemo Next.
8. V primeru, da smo izbrali opcijo Internet Printing, bo potrebna tudi namestitev Internet Information Services (IIS), kar potrdimo s klikom na gumb Add Required Role Services.

9. Pred začetkom namestitve še preverimo, če smo izbrali pravilne nastavitve za namestitev, nato kliknemo gumb Install.

Po namestitvi vloge Print and Document Services in konfiguraciji tiskalniškega strežnika je potrebno namestiti še vse omrežne tiskalnike. To storimo po sledečem postopku:

1. Kliknemo Start, pokažemo na Administrative Tools in izberemo Print Managment.
2. Na levi strani kliknemo Print Servers, nato kliknemo na izbrani tiskalniški strežnik, z desnim miškinim gumbom kliknemo na Printers in izberemo Add Printer.
3. V prvem koraku čarovnika Network Printer Installation Wizard izberemo drugo opcijo: Add a TCP/IP or Web Services Printer by IP address or hostname. Samodejno iskanje in zaznava tiskalnikov v našem primeru namreč ni mogoča, ker se vsi tiskalniki ne nahajao v istem podomrežju kot tiskalniški strežnik.
4. V naslednjem koraku izberemo opcijo TCP/IP device, vpišemo IP naslov tiskalnika in kliknemo Next.
5. V naslednjem koraku izberemo že pravilni gonilnik za izbrani tiskalnik in kliknemo Next.
6. V naslednjem koraku vpišemo ime tiskalnika, ime tiskalnika za skupno rabo, njegovo lokacijo in morebitne komentarje. Izključimo še opcijo Share this printer in kliknemo Next.
7. Po želji lahko še natisnemo preizkusno stran oziroma zaključimo namestitev.

Ko so tiskalniki nameščeni, pa jim je potrebno namestiti še dodatne gonilnike. V orodju Print Management tool to storimo tako:

1. Z desnim miškinim gumbom kliknemo na tiskalnik, kateremu želimo namestiti dodatne gonilnike, in izberemo Manage Sharing.
2. Kliknemo na Additional Drivers. To nam odpre okno za namestitev dodatnih gonilnikov.
3. Obkljukamo procesorsko arhitekturo, za katero želimo namestiti dodatne gonilnike. Na primer: če na tiskalniškem strežniku teče 64-bitni operacijski sistem, to pomeni, da so 64-bitni gonilniki že privzeto nameščeni in je potrebno dodatno namestiti samo 32-bitne verzije gonilnikov. V tem primeru obkljukamo opcijo x86.
4. V primeru, da tiskalniški strežnik nima dodatnih gonilnikov, shranjenih v svoji shrambi, se nam odpre okno, ki nas vpraša za lokacijo dodatnih gonilnikov.

.

3.6 Nadgradnja HP Thin Client terminalov

Večina uporabnikov v podjetju bo do Remote Desktop strežnikov in objavljenih namizij ter aplikacij dostopala preko HP Thin Client terminalov. Na terminalih je nameščen operacijski sistem Windows CE različnih verzij. Ker je za dostopanje in uporabo vseh funkcij Remote Desktop Services na Windows Server 2008 R2 potreben vsaj Remote Desktop odjemalca verzije 6.0, je bilo potrebno terminale nadgraditi. Pri terminalih z operacijskim sistemom verzije 5.0 in 6.0 ni bilo nobenih težav. V Windows CE 6.0 je prava verzija RDC odjemalca že nameščena, terminale z operacijskim sistemom Windows CE 5.0 in 5.5 pa smo enostavno nadgradili s pomočjo vgrajenega orodja za nadgradnje. Novejše verzije operacijskega sistema za te terminale so namreč kupcem terminalov prosto dostopne preko spletne strani proizvajalca. Težave pa so se pojavile pri starejših terminalih z operacijskim sistemom verzije 4.2. Teh namreč ni mogoče nadgraditi na novejše verzije tako zaradi licenčnih kot tudi zaradi strojnih omejitev. Za te terminale smo zato uporabili alternativno verzijo dostopa, uporabo Linux operacijskega sistema s pomočjo zagona preko omrežja (network boot), ki je opisan v naslednjem poglavju.

3.7 Nadgradnja Linux terminalov

Kar nekaj uporabnikov pa za dostop uporablja Linux terminale. Ti terminali so narejeni iz starejših, že odsluženih računalnikov. Teh računalnikov zaradi premalo zmogljive strojne opreme ni več mogoče uporabljati za delovne postaje, za vlogo terminala pa so povsem zadovoljivi, saj se na terminalu izvajata le zaslonska slika in uporabnikova interakcija, vse zahtevnejše procesiranje pa se izvaja na strežniku. Ti terminali ne vsebujejo trdih diskov, ampak namesto tega uporabljajo majhen lahek Linux opreracijski sistem Thinstation, do katerega dostopajo preko omrežja (network boot). Čeprav je Thinstation operacijski sistem zasnovan na Linuxu, pa uporabniki tega sploh ne opazijo, saj se takoj po zagonu operacijskega sistema uporabniku prikaže prijavno okno Remote Desktop odjemalca in je zato uporabniška izkušnja povsem enaka, kot če bi uporabljali HP Thin Client terminale ali pa poganjali Remote Desktop odjemalca iz računalnika z operacijskim sistemom Windows. Nadgradnja teh terminalov ni bila problematična. Nadgraditi je bilo treba le sliko (image) Thinstation operacijskega sistema, ki se uporablja za zagon preko omrežja, in ji dodati novo verzijo RDP protokola. Vse to je bilo na voljo na spletni strani projekta Thinstation.

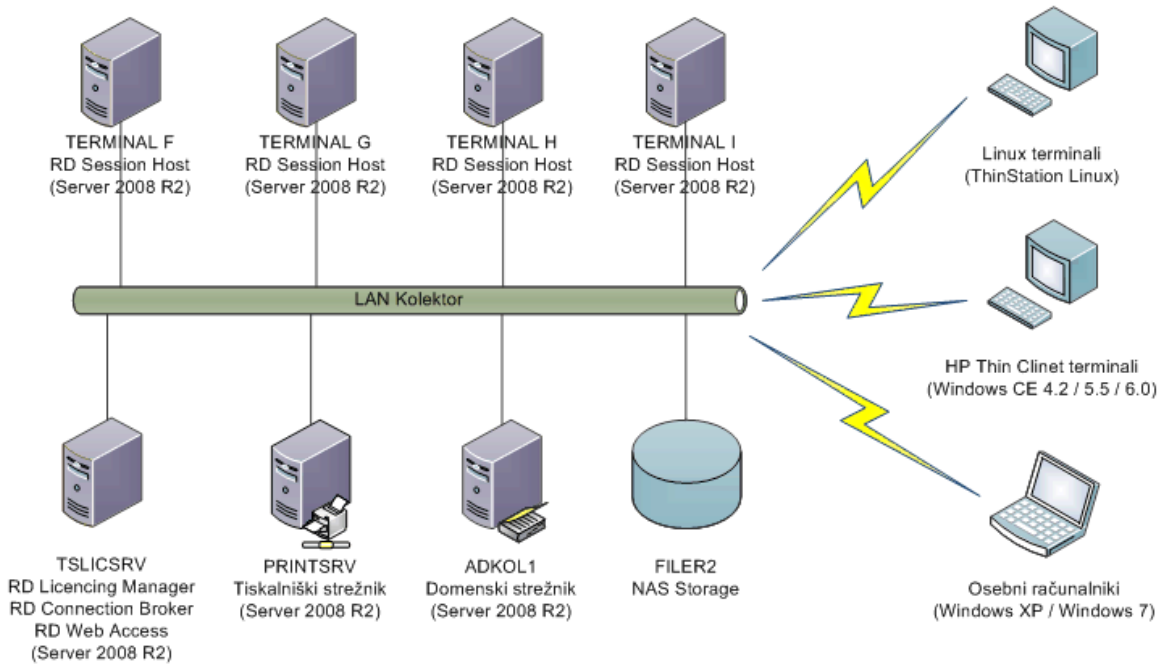
3.8 Izvedba pilotskega projekta

Preden smo se odločili za postavitev produkcijskega okolja Microsoft Remote Desktop Services, smo izvedli pilotski projekt. Za to smo se odločili uporabiti kar testno okolje, ki je po funkcionalnosti povsem identično produkcijskemu okolju, ki smo ga postavili kasneje, le

da je strežniška farma sestavljena le iz dveh strežnikov, kar pa je za pilotski projekt z majhnim številom uporabnikov povsem dovolj.

V pilotski projekt smo povabili približno deset uporabnikov, tako da smo vključili vse bistvene funkcije in oddelke podjetja. Cilj je bil namreč v praksi stestirati vse funkcionalnosti Remote Desktop Services. Uporabnikom smo najprej na kratko pojasnili bistvene novosti in spremembe, nato pa smo jim dali teden časa, da dobro preizkusijo novi sistem in preverijo izvedbo in delovanje vseh svojih vsakodnevnih opravkov in nalog.

3.9 Postavitev produkcijskih strežnikov



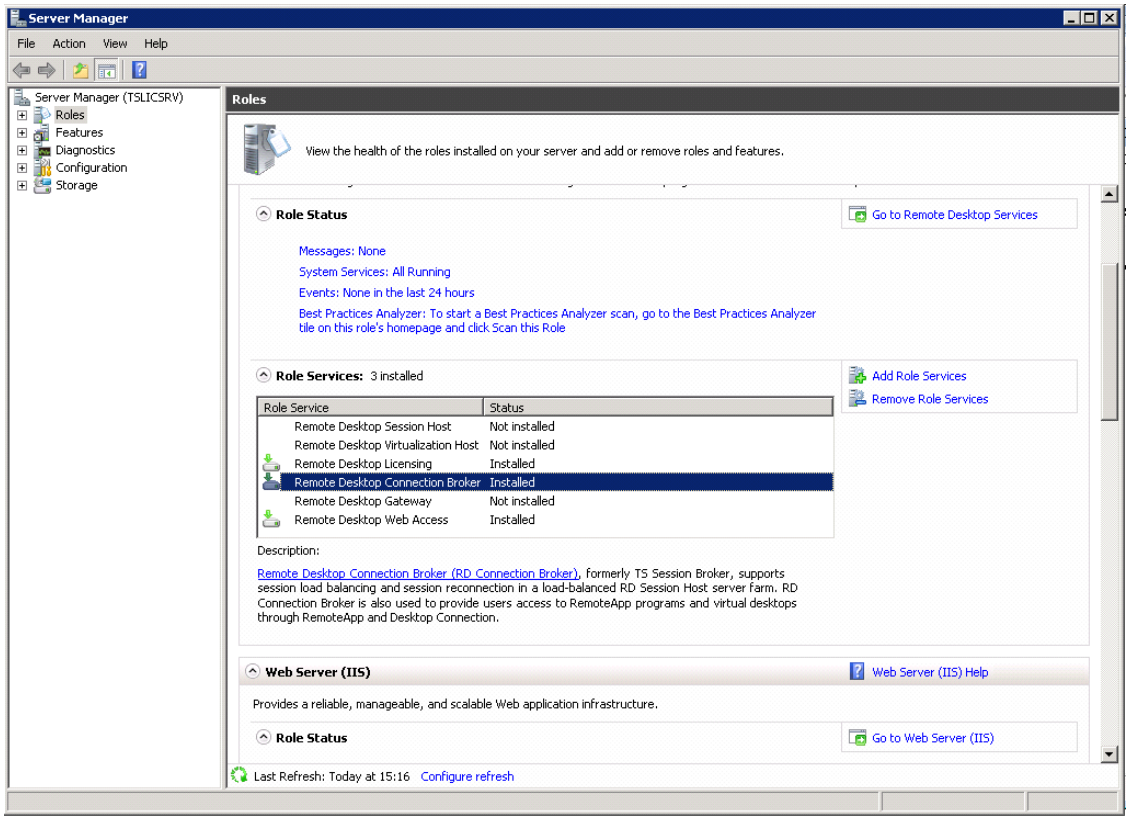
Slika 6: Diagram načrtovanega terminalskega okolja

3.9.1 Namestitev osnovnega operacijskega sistema

Sama namestitev operacijskega sistema Windows Server 2008 je precej preprosta. Ob zagonu strežnika izberemo opcijo zagona iz namestitvenega DVD-ja, nato pa nas namestitveni program popelje skozi nekaj opcij. Najprej si izberemo jezik, ki ga bomo uporabljali skozi namestitev. Naslednji korak je aktivacija izdelka. Vpišemo ključ izdelka in izberemo opcijo, da se operacijski sistem takoj po namestitvi avtomatsko aktivira. Na voljo imamo več verzij operacijskega sistema, tako da v naslednjem koraku izberemo tisto, ki nam najbolj ustreza. V našem primeru smo se odločili za osnovno, 64-bitno različico Windows Server 2008 Standard. Nato izberemo še, ali želimo polno namestitev, ali le Core verzijo, preberemo in

potrdimo Microsoftovo licenčno pogodbo. V naslednjem koraku izberemo še disk, kamor naj se operacijski sistem namesti, po potrebi lahko ustvarimo ali spremenimo particije. Nato sledi namestitev, ki na disku zasede približno 10 GB prostora in traja približno 20 minut, seveda odvisno od zmogljivosti strojne opreme. Po ponovnem zagonu računalnika se nam odpre prijavno okno, kjer se prijavimo kot administrator, ob prvi prijavi pa moramo obvezno spremeniti geslo. Po uspešni prijavi strežnik še priključimo v Active Directory domeno in ga tako postavimo v omrežje podjetja. Nato je potrebna še uvrstitev v ustrezno organizacijsko enoto v aktivnem imeniku (Active Directorij - AD). Za potrebe terminalske farme postavimo specifično organizacijsko enoto (Organizational Unit - OU), v katero bomo uvrstili vse terminalske strežnike, saj bodo le-ti vse konfiguracijske nastavitve dobili preko ustrezne skupinske politike (Group policy - GPO), ki bo vezana na ustrezno OU.

3.9.2 Namestitev storitve RD Session Host



Slika 7: Vloge v orodju Server Manager

Storitev RD Session Host je osnovna storitev, ki jo bomo namestili na strežnike v farmi. S pomočjo te storitve bodo uporabniki dostopali do aplikacij, ki jih bo strežniška farma gostila. Vlogo RD Session Host na strežnike namestimo tako, da sledimo naslednjemu postopku:

1. Na strežniku, kjer želimo namestiti vlogo RD Session Host, odpremo Administrative Tools ter iz skupine izberemo Server Manager.

2. V levem delu okna odpremo vejo Roles ter na desni strani izberemo Add Roles.
3. V naslednjem koraku kliknemo Next.
4. V naslednjem koraku izberemo Remote Desktop Services in kliknemo Next.
5. V naslednjem koraku kliknemo Next.
6. V koraku Select Role Services bomo izbrali samo RD Session Host vlogo. V celotni farmi bomo v končni fazi potrebovali tudi RD Session Broker in pa RD Licensing, vendar bomo ti vlogi namestili na specifična strežnika.
7. V naslednjem koraku preberemo obvestilo in kliknemo Next.
8. V koraku Specify Authentication Method for RD Session Host izberemo Do not require Network Level Authentication (čeprav bi bil to varnejši način, a nismo imeli ustrezne PKI infrastrukture, da bi lahko izdali certifikate) ter izberemo Next.
9. V koraku Specify Licensing Mode izberemo Configure later (konfiguracijo bomo kasneje izbvedli preko skupinskih politik) ter izberemo Next.
10. V naslednjem koraku poleg skupine Administrators, ki ima pravico prijave na terminalske strežnike, dodamo še specifično skupino, ki smo jo kreirali v AD, preko katere bomo nadzirali dostop do strežnikov. Za nadaljevanje namestitve kliknemo Next.
11. V naslednjem koraku pregledamo izbrane nastavitve in kliknemo Install.
12. Po končani namestitvi kliknemo Close, a ne izvedemo ponovnega zagona računalnika. Ponovni zagon bomo izvršili, ko bodo končane vse nastavitve.

3.9.3 Namestitev vloge RD Session Broker

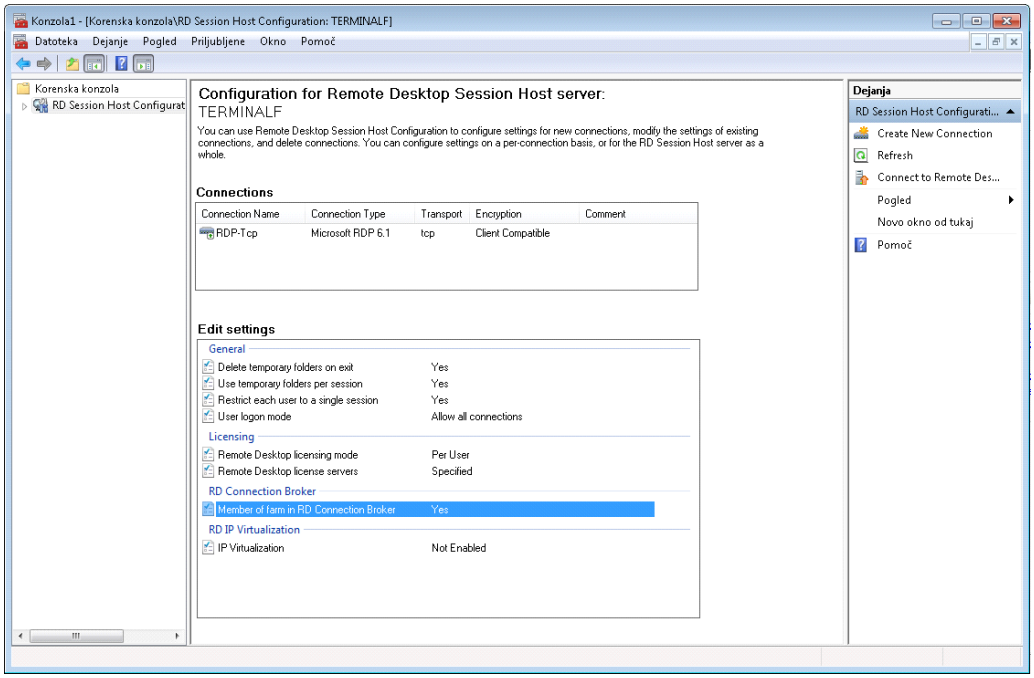
RD Session Broker vlogo je potrebno namestiti na strežnik, ki ga želimo uporabljati za nadzor informacij o uporabniških sejah v strežniških farmah, ki uporabljajo razporeditev obremenitve. RD Session Broker strežnik lahko zaradi majhne performančne obremenitve namestimo na manj zmogljive strežnike, prav tako pa ravno zaradi tega lahko posamezni strežnik uporabljamo tudi za več farm. Priporočeno je, da se RD Session Broker vlogo namesti na strežnike, ki niso hkrati terminalski strežniki. Tako to kasneje, ob morebitnih vzdrževalnih delih na posameznih terminalskih strežnikih, ne vpliva na delovanje RD Session Broker storitve.

Ob namestitvi RD Session Broker vloge pride na strežniku do sledečih sprememb:

- Namesti se RD Session Broker service, ki je privzeto nastavljena na nastavitvi Started in Automatic.
- Kreira se lokalna skupina Session Directory Computers.

Vlogo RD Session Broker namestimo po naslednjem postopku:

1. Kliknemo Start, pokažemo na Administrative Tools in izberemo Server Manager.
2. V razdelku Roles Summary kliknemo na Add Roles.
3. V koraku Before You Begin čarovnika Add Roles kliknemo Next.
4. V koraku Select Server Roles obkljukamo Terminal Services in kliknemo Next.
5. Pregledamo stran Terminal Services in kliknemo Next.
6. V koraku Select Role Services obkljukamo RD Session Broker in kliknemo Next.
7. V koraku Confirm Installation Selections kliknemo Install.
8. V koraku Installation Results preverimo, ali je namestitev uspela, nato kliknemo Close.



Slika 8: Nastavitve upravljalca z povezavami in sejami

Da lahko terminalski strežniki uporabljajo RD Session Broker, moramo njihove račune (computer account) dodati v skupino Session Directory Computers na RD Session Broker strežniku.

Terminalski strežnik dodamo v skupino Session Directory Computers po naslednjem postopku:

1. Na RD Session Broker strežniku kliknemo na Start, nato na Administrative Tools in izberemo Computer Management.

2. Na levi strani razširimo vejo Local Users and Groups in kliknemo na Groups.
3. Na desni strani z desnim miškinim gumbom kliknemo na skupino Session Directory Computers in nato izberemo Properties.
4. Kliknemo Add.
5. V koraku Select Users, Computers or Groups kliknemo na Object Types.
6. Obkljukamo Computers in kliknemo OK.
7. V naslednjem koraku poiščemo in dodamo račune za vse terminalske strežnike, ki bi jim radi omogočili uporabo RD Session Broker storitev.
8. Ko končamo, kliknemo OK.

Podrobnejše RD Session Broker nastavitve za terminalske strežnike v farmi smo izvedli s pomočju skupinskih politik (GPO), kar je tudi priporočeno s strani Microsofta. Te nastavitve so podrobneje opisane v poglavju 3.9.9.

3.9.4 Namestitev vloge RD Licensing

Za licenčno pokritost terminalskih strežnikov, ki jih uporabljamo v produkcijskem okolju, potrebujemo tudi vlogo RD Licensing, ki mora biti nameščena na enem izmed strežnikov.

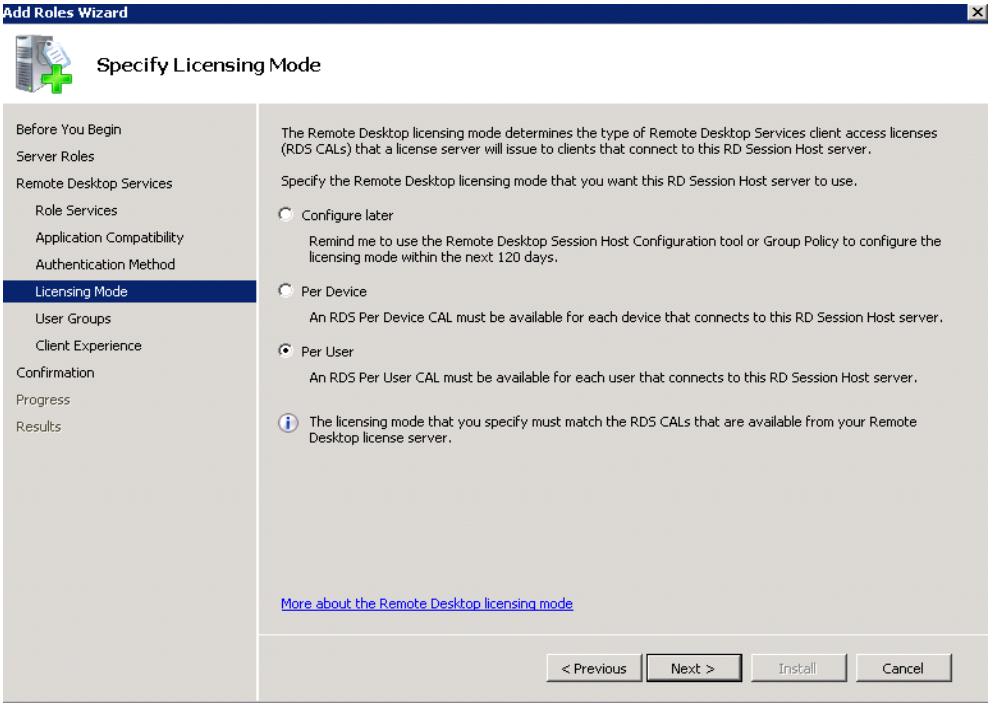
Vlogo namestimo po naslednjem postopku:

1. Kliknemo Start, nato Administrative Tools in nato Server Manager.
2. Na levi strani z desnim miškinim gumbom kliknemo na Roles in nato Add Roles.
3. V čarovniku Add Roles, v koraku Before You Begin, kliknemo Next.
4. V koraku Select Server Roles pod Roles obkljukamo Remote Desktop Services (Če nameščamo RD Licensing vlogo na strežnik, kjer je že nameščena vloga Terminal Services, bo ta opcija že izbrana in zatemnjena.).
5. V naslednjem koraku kliknemo Next.
6. V koraku Remote Desktop Services kliknemo Next.
7. V koraku Select Role Services obkljukamo RD Licensing
8. V koraku Configure Discovery Scope for RD Licensing nastavimo scope za naš licenčni strežnik.
9. V istem koraku nastavimo lokacijo, kjer bo shranjena RD Licensing podatkovna baza. V primeru, da bomo shranili podatkovno bazo na privzeto lokacijo, kliknemo Next. Če bi

radi izbrali posebno lokacijo za podatkovno bazo, kliknemo gumb Browse in izberemo direktorij, ki mora obvezno biti na lokalnem disku strežnika.

10. V naslednjem koraku Confirm Installation Selections preverimo, ali smo izbrali pravilne nastavitve za namestitev in kliknemo Install.

11. V koraku Installation Results preverimo, če so se vse opcije uspešno namestile, nato kliknemo Close.



Slika 9: Izbira vrste licenciranja

Ko je vloga RD Licensing nameščena, lahko uporabljamo orodje Remote Desktom Licensing Manager za povezavo na in upravljanje z Remote Desktop licenčnimi strežniki. Lincenčne strežnike lahko s pomočjo orodja RD Licensing Manager upravljamo tudi iz drugih računalnikov. Edini pogoj je, da si orodje prej namestimo.

Ko je RD Licensing Manager nameščen, se na licenčni strežnik povežemo po sledečem postopku:

1. Odpremo RD Licensing Manager. To storimo tako, da kliknemo na Start, pokažemo na Remote Desktop Services in izberemo RD Licensing Manager.

2. V meniju Action kliknemo Connect.

3. V polje Server vpišemo ime licenčnega strežnika, na katerega bi se radi povezali, nato kliknemo gumb Connect.

Ko se RD Licensing Manager zažene, skuša sam poiskati vse licenčne strežnike v omrežju, ki so avtomatsko dosegljivi in za katere ima trenutni uporabnik ustrezne administrativne pravice.

Po namestitvi je potrebno licenčni strežnik aktivirati, s čimer strežnik potrdimo in mu tako omogočimo dodeljevanje licenc. Aktivacijo izvedemo s pomočjo opcije Activate Server Wizard v orodju RD Licensing Manager Tool. Izvedemo jo lahko na tri načine, in sicer avtomatsko z direktno povezavo na Microsoft Clearinghouse, preko spletnega brskalnika ali pa preko telefona.

V našem primeru smo izbrali aktivacijo preko interneta. Pri tej metodi se s pomočjo TCP/IP protokola preko TCP vrat 443 povežemo direktno na Microsoft Clearinghouse. Izvedemo jo po sledečem postopku:

1. Kliknemo na Start menu, nato na Administrative tools, Remote Desktop Services in nato izberemo RD Licensing Manager.

2. Z desnim miškinim gumbom kliknemo na licenčni strežnik, ki ga želimo aktivirati, in izberemo Activate Server. To požene čarovnika za aktiviranje.

3. V naslednjem koraku kliknemo Next.

4. V koraku Connection Method iz seznama izberemo Automatic connection (recommended) in kliknemo Next.

5. V koraku Company Information vpišemo podatke, kot so ime odgovorne osebe, ime podjetja in državo oziroma regijo, kjer se podjetje nahaja, in kliknemo Next.

6. V naslednjem koraku lahko vpišemo še nekatere neobvezne dodatne informacije, kot sta e-poštni naslov in naslov podjetja.

7. Kliknemo Next in strežnik se aktivira.

8. V koraku Completing the Activate Server imamo dve možnosti:

    - če želimo namestiti licence na strežnik takoj, se prepričamo, ali je opcija Start Install Licenses Wizard now obkljukana, nato kliknemo Next in sledimo nadaljnjim navodilom.

    - če želimo namestiti licence kasneje, odstranimo kljukico iz opcije Start Install Licenses Wizard now in kliknemo Finish.

Licence Remote Desktop client access licenses (RDS CALs) lahko namestimo na tri načine: avtomatsko z direktno povezavo na Microsoft Clearinghouse, preko spletnega brskalnika ali pa preko telefona. V našem primeru smo se tudi tukaj odločili za avtomatsko namestitev. Avtomatska metoda zahteva internetno povezavo na računalniku, s katerega poganjamo orodje Remote Desktop Licensing Manager. Tako v primeru, da poganjamo orodje z drugega računalnika, licenčni strežnik ne potrebuje internetne povezave. Metoda uporablja protokol TCP/IP, natančneje TCP vrata 443, preko katerih se poveže direktno na Microsoft Clearinghouse. Izvedli smo jo po naslednjem postopku:

1. Najprej odpremo Remote Desktop Licensing Manager. To storimo tako, da kliknemo Start, nato Administrative Tools, pokažemo na Remote Desktop Services in izberemo Remote Desktop Licensing Manager.

2. Preverimo, ali je metoda za povezavo nastavljena na Automatic connection (recommended). To storimo tako, da z desnim miškinim gumbom kliknemo na licenčni strežnik, na katerega želimo namestiti licence, in kliknemo Properties. V zavihku Connection Method preverimo in po potrebi spremenimo metodo za povezavo, nato kliknemo OK.

3. Z desnim miškinim gumbom kliknemo na licenčni strežnik, na katerega želimo namestiti licence, in kliknemo Install Licenses. To zažene čarovnika Install Licenses Wizard.

4. V prvem koraku kliknemo Next.

5. V koraku License Program izberemo, na kakšen način smo kupili licence in kliknemo Next.

6. Glede na izbiro v prejšnjem koraku čarovnik ugotovi, katere podatke je treba vnesti v tem koraku. Večinoma je potrebno zgolj vpisati licenčno številko oziroma številko pogodbe, sklenjene z Microsoftom.

7. Ko vnesemo zahtevane podatke, kliknemo Next.

8. V koraku Product Version and License Type izberemo željeno verzijo, tip in število licenc za naše okolje. Vsi podatki so odvisni od tega, kakšne licence smo kupili.

9. Ko vnesemo zahtevane podatke, kliknemo Next.

10. Čarovnik se avtomatsko poveže z Microsoft Clearinghouse, ki preveri in odobri našo zahtevo. Nato se licence avtomatsko namestijo na licenčni strežnik.

11. Za zaključek namestitve licenc kliknemo Finish. Licenčni strežnik zdaj lahko dodeljuje licence odjemalcem, ki se povezujejo na Remote Desktop Session Host strežnike.

3.9.5 Network Load Balancing

Network Load Balancing (NLB) oziroma po slovensko omrežna razporeditev obremenitve je omrežna tehnologija, ki jo Microsoft ponuja v vseh svojih operacijskih sistemih iz družine Windows Server. NLB uporablja razdelitveni algoritem za razporeditev omrežnega prometa na več gostiteljev. Na ta način pomaga izboljšati razširljivost in razpoložljivost kritičnih IP storitev, kot so spletni strežniki, navidezna zasebna omrežja, pretočne multimedijske vsebine, terminalske storitve, proxy strežniki ... NLB prav tako omogoča visoko dostopnost s pomočjo zaznavanja napak na posameznih gostiteljih in samodejno prerazporeditev prometa na ostale delujoče gostitelje.

Za ustrezno razporeditev zahtev zunanjih uporabnikov terminalskih storitev imamo v splošnem dve možnosti realizacije, in sicer:

- Uporaba Network Load Balancing funkcionalnosti v Windows Server 2008
- DNS mehanizem Round Robin

Z vidika administracije je bistveno lažji mehanizem Round Robin, vendar se nam lahko zgodi, da uporabnik s pomočjo tega mehanizma vseeno poskuša vzpostaviti povezavo z nedelujočim strežnikom (vendar samo enkrat), pri mehanizmu NLB (Network Load Balancing) pa te možnosti praktično ni. V okviru NLB mehanizma bo uporabnik poskušal vzpostaviti povezavo samo z aktivnimi strežniki, vendar pa je implementacija postavitve kompleksnejša.

3.9.5.1 Namestitev NLB

NLB funkcionalnost mora biti nameščena na vseh strežnikih, ki bodo postali del terminalske farme.

Funkcionalnost namestimo po naslednjem postopku:

1. Kliknemo Start, nato na Administrative tools in izberemo Server Manager.
2. Iz drevesne strukture na levi izberemo Features in na desni kliknemo na Add Feature.
3. Iz seznama možnosti izberemo Network Load Balancing in kliknemo Next.
4. Počakamo, da se namestitev zaključi in kliknemo gumb Close.

3.9.5.2 Konfiguracija NLB

Po končani namestitvi je potrebno NLB še konfigurirati. Za to uporabimo konzolo, ki se je dodala v skupino Administrative Tools po uspešni namestitvi funkcionalnosti.

NLB konfiguriramo po naslednjem postopku:

1. Kliknemo Start, pokažemo na Administrative Tools in kliknemo na Network Load Balancing Manager.
2. Iz menija izberemo Cluster ter možnost New (To naredimo samo prvič, ko NLB postavljamo. Če želimo konfigurirati obstoječi NLB, izberemo Connect to Existing.).
3. V nadaljevanju izberemo ime strežnika, kjer bomo kreirali NLB gručo in pa javno mrežno kartico, preko katere bodo na strežnik dostopali odjemalci. Za nadaljevanje postopka kliknemo Next.

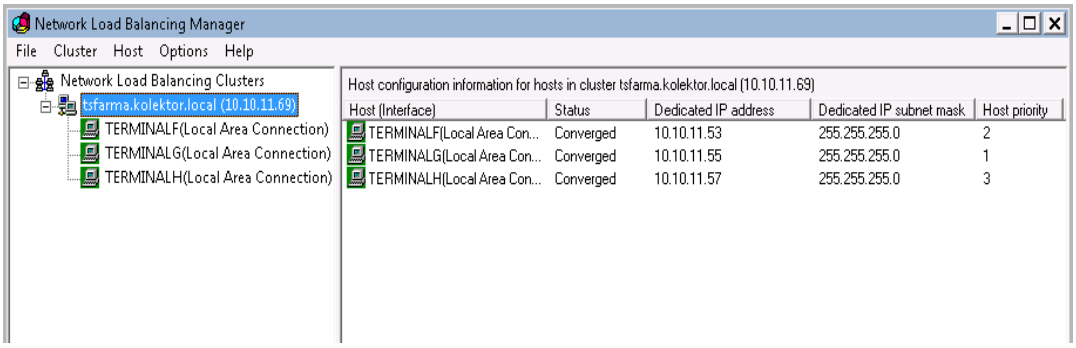
4. V nadaljevanju pregledamo nastavitve in nadaljujemo z Next.

5. V naslednjem koraku dodamo (določimo) virtualni IP, ki ga bo imela NLB gruča. Tako bo javna mrežna kartica dobila še en IP naslov (Virtualni IP naslov), preko katerega bodo dosegljivi vsi strežniki, ki bodo pripadali NLB gruči.

6. V naslednjem koraku izberemo ime NLB gruče, kot bo zapisana v DNS strežniku, ter izberemo Next.

7. V nadaljevanju lahko po potrebi omejimo vrata, preko katerih bo NLB deloval, in kliknemo Finish.

S tem je kreiranje NLB gruče končano. V naslednjih korakih je potrebno v NLB gručo samo še dodati ustrezne strežnike.



Slika 10: Strežniki, vključeni v gručo za razporeditev obremenitve

3.9.5.3 Dodajanje strežnikov v NLB gručo

Vsak terminalski strežnik, za katerega želimo, da je del neke farme, je potrebno dodati tudi v NLB gručo. Na ta način bo dosegljiv preko enotnega IP naslova.

Če želimo strežnik dodati v NLB, je potrebno izpolniti določene kriterije:

- Strežnik mora imeti dve mrežni kartici, eno povezano v javno omrežje, drugo pa povezano v privatno – NLB omrežje.
- Nameščeno mora imeti NLB funkcionalnost.

Ob izpolnjenih predpogojih za dodajanje v NLB gručo je postopek dodajanja sledeči:

1. Odpremo Network Load Balancing Manager na enem izmed računalnikov, ki je že del NLB gruče.
2. Z desnim gumbom miške kliknemo na ime NLB gruče in iz menija izberemo Add node …
3. V naslednjem koraku izberemo Host računalnik, ki bi ga želeli včlaniti v NLB gručo. Ko se na računalnik povežemo, se v spodnjem delu prikažejo tudi mrežne kartice, ki so na

strežniku konfigurirane. Iz seznama izberemo javno mrežno kartico (preko katere se bodo povezovale delovne postaje) in kliknemo Next.

4. V naslednjem koraku preverimo nastavitve (IP naslov (javni), stanje ob zagonu (Started)) in kliknemo Next.

5. V nadaljevanju lahko po potrebi omejimo porte, preko katerih bo NLB deloval, in kliknemo Finish. S tem je dodajanje v NLB gručo končano.

Po konfiguraciji NLB in dodajanju strežnikov v NLB gručo lahko delovanje le te preizkusimo tako, da se poskušamo povezati na terminalsko farmo, obenem pa izklapljamo strežnike, ki so del gruče.

3.9.6 Namestitev uporabniške programske opreme

Aplikacije, za katere bi radi, da do njih dostopajo terminalski uporabniki, je potrebno namestiti na poseben način, s pomočjo opcije Install application on Remote Desktop v nadzorni plošči Control Panel. Ta opcija prestavi operacijski sistem v tako imenovani Install mode, ki omogoča nameščanje in pravilno nastavitev aplikacij za delovanje v večuporabniškem okolju. Aplikacije namestimo po sledečem postopku:

1. Poženemo Install application on Remote Desktop. To storimo tako, da kliknemo na Start in izberemo Control Panel. V oknu Control Panel kliknemo na Install application on Remote Desktop.

2. S pomočjo čarovnika poiščemo zagonsko datoteko aplikacije, ki jo želimo namestiti, in sledimo namestitvenemu postopku aplikacije.

3. Drugi korak ponovimo za vse aplikacije, ki jih želimo namestiti.

V primeru, da moramo namestiti veliko število aplikacij, si lahko namestitev olajšamo tako, da sami vključimo ali izključimo Install mode. Na ta način ni več potrebno uporabljati opcije Install applications on Remote desktop in njenega čarovnika za namestitev vsake posamezne aplikacije. Install mode vključimo iz ukazne vrstice z ukazom `change user /install`. Ko zaključimo z nameščanjem aplikacij, pa preklopimo nazaj v tako imenovani Execute mode, ki omogoča poganjanje večuporabniških aplikacij, z ukazom `change user /execute`.

3.9.7 Namestitev vloge RD Web Access

Vlogo RD Web Access je moramo namestiti na strežnik, preko katerega bodo uporabniki s pomočjo spletnega vmesnika dostopali do RemoteApp programov, nameščenih na terminalskih strežnikih. Ko nameščamo RD Web Access vlogo, se hkrati namesti tudi komponenta Microsoft Internet Information Services, ki deluje kot spletni strežnik, na katerem teče spletni vmesnik.

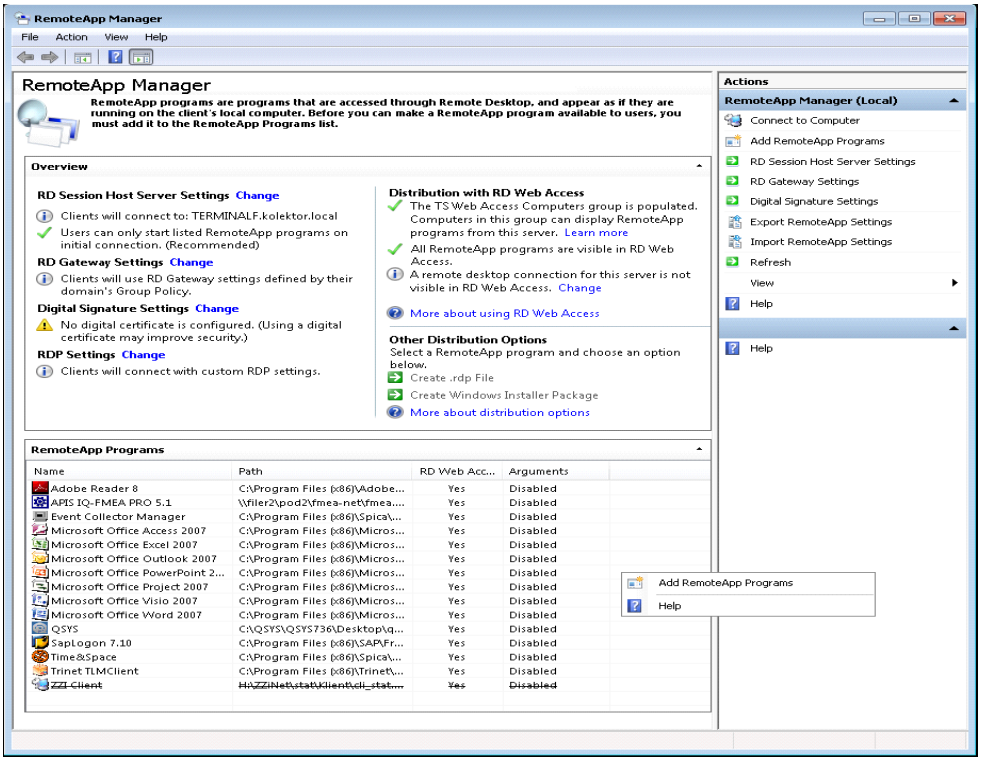
Vlogo RD Web Access namestimo po sledečem postopku:

1. Na strežniku, na katerega bi radi namestili vlogo RD Web Access, odpremo Server Manager. To storimo tako, da kliknemo Start, pokažemo na administrative Tools in izberemo Server Manager.
2. V primeru, da je vloga Remote Desktop Services že nameščena:
    - V razdelku Roles Summary kliknemo Add Roles.
    - V koraku Before You Begin kliknemo Next.
    - V koraku Select Server Roles obkljukamo Remote Desktop Services in kliknemo Next.
    - V koraku Remote Desktop Services preverimo nastavitve in kliknemo Next.
    - V koraku Select Role Services obkljukamo Remote Desktop Web Access.
3. V primeru, da vloga Remote Desktop Services še ni nameščena:
    - V koraku Roles Summary kliknemo na Remote Desktop Services.
    - V koraku Role Services kliknemo Add Role Services.
    - V koraku Select Role Services obkljukamo Remote Desktop Web Access.
4. V naslednjem koraku preverimo podatke o dodatnih zahtevanih komponentah in kliknemo Add Required Role Services.
5. V naslednjem koraku kliknemo Next.
6. V koraku Web Server (IIS) preverimo podatke in kliknemo Next.
7. V koraku Select Role Services, kjer lahko izberemo dodatne komponente za IIS, kliknemo Next.
8. V koraku Confirm Installation Selections kliknemo Install.
9. V zadnjem koraku preverimo, ali se je namestitev uspešno zaključila, in kliknemo Close.

3.9.8 Konfiguracija strežnika RD Web Access in aplikacij RemoteApp

3.9.8.1 Dodajanje aplikacij v RemoteApp seznam

Da bodo programi, ki so nameščeni na RD Session host strežniku, na voljo oddaljenim uporabnikom, jih je potrebno dodati na seznam RemoteApp programov. To storimo po naslednjem postopku:



Slika 11: Dodajanje aplikacij v RemoteApp seznam

1. Na RD Session Host strežniku odpremo RemoteApp Manager. To storimo tako, da kliknemo Start, pokažemo na Administrative Tools, nato na Remote Desktop Services in nato kliknemo RemoteApp Manager.

2. V razdelku Actions kliknemo na Add RemoteApp Programs.

3. V koraku Welcome to the RemoteApp Wizard kliknemo Next.

4. V koraku Choose programs to add to the RemoteApp Programs list obkljukamo programe, ki bi jih radi dodali na seznam RemoteApp programov. Naenkrat lahko označimo tudi več programov. V koraku Choose programs to add to the RemoteApp Programs list so prikazani samo programi, ki jih čarovnik najde v All Users Start menuju na RD Session Host strežniku. Če programa, ki ga želimo dodati, ni na seznamu, kliknemo na gumb Browse in poiščemo in izberemo zagonsko datoteko (.exe) željenega programa.

5. Do nastavitev za posamezni RemoteApp program pridemo tako, da z desnim miškinim gumbom kliknemo na ime programa in izberemo Properties. Nastavljamo lahko sledeče:
    - Ime programa, ki bo prikazano uprabnikom.
    - Pot do zagonske datoteke programa.
    - Alias programa, ki je enolični identifikator programa in je po navadi kar enak imenu programa brez končnice.
    - Ali je program na voljo preko RD Web Access.
    - Ali so pri zagonu programa dovoljeni argumenti ukazne vrstice.
    - Ikono programa.
    - Uporabnike oziroma skupine uporabnikov, ki imajo dostop do programa preko spletnega vmesnika RD Web Access.
6. Ko zaključimo z nastavljanjem lastnosti programa, kliknemo OK in nato Next.
7. V koraku Review Settings preverimo nastavitve in kliknemo Finish.

Programi, ki smo jih izbrali, bi se zdaj morali pojaviti na seznamu RemoteApp programov.

3.9.8.2 Nastavitev pravic za dostop do RemoteApp programov

Po privzetih nastavitvah imajo do RemoteApp programov preko spletnega vmesnika RD Web Access dostop vsi avtenticirani domenski uporabniki. Po potrebi pa lahko pravice za dostop do posameznih programov omejimo na nivoju uporabnikov oziroma skupin uporabnikov. Pravico za dostop do posameznih programov uporabnikom oziroma skupinam nastavimo po sledečem postopku:

1. Na RD Session Host strežniku odpremo RemoteApp Manager. To storimo tako, da kliknemo Start, pokažemo na Administrative Tools, nato na Remote Desktop Services in nato kliknemo RemoteApp Manager.
2. Na seznamu RemoteApp programov kliknemo na program, do katerega želimo omejiti dostop.
3. V razdelku Actions kliknemo na Properties in nato User Assignment tab.
4. V naslednjem koraku kliknemo Specified domain users and domain groups, nato kliknemo Add.
5. V naslednjem koraku v oknu Select Users or Groups izberemo uporabnike oziroma skupine, ki jim želimo omogočiti dostop do izbranega programa.

6. Kliknemo OK, da zapremo okno Select Users or Groups.
7. Kliknemo OK, da zapremo okno RemoteApp Properties.

3.9.8.3 Vključitev RemoteApp programov v RD Web Access

Privzeto so vsi RemoteApp programi vključeni za uporabo preko RD Web Access, že takoj ko jih dodamo na RemoteApp seznam na RD Session Host strežniku. Po sledečem postopku lahko na RD session Host strežniku, kjer so konfigurirani RemoteApp programi, ugotovimo, če je posamezni program vključen v RD Web Access oziroma spremenimo to nastavitev:

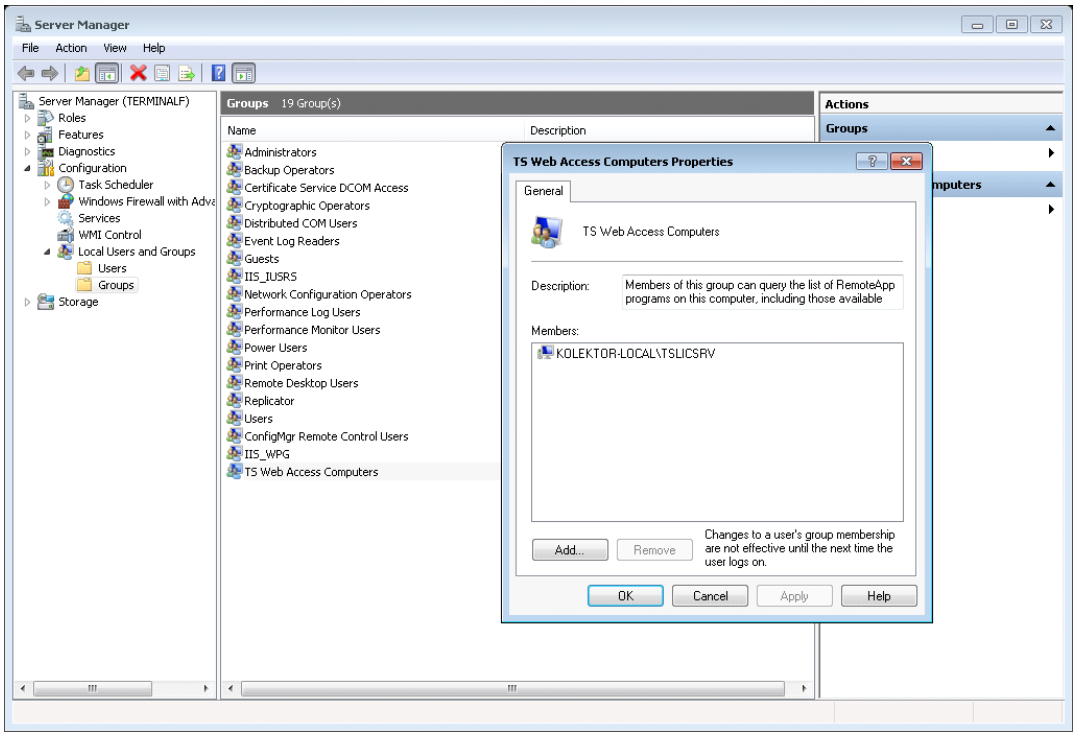
1. Na RD Session Host strežniko odpremo RemoteApp Manager. To storimo tako, da kliknemo Start, pokažemo na Administrative Tools, nato na Remote Desktop Services in izberemo RemoteApp Manager.
2. V seznamu RemoteApp programov preverimo, ali je pri programu, ki ga želimo vključiti v RD Web Access, v stolpcu RD Web Access zapisana beseda Yes.
3. Nastavitev spremenimo tako, da kliknemo na ime programa in v razdelku Actions izberemo Show za vklop oziroma Hide za izklop vključitve programa v RD Web Access.

3.9.8.4 Dodajanje RD Web Access strežnika v varnostno skupino

V primeru, da sta RD Web Access strežnik in RD Session Host strežnik, ki gosti RemoteApp programe, različna strežnika, je potrebno računalniški račun RD Web Access strežnika dodati v varnostno skupino RD Web Access Computers na RD Session Host strežniku. To naredimo po sledečem postopku:

1. Na RD Session Host strežniku kliknemo Start, pokažemo na Administrative Tools in izberemo Computer Managment.
2. Na levi strani razširimo Local Users and Groups in nato kliknemo na Groups.
3. Na desni strani dvokliknemo RD Web Access Computers.
4. V oknu RD Web Access Computers Properties kliknemo Add.
5. V oknu Select Users, Computers or Groups kliknemo Object Types.
6. V oknu Object Types obkljukamo Computers in kliknemo OK.
7. V vnosno polje Enter the object names to select vpišemo ime uporabniškega računa RD Web Access strežnika in kliknemo OK.

8. V zadnjem koraku kliknemo OK, da zapremo okno RD Web Access Computers Properties.



Slika 82: Nastavljanje varnostnih skupin za strežnik za spletni dostop

3.9.8.5 Konfiguracija spletnega vmesnika RD Web Access strežnika

Če želimo uporabnikom omogočiti dostop do RemoteApp aplikacij in Remote Desktop Connection preko spletnega vmesnika, moramo konfigurirati RD Web Access in navesti vir, ki bo zagotavljal RemoteApp aplikacije in navidezna namizja, ki bodo prikazana uporabnikom. RD Web Access lahko nastavimo za uporabo enega od naslednjih virov:

- Remote Desktop Connection Broker strežnik
- RemoteApp vir

RD Connection Broker strežnik omogoča uporabnikom dostop do virtualnih namizij ki gostujejo na RD Virtualization strežnikih, in do RemoteApp programov, ki gostujejo na oddaljenih RD Session Host strežnikih.

RemoteApp vir je individualni RD Session Host strežnik ali farma, sestavljena iz več enako nastavljenih RD Session Host strežnikov, na katerih so konfigurirani RemoteApp programi. Določimo lahko več RemoteApp virov.

Vir, ki bo zagotavljal RemoteApp aplikacije, nastavimo po sledečem postopku:

1. Povežemo se na RD Web Access spletno stran. To lahko storimo po enem izmed dveh postopkov:

   - Na RD Web Access strežniku kliknemo Start, pokažemo na Administrative Tools, nato na Remote Desktop Services in nato kliknemo Remote Desktop Web Access Configuration.

   - S pomočjo Internet Explorerja se povežemo na RD Web Access spletno stran. Po privzetih nastavitvah je spletna stran dosegljiva na sledečem naslovu: `https://ime_streznika/rdweb`, kjer je ime_streznika fully quailified domain name (FQDN) RD Web Access strežnika.

2. Na spletno stran se prijavimo ali z uporabniškim računom lokalnega administratorja na RD Web Access strežniku ali pa z uporabniškim računom, ki je član skupine RD Web Access Administrators na RD Web Access strežniku.

3. V naslovni vrstici kliknemo na Configuration.

4. V naslednjem koraku izberemo enega izmed željenih virov: RD Connection Broker ali pa One or more RemoteApp sources. Če smo izbrali RD Connection Broker strežnik, v polje Source name vpišemo NetBIOS ime oziroma FQDN RD Connection Broker strežnika. Če pa smo izbrali One or more RemoteApp sources, v polje Source name vpišemo NetBIOS ime oziroma FQDN RemoteApp vira. Če bomo kot vir uporabljali farmo RD Session Host strežnikov, vpišemo DNS ime farme. V primeru, da bomo uporabljali več RemoteApp virov, vpišemo v polje imena vseh virov, ki jih ločimo s podpičji.

5. Ko končamo, kliknemo OK, da shranimo spremembe.

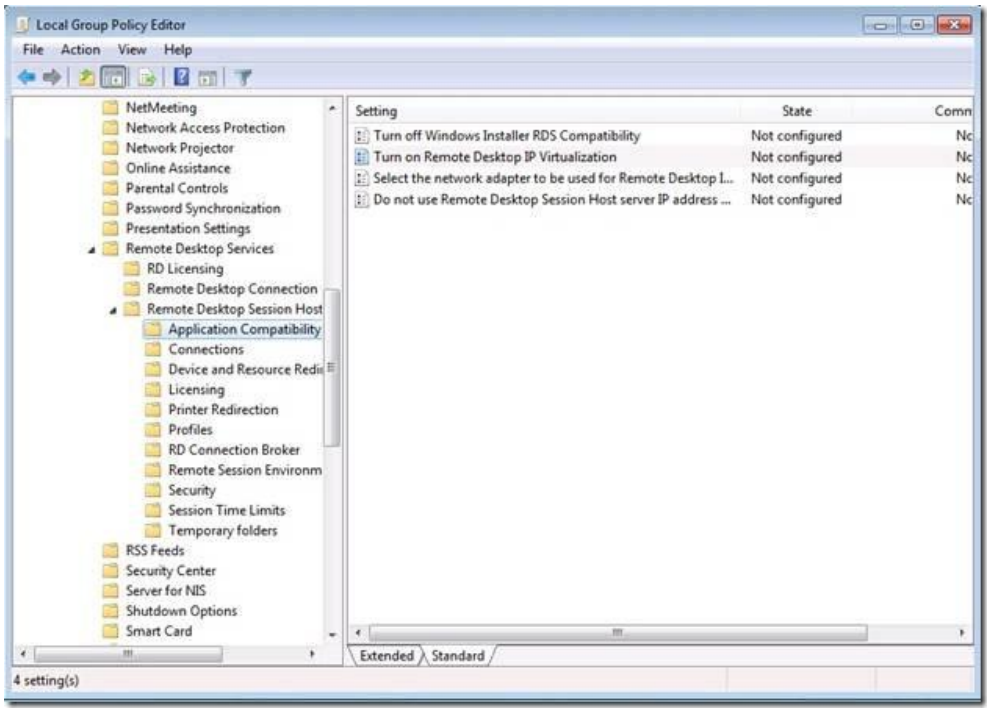
Slika 93: Nastavljanje spletnega vmesnika

V primeru, da smo za vir izbrali One or more RemoteApp sources, je potrebno vpisati še ime in ID povezave. Ime bo uporabljeno za identifikacijo povezave med RD Web Access strežnikom in uporabnikom. To storimo tako, da na RD Web Access strežniku s pomočjo tekstovnega urejevalnika odpremo datoteko `%windir%\Web\RDWeb\App_Data\RDWebAccess.config` in vpišemo zahtevane podatke.

Tudi v primeru, da smo za vir izbrali RD Connection Broker strežnik, je potrebno vpisati še ime in ID povezave. To pa storimo s pomočjo orodja Remote Desktop Connection Manager tool na RD Connection Broker strežniku.

3.9.9 Konfiguracija strežnikov s skupinskimi politikami

Group Policy (oziroma slovensko skupinske politike) je niz pravil, ki jih lahko uporabimo za nadzor oziroma konfiguracijo delovnega okolja ter uporabniških in računalniških računov v okolju Windows. V Microsoftovih operacijskih sistemih so prisotne že od Windows NT dalje. Skupinske politike omogočajo centralizirano upravljanje in konfiguracijo operacijskih sistemov, aplikacij in nastavitve uporabniških računov v Active Directory okolju. Z drugimi besedami, skupinske politike omejujejo to, kaj uporabnik lahko in česa ne more narediti na računalniškem sistemu. Uporabljajo se jo za omejevanje določenih aktivnosti, ki lahko predstavljajo varnostno tveganje, na primer: onemogočajo dostop do upravitelja opravil, omejujejo dostop do določenih map, onemogočajo prenos potencialno nevarnih datotek ... Zaradi teh funkcionalnosti se skupinske politike zelo pogosto uporabljajo v okoljih večjih podjetij, pa tudi v raznoraznih manjših organizacijah, kot so na primer šole, fakultete in podobne ustanove ter manjša podjetja.



Slika 104: Urejevalnik skupinskih politik

V našem projektu smo skupinske politike uporabili v dveh primerih: pri konfiguraciji terminalskih strežnikov in konfiguraciji oziroma omejitvah terminalskih uporabnikov. Opcije, ki smo jih uporabili, so opisane v naslednjih dveh poglavjih.

3.9.9.1 Skupinske politike, ki konfigurirajo terminalske strežnike

Lokacija	Nastavitev
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections	
Restrict Remote Desktop Services users to a single Remote Desktop session	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection	
Do not allow driver redirection	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Licensing	
Use the specified Remote Desktop license servers	Enabled (tslicsrv.kolektor.local)
Set the Remote Desktop licensing mode	Enabled (Per User)
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Profiles	
Set Remote Desktop Services User Home Directory	Enabled (\\filer2\home)
Set path for Remote Desktop Services Roaming User Profile	Enabled (\\filer2\profiles)
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\RD Connection Broker	
Configure RD Connection Broker farm name	Enabled (tsfarma.kolektor.local)
Configure RD Connection Broker server name	Enabled (tslicsrv.kolektor.local)
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Remote Session Environment	
Remove »Disconnect« option from Shut Down dialog	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits	
Set time limit for disconnected sessions	Enabled (30 minutes)
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security	
Allways prompt for password upon connection	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary folders	
Don not delete temp folder upon exit	Disabled
Do not use temporary folders per session	Disabled

Tabela 2: Skupinske politike, ki konfigurirajo terminalske strežnike

3.9.9.2 Skupinske politike, ki konfigurirajo terminalske uporabnike

Lokacija	Nastavitev
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options	
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Interactive logon: Do not display last user name	Enabled
Computer Configuration\Windows Settings\Security Settings\System Services	
Help and Support	Disabled
Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services	
Restrict Terminal Services users to a single remote session	Enabled
Remove Disconnect option from Shut Down dialog box	Enabled
Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services \Client/Server data redirection	
Do not allow drive redirection	Enabled
Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services \Sessions	
Set time limit for disconnected sessions	Enabled
Computer Configuration\Administrative Templates\System\Group Policy	
User Group Policy loopback processing mode	Enabled
User Configuration\Windows Settings\Folder Redirection	
My Documents	Enabled
User Configuration\Administrative Templates\Windows Components\Internet Explorer	
Search: Disable Find Files via F3 within the browser	Enabled
User Configuration\Administrative Templates\Windows Components\Internet Explorer\Browser menus	
Disable Context menu	Enabled
User Configuration\Administrative Templates\Windows Components\Application Compatibility	
Prevent access to 16-bit applications	Enabled
User Configuration\Administrative Templates\Windows Components\Windows Explorer	
Remove the Folder Options menu item from the Tools menu	Enabled
Remove File menu from Windows Explorer	Enabled
Remove Map Network Drive and Disconnect Network Drive	Enabled
Remove Search button from Windows Explorer	Enabled
Remove Security Tab	Enabled
Remove Windows Explorer's default context menu	Enabled

Hide the Manage item on the Windows Explorer shortcut menu	Enabled
Hide these specified drives in My Computer	Enabled (A, B, C, and D drives only)
Prevent access to drives from My Computer	Enabled (A, B, C, and D drives only)
Remove Hardware tab	Enabled
No “Computers Near Me” in My Network Places	Enabled
No “Entire Network” in My Network Places	Enabled
Turn off Windows+X hotkeys	Enabled
Turn on Classic Shell	Enabled
User Configuration\Administrative Templates\Windows Components\Windows Explorer \Common Open File Dialog	
Hide the common dialog places bar	Enabled
User Configuration\Administrative Templates\Windows Components\Task Scheduler	
Prohibit Task Deletion	Enabled
Hide Property Pages	Enabled
Prevent Task Run or End	Enabled
Prohibit New Task Creation	Enabled
User Configuration\Administrative Templates\Windows Components\Windows Messenger	
Do not allow Windows Messenger to be run	Enabled
Configuration\Administrative Templates\Windows Components\Windows Update	
Remove access to use all Windows Update features	Enabled
User Configuration\Administrative Templates\Start Menu & Taskbar	
Remove links and access to Windows Update	Enabled
Remove common program groups from Start Menu	Enabled
Remove pinned programs list from Start Menu	Enabled
Remove Network Connections from Start Menu	Enabled
Remove the Search menu from Start Menu	Enabled
Remove Drag-and-Drop shortcut menus on Start Menu	Enabled
Remove Favorites menu from Start Menu	Enabled
Remove Help menu from Start Menu	Enabled
Remove Run menu from Start Menu	Enabled
Remove My Network Place icon from Start Menu	Enabled
Add Logoff to Start Menu	Enabled
Remove and prevent access to Shut Down command	Enabled

Prevent changes to Taskbar and Start Menu settings	Enabled
Remove access to the shortcut menus for the taskbar	Enabled
User Configuration\Administrative Templates\Desktop	
Remove Properties from My Documents shortcut menu	Enabled
Remove Properties from My Computer shortcut menu	Enabled
Remove Properties from Recycle Bin shortcut menu	Enabled
Hide My Network Places icon on desktop	Enabled
Prohibit user from changing My Documents path	Enabled
User Configuration\Administrative Templates\Control Panel\Add or Remove Programs	
Remove Add or Remove Programs	Enabled
User Configuration\Administrative Templates\System	
Prevent access to the command prompt	Enabled
Prevent access to registry editing tools	Enabled
User Configuration\Administrative Templates\System\CTRL+ALT+DEL Options	
Remove Task Manager	Enabled
User Configuration\Administrative Templates\System\Scripts	
Run legacy logon scripts hidden	Enabled

Tabela 3: Skupinske politike, ki konfigurirajo terminalske uporabnike

4. Prehod na novi sistem

4.1 Postopna selitev uporabnikov na novi sistem

Po uspešno zaključenih vseh fazah postavitve, konfiguracije in testiranja produkcijske Remote Desktop Services strežniške farme je sledila selitev uporabnikov na novi sistem. Selitve smo se lotili postopoma, tako da smo najprej preselili uporabnike v enem oddelku, nato uporabnike v naslednjem in tako dalje. Preselili smo vsakega uporabnika posebej, tako da smo na njegovem odjemalcu za privzeto povezavo nastavili novo Remote Desktop Services farmo, staro pa odstranili. Po prvi prijavi na nove strežnike pa je bilo potrebno še prekopirati uporabnikove dokumente in ostale datoteke na nove lokacije zaradi spremembe v uporabniških profilih. Prav tako pa smo na ta način vsakemu uporabniku lahko še na kratko predstavili novosti, prednosti in morebitne spremembe glede na prejšnji sistem. Sprva smo načrtovali selitev izvesti avtomatsko, s pomočjo vnaprej napisanih skript, ampak se je po temeljitem premisleku izkazala izbrana možnost za boljšo. Med drugim tudi zaradi odkrivanja morebitnih napak in problemov, ki jih do tedaj še nismo opazili. Med selitvijo smo naleteli tudi na nekaj težav, ki pa niso bile bistvenega pomena: nekateri uporabniki so imeli iz neznanih razlogov napačno nastavljene pravice na nekaterih datotekah in mapah znotraj svojih uporabniških profilov, kar je bila posledica napačne nastavitve dedovanja pravic. To smo rešili s ponovno pravilno nastavitvijo pravic pri nekaterih uporabnikih; nekatere nastavitve namizja pri določenih uporabnikih na novem sistemu niso bile pravilno nastavljene, kar smo rešili s spremembo nekaterih postavk v skupinskih politikah.

4.2 Sprotno odpravljanje težav in napak pri prehodu na nov sistem

Pri tako obsežnem projektu je seveda normalno, da kdaj pa kdaj pride tudi do raznih težav in napak. Ker smo projekt izvajali po korakih, smo tudi morebitne nastale težave reševali sproti, kar je tudi opisano v vsakem posameznem poglavju, kjer so se morebitne težave pojavile. Še največ problemov nam je povzročala nadgradnja HP Thin Client terminalov zaradi velikega števila različnih verzij nameščenih operacijskih sistemov Windows CE. Kar nekaj časa pa smo se ukvarjali tudi s testiranjem delovanja aplikacij na 64-bitnem operacijskem sistemu Windows 2008 in z nadgrajevanjem oziroma iskanjem pravih, delujočih verzij aplikacij. Nekaj manjših težav smo imeli tudi s pravicami na datotekah in mapah nekaterih uporabnikov pri selitvi uporabniških profilov na novi sistem. Pri posameznih uporabnikih so bile pravice napačno nastavljene, kot posledica napačno nastavljenega dedovanja pravic na posameznih mapah. Ko smo ugotovili, kaj je vzrok za napačno nastavljene pravice, smo težavo tudi dokaj hitro odpravili. In sicer s ponovno pravilno nastavitvijo pravic in njihovega dedovanja na posameznih mapah znotraj profilov uporabnikov, ki so imeli težave.

4.3 Zaključek projekta z vprašalnikom za uporabnike

Pred začetkom projekta smo uporabnike povprašali za mnenje o trenutni rešitvi. Mednje smo razdelili vprašalnik, s pomočjo katerega so lahko pokomentirali delovanje sistema ter opisali svoje izkušnje in težave.

Večina uporabnikov je tak način dela (terminalske storitve) ocenila pozitivno, saj se z uporabo terminalskih storitev ni strinjalo le pet procentov uporabnikov. Prav tako je večina pozitivno ocenila splošno delovanje, odzivnost in stabilnost samega sistema, dobili pa smo precej kritik na nekaj specifičnih delov sistema, ki pa smo jih že vnaprej pričakovali. Največ kritik je letelo na stare 16-bitne DOS aplikacije, ki so na terminalskih strežnikih delovale bodisi počasi ali pa so pogosto zamrznile. Posledica tega je bila tudi nezmožnost tiskanja iz teh aplikacij, kar je uporabnikom, ki morajo vsakodnevno tiskati podatke, povzročalo precej preglavic. Druga stvar, ki je še precej motila uporabnike, je bilo nedelovanje redirekcije USB ključev, merilnih pripomočkov in ostalih zunanjih naprav, priklopljenih na odjemalce. Nekateri uporabniki pa so se pritoževali tudi nad dolgo prijavno in odjavno proceduro. Po krajšem testu smo ugotovili, da se to dogaja le pri uporabniki z velikimi uporabniškimi profili.

Po prehodu na novi sistem smo uporabnike ponovno vprašali za mnenje s pomočjo podobnega vprašalnika. Rezultati drugega vprašalnika so bili pričakovani. Vse napake prejšnjega sistema so bile s prehodom na novi sistem odpravljene, kar je bil tudi eden izmed ciljev prenove. Stare DOS aplikacije so večinoma ukinjene oziroma se nadomeščajo z novimi okenskimi ali spletnimi aplikacijami, ki na novih terminalskih strežnikih delujejo hitreje in brez težav. Ena izmed za uporabnike bistvenih novosti je tudi povsem transparenta redirekcija USB naprav iz odjemalca v uporabnikovo sejo na terminalskem strežniku. Težave z dolgimi prijavnimi in odjavnimi procedurami pa smo uspešno rešili z uporabo funkcionalnosti Folder redirection.

Da so uporabniki z novim sistemom zadovoljni, nam priča predvsem to, da smo na vprašalnikih dobili skoraj same pozitivne kritike. Navdušeni so bili predvsem nad tem, da je novi sistem odpravil najhujše, že prej omenjene težave. Mnenja so bila deljena edino glede novega (Windows7/Aero) uporabniškega vmesnika. Večina je nad njim sicer navdušena, nekateri pa so zaradi majhnih sprememb še malo zmedeni, ampak so zaradi prednosti, ki jih prinaša, vseeno podali pozitivno mnenje.

5. Sklepne ugotovitve

5.1 Prednosti in izboljšave na uporabniškem nivoju

Prednosti in izboljšave za uporabnike so poleg hitrejšega in bolj stabilnega delovanja, ki so posledica nadgradnje strojne opreme in namestitve najnovejšega Microsoftovega operacijskega sistema, večinoma vizualne narave. Windows Server 2008 R2 za Remote Desktop uporabnike namreč omogoča povsem isto uporabniško izkušnjo kot novi operacijski sistem Windows 7, kar vključuje vse prednosti in novosti, vključno z Aero vmesnikom. Prav tako je uporabnikom na voljo celoten uporabniški vmesnik, preveden v slovenski jezik. Poleg vizualnih pa je za uporabnike najbrž najbolj dobrodošla novost povsem transparentna redirekcija USB ključkov in ostalih lokalnih naprav na USB vodilu iz uporabniških terminalov v njihovo sejo na strežnikih.

5.2 Prednosti in izboljšave na administratorskem nivoju

Konkretnih prednosti in izboljšav na administratorskem nivoju je malo, saj je že prejšnji sistem administratorjem precej olajševal delo. Tako kot v Remote Desktop Services je bila tudi na prejšnjem sistemu omogočena enostavna distribucija programov, enostavna masovna nadgradnja tako strežnikov kot programov in lažja uporaba nestandardnih programov. Oba sistema prav tako omogočata precej manj administracije glede na število uporabnikov v primerjavi z uporabo navadnih računalnikov. Administracija uporabnikov, njihovih sej in aplikacij, ki jih uporabljajo, se namreč v obeh sistemih izvaja centralno, zgolj na terminalskih strežnikih. Konkretne novosti, ki jih prinašata Windows Server 2008 R2 in Remote Desktop Services, pa so predvsem veliko stabilnejše delovanje od prejšnjih operacijskih sistemov (Windows Server 2003), bolj dodelane skupinske politike in pa odlična integracija z ostalimi Microsoftovimi sistemi, kar pomeni tudi možnost enostavnega upravljanja s strežniki z osnovnimi managment konzolami, ki so že vgrajene v operacijski sistem Windows 7.

5.3 Slabosti oziroma pomanjkljivosti nove rešitve

Po nekajmesečni uporabi novega sistema smo opazili tudi nekaj pomanjkljivosti. Glavna med njimi je performančne narave. Na novem sistemu lahko na posameznem gostitelju oziroma terminalskem strežniku (RD Session Host) hkrati gostuje manjše število uporabnikov (15—20) kot na prejšnjem sistemu (25—30). Pri večanju številu uporabnikov gostitelj kmalu postane slabše odziven. Najverjetne je to posledica dveh dejavnikov: novejšega, kompleksnejšega operacijskega sistema in pa novejših, bolj strojno zahtevnih verzij samih nameščenih aplikacij. Zaključimo lahko, da za novi, sodobnejši sistem, z novejšimi aplikacijami, potrebujemo ali večje število gostiteljev oziroma terminalskih strežnikov v farmi ali pa zmogljivejšo strojno opremo.

Druga nadležna pomanjkljivost pa je v bistvu napaka v operacijskem sistemu. Ob uporabi roaming uporabniških profilov in funkcionalnosti Folder Redirection se uporabniku v primeru, ko mu poteče geslo za njegov uporabniški profil in ga ne spremeni v zahtevanem času, kreira nov profil. To se zgodi samo v primeru, ko nastavimo lokacijo profilov preko novih GPO pravil, zato smo zaenkrat za to funkcionalnost še vedno prisiljeni uporabljati stara GPO pravila. O napaki smo obvestili Microsoft, kjer so napako potrdili in nam zagotovili, da jo bodo v enem izmed naslednjih popravkov odpravili.

5.4 Zaključno mnenje

Izvedbo projekta, ki sem ga opisal v diplomskem delu, ocenjujem kot zelo uspešno. Kot prvo zato, ker smo se projekta z najnovejšo verzijo operacijskega sistema Windows 2008 R2 in njegove prenovljene funkcionalnosti Remote Desktop Services lotili takoj po izidu le-tega in smo zato tudi prvi v Sloveniji. Tako smo se lahko med potekom projekta zanašali le na Microsoftovo tehnično dokumentacijo, ki pa takoj po izidu še ni bila najbolj popolna, in pa na lastno znanje in izkušnje. Kot drugo pa zato, ker smo uspešno pripravili, namestili, skonfigurirali in vpeljali v produkcijsko omrežje podjetja rešitev, ki bo podjetju prinesla precej koristi. Glavna med njimi, in vedno zelo aktualna, je cena same rešitve, ki je precej nižja v primerjavi s produktom, ki je bil v uporabi prej. Nižji ceni pa sledijo še mnoge predvsem tehnične prednosti in izboljšave, tako za uporabnike kot tudi za administratorje, opisane v prejšnjih dveh poglavjih.

Poleg koristi, ki jih je projekt prinesel podjetju, pa sem imel ogromno koristi tudi sam. Pridobil oziroma poglobil sem znanja o strežniški in omrežni arhitekturi ter namestitvi, konfiguraciji in administraciji Microsoftovih strežniških operacijskih sistemov in njihovih funkcionalnosti, ki jih bom lahko s pridom uporabljal tudi v prihodnosti.

6. Priloge

Priloga1: Vprašalnik za uporabnike – Citrix

1. Se vam zdi ideja lahkih odjemalcev zanimiva in uporabna ali še vedno prisegate na poganjanje aplikacij iz lokalnega diska?

   - ☐ zelo mi je všeč, saj mi ni potrebno nameščati najnovejših različic programa in nastavljati raznih nastavitev, ker za to skrbi sistemski administrator na Citrix strežniku in sem lahko osredotočen izključno na funkcionalnost programa
   - ☐ delno mi je všeč, ampak še vedno imam raje lokalno nameščene aplikacije, da lahko sam nameščam nove različice in dodatke
   - ☐ sploh mi ni všeč

2. Ali vam ICA odjemalec pri povezavi na Citrix strežnik povzroča kakšne težave?

   - ☐ NE
   - ☐ DA, kratek opis problema:
     .....
     .....
     .....

3. Ali povezava na Citrix strežnik in prijava v sistem pri zagonu aplikacije traja ta predolgo?

   - ☐ ne opazim večje zakasnitve
   - ☐ prijava in zagon trajata nekoliko dlje, kot če bi aplikacijo izvajal iz lokalnega diska
   - ☐ celotna procedura je zelo dolgotrajna in moteča

4. Vas pri sistemu Citrix kaj moti?

   - ☐ NE
   - ☐ DA, predolg čas prijave v sistem
   - ☐ DA, počasnejše delovanje aplikacij
   - ☐ DA, drugo:
     .....
     .....
     .....

5. Ali vas dejstvo, da se lahko nadrejeni priključi v vašo ICA sejo in vas opazuje pri delu, medtem ko vi sploh ne veste, da se to dogaja, moti?

   - ☐ DA, to me zelo moti

- ☐ NE, saj lahko nadzoruje le programe, ki jih izvajam na Citrix strežniku, ti pa so službene narave, mojih osebnih stvari (npr. E-mail ...) pa ne more pregledovati, ker jih izvajam lokalno

6. Kakšna je vaša ocena dela preko Citrix sistema?

   - ☐ zelo primeren
   - ☐ primeren
   - ☐ zadovoljiv
   - ☐ sistem se mi zdi neprimeren, ker:
     .....
     .....
     .....

Priloga 2: Vprašalnik za uporabnike – RDS

1. Se vam zdi ideja lahkih odjemalcev zanimiva in uporabna ali še vedno prisegate na poganjanje aplikacij iz lokalnega diska?

   - ☐ zelo mi je všeč, saj mi ni potrebno nameščati najnovejših različic programa in nastavljati raznih nastavitev, ker za to skrbi sistemski administrator na Citrix strežniku in sem lahko osredotočen izključno na funkcionalnost programa
   - ☐ delno mi je všeč, ampak še vedno imam raje lokalno nameščene aplikacije, da lahko sam nameščam nove različice in dodatke
   - ☐ sploh mi ni všeč

2. Ali vam povezava na nove terminalske strežnike povzroča kakršnekoli težave?

   - ☐ NE
   - ☐ DA, kratek opis problema:
     .....
     .....
     .....

3. Ali povezava na terminalski strežnik in prijava v sistem pri zagonu aplikacije trajata predolgo?

   - ☐ povezava in prijava sta hitrejši kot na prejšnjem sistemu
   - ☐ prijava in zagon trajata nekoliko dlje kot na prejšnjem sistemu
   - ☐ celotna procedura je zelo dolgotrajna in moteča

4. Vas pri sistemu Remote Desktop Services kaj moti?

   - ☐ NE
   - ☐ DA, predolg čas prijave v sistem

- ☐ DA, počasnejše delovanje aplikacij
- ☐ DA, drugo:

  .....
  .....
  .....

5. Kakšna je vaša ocena dela preko novega Remote Desktop Services sistema v primerjavi s prejšnjim sistemom Citrix?

   - ☐ prejšnji sistem je bil boljši, ker:

     .....
     .....
     .....
   - ☐ novi sistem je boljši, ker:

     .....
     .....
     .....

7. Viri

[1] Charlie Russel, Craig Zacker, Introducing Windows Server 2008 R2, Redmond: Microsoft Press, 2009

[2] Steve Seguis, Microsoft Windows Server 2008 Administration, New York: McGraw Hill, 2008

[3] Microsoft Corporation, Locking Down Windows Server 2003 Terminal server Sessions, julij 2003

[4] (2009) Citrix Delivery Center. Dostopno na: http://www.citrix.com/English/ps2/products/product.asp?contentID=683711&ntref=prod_top

[5] (2009) Microsoft Windows Server 2008 R2. Dostopno na: http://www.microsoft.com/windowsserver2008/en/us/default.aspx

[6] (2009) Microsoft Remote Desktop Services. Dostopno na: http://www.microsoft.com/windowsserver2008/en/us/rds-product-home.aspx

[7] (2009) Microsoft TechNet – Windows Server 2008 and Windows Server 2008 R2. Dostopno na: http://technet.microsoft.com/en-us/windowsserver/2008/default.aspx

[8] (2009) Microsoft TechNet – Terminal Services. Dostopno na: http://technet.microsoft.com/en-us/windowsserver/terminal-services/default.aspx

[9] (2009) Remote Desktop Services (Terminal Services) Team Blog. Dostopno na: http://blogs.msdn.com/rds/default.aspx