Opinnäytetyö (AMK)

Tietotekniikka

Sulautetut järjestelmät

2010

Sami Kinnunen

ETÄTYÖYMPÄRISTÖN ASENNUS JA KONFIGUROINTI

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietotekniikka | Sulautetut järjestelmät

25.2.2010 | 34

Ohjaaja: Tiina Ferm

Sami Kinnunen

ETÄTYÖYMPÄRISTÖN ASENNUS JA KONFIGUROINTI

Yritysten kiinnostus työntekijöiden etätyöskentelyyn on lisääntynyt jatkuvasti. Kansainvälistyminen on aiheuttanut sen, että töitä on usein tärkeää saada tehtyä myös matkojen aikana. Microsoft on mahdollistanut tämän jo Windows NT 4.0 Server -palvelinversiostaan lähtien, mutta uudempien versioiden myötä etäpalvelujen käytöstä on tullut käyttäjäystävällisempää.

Tämä opinnäytetyö käsittelee Microsoft Windows Server -palvelinkäyttöjärjestelmiensä mukana toimittaman etätyöpöytäpalvelun (ent. etäpäätepalvelu) asennusta ja konfigurointia. Palvelu luotiin yrityksen Nova Solutions Oy:n ylläpito-osaston testiympäristöön testaus- ja kehitystyötä varten.

Testiympäristö on luotu virtuaalipalvelimilla, jolloin lisäpalvelimien asentaminen ympäristöön on helppoa ja nopeaa. Tässä projektissa etätyöpöytäpalvelu asennetaan yhdelle virtuaalipalvelimelle. Palvelimia lisätään myöhemmin, mikäli tarvetta esiintyy. Palvelusta otetaan käyttöön etätyöpöydän yhdyskäytävä, web-liittymä sekä etäohjelmat.

Etäjärjestelmän asennus sujui odotetusti eikä yllätyksiä ilmennyt. Konfigurointi onnistui Microsoftin TechNet -sivuston ohjeiden avulla myös ilman ongelmia. Microsoft on lisännyt uusimpaan etätyöpöytäpalveluunsa odotettuja ja toimivia uudistuksia. Yksi onnistuneimmista uusista ominaisuuksista on mahdollisuus rajata Web-liittymän näkymästä ohjelmia käyttäjäryhmäkohtaisesti.

Microsoftin etätyöpöytäpalvelu osoittautui Nova Solutions Oy:n ylläpito-osaston tarpeisiin erinomaistsi soveltuvaksi palveluksi.

ASIASANAT:

Palvelimet, tietojärjestelmät, atk-järjestelmät, käyttöjärjestelmät, Windows, etätyö, Microsoft

BACHELOR´S THESIS | ABSTRACT

UNIVERSITY OF APPLIED SCIENCES

Information Technology | Embedded Systems

25.2.2010 | 34

Lecturer: Tiina Ferm

Sami Kinnunen

INSTALLATION AND CONFIGURATION OF REMOTE WORK ENVIRONMENT

In today's business world companies are more and more interested in possibilities for its employees to work remotely. Globalization has caused a need to be able to work outside the office. Microsoft has provided such possibilities already by its early Windows NT 4.0 Server versions. Microsoft has however significantly improved their product to be more user friendly.

This thesis discusses the installation and configuration of Windows Server 2008 R2 –server operating systems Remote Desktop Services (before Terminal Services). This was installed as a testing and development environment for Nova Solution Oy Service & Support –department.

Test environment was created in virtual servers, which allows an easy and fast way to increase servers. In this project Remote Desktop Services was installed in one virtualserver. Servers will be added later on if needed. Remote Desktop Gateway, Remote Desktop Web Access and Remote Desktop RemoteApp –roles will also be installed.

Installation of Remote environment completed as expected without problems. Configuration was also succesful with the help of Microsoft TechNet –websites guides.

Microsoft has added expected new features for its latest version of Remote Desktop Services. One of the most successful new features is the possibility to choose which remote programs are visible to which user on WebAccess –site. Remote Desktop Services proved to be an excellent product for the needs of Nova Solutions Oy's Service & Support department.

KEYWORDS:

Servers, information systems, IT-systems, operating systems, Windows, remote work, Microsoft

SISÄLTÖ

Lyhenteet

AD	Aktiivihakemisto (Active Directory)
RDS	Etätyöpöytäpalvelut (Remote Desktop Services)
RD	Etätyöpöytä (Remote Desktop)
CAL	Käyttöoikeuslisenssi (Client Access License)
RDP	Etätyöpöytäprotokolla (Remote Desktop Protocol)
SSL	Secure Sockets Layer
RD CAP	Etätyöpöytäyhteyden auktorisointikäytäntö (Remote Desktop Connection Authorization Policy)
RD RAP	Etätyöpöytäresurssein auktorisointikäytäntö (Remote Desktop Resource Authorization Policy)
RD Session Host	Etätyöpöytäistunnon isäntä (Remote Desktop Session Host)
RD Connection Broker	Etätyöpöytäyhteyden välittäjä (Remote Desktop Connection Broker)
RD Licensing	Etätyöpöydän lisensointi (Remote Desktop Licensing)
RD Gateway	Etätyöpöydän yhdyskäytävä (Remote Desktop Gateway)
RD Web Access	Etätyöpöydän web-liittymä (Remote Desktop Web Access)
RDS Manager	Etätyöpöytäpalvelun hallintatyökalu (Remote Desktop Services Manager)
RemoteApp	Etäohjelma (Remote Application)

1 Johdanto

Yritysten kiinnostus etätyöskentelymahdollisuuksiin on jatkuvasti kasvanut. Etätyöskentely tuo joustavuutta työntekoon sekä työntekijän että työnantajan näkökulmasta (Pekkola & Uskelin 2007, 13). Etätyöskentely-ympäristön rakentamiseen on useampia eri valmistajien tarjoamia ratkaisuja. Yksi pitkäaikaisista etätyöskentely-ympäristöjen toimittajista on Citrix (www.citrix.com). Viime aikoina Microsoft (www.microsoft.com) on kuitenkin lisännyt osuuttaan tällä saralla.

Etätyöpöytäpalvelut on palvelu, jolla Microsoft tarjoaa etätyöskentelymahdollisuudet. Etätyöpöytäpalvelu on ollut osa Microsoftin palvelinkäyttöjärjestelmiä jo Windows NT:n ajoilta 1980-luvulta asti nimellä Terminal Services (Tulloch M. 2006). Windows Server 2008 -palvelinkäyttöjärjestelmä toi kuitenkin mukanaan useita toivottuja ominaisuuksia ja parannuksia.

Etätyöpöytäpalvelun tärkeys ja hyöty kasvavat nykymaailmassa päivä päivältä. Globalisaatio ja kansainvälisyys nostaa yritysten työntekijöiden tarvetta päästä yrityksen tietojärjestelmään toimipisteen ulkopuolelta.

Tässä dokumentissa käydään läpi Microsoft Windows Server 2008 R2:n etätyöpöytäpalvelun asennus ja konfigurointi eli asetusten määritys.

Etätyöpöytäpalvelun uudesta versiosta ei vielä ole painettua materiaalia saatavilla. Kirjallisen materiaalin puute osaltaan hankaloitti tiedon saantia. Kirjallisen materiaalin puutteen vuoksi lähteenä käytettiin suurimmalta osin Microsoftin TechNet -portaalia, joka sisältää runsaasti tietoa etätyöpöytäpalvelusta.

2 Etätyöpöytäpalvelut

Microsoft julkaisi ensimmäisen version etäpäätepalvelusta käyttöjärjestelmässään Windows NT 4.0 (Tulloch M. 2006). Palvelua kehitettiin Windows 2000 ja Windows Server 2003 -käyttöjärjestelmäversioissa.

Palvelua ja palvelun käyttämää protokollaa kehitettiin Windows Server 2008 ja Windows Vista -käyttöjärjestelmissä. Windows Server 2008 R2 –palvelin-käyttöjärjestelmäversion myötä etäpäätepalvelun nimi muutettiin etätyöpöytäpalveluksi (Russel & Zacker 2010, 47).

Windows -käyttöjärjestelmä sisältää kaksi asiakasohjelmaa, jotka käyttävät etätyöpöytäpalvelua: Etätuki (Remote Assistance) on käytettävissä kaikissa Windows XP tai uudemmissa Windows -käyttöjärjestelmissä. Etätyöpöytäyhteys (Remote Desktop Connection) on käytettävissä osassa Microsoftin käyttöjärjestelmiä, jotka ovat Windows NT Terminal Server ja uudemmat palvelinkäyttöjärjestelmät, Windows XP Professional, Windows Vista Business, Enterprise ja Ultimate sekä Windows 7 Professional, Enterprise ja Ultimate. Windows XP, Vista ja 7 -versioissa etätyöpöytäyhteys tukee vain yhden käyttäjän kirjautumista tietokoneelle kerrallaan.

2.1 Etätyöpöytäpalvelun rakenne

Etätyöpöytäpalvelun palvelinkomponentti on etätyöpöytäistunnon isäntä. Tämä palvelinkomponenti kuuntelee TCP-porttia 3389.

Etätyöpöytäpalvelu koostuu seuraavista palvelinrooleista (Microsoft TechNet 2009):

- etätyöpöytäistunnon isäntä
- etätyöpöydän lisensointi
- etätyöpöydän yhdyskäytävä
- etätyöpöytäyhteyden välittäjä
- etätyöpöydän web-liittymä

Edellämainittuja rooleja hallitaan seuraavilla hallintatyökaluilla:

- etätypöytäpalvelun hallintatyökalu
- etätyöpöytäistunnon isännän konfigurointityökalu
- etätyöpöydän yhdyskäytävän hallintatyökalu

- etätyöpöydän lisenssien hallintatyökalu
- etäohjelman hallintatyökalu

Etätyöpöytäistunnon isäntä

Etätyöpöytäistunnon isäntä on etätyöpöytäpalvelun palvelinrooli. Etätyöpöytäistunnon isännän avulla Windows Server 2008 R2 -pohjainen palvelin voi tarjota Windows -ohjelmia tai täyden etätyöpöytäyhteyden. Käyttäjät voivat omilta tietokoneiltaan ajaa etätyöpöytäpalvelimen tarjoamia ohjelmia ja verkkopalveluja kuten esimerkiksi tulostuspalveluja.

Etätyöpöydän lisensointipalvelin

Etätyöpöydän lisensointipalvelin hallitsee etätyöpöytäpalvelun käyttöoikeuslisenssejä (Microsoft TechNet 2009). Lisenssejä on kahdenlaisia: käyttäjälisenssejä (User Client Access License) ja laitelisenssejä (Device Client Access License). Käyttäjälisenssimallissa jokaisella käyttäjällä täytyy olla oma käyttäjälisenssinsä. Laitelisenssimallissa taas jokaisella laitteella on oma lisenssinsä riippumatta siitä, kuinka monta käyttäjää kyseistä laitetta käyttää. (Microsoft TechNet 2009). Käyttäjälisenssimalli on yleisimmin käytetty lisensointimalli. Laitelisenssimallin käyttäminen on järkevää, mikäli yrityksessä on vähän tietokoneita mutta paljon käyttäjiä, eikä käyttäjillä ole ns. henkilökohtaisia tietokoneita. Tällaisessa skenaariossa laitelisenssimalli tulee huomattavasti edullisemmaksi kuin käyttäjälisenssimalli. Esimerkiksi kirjastoissa asiakkaiden käytössä olevissa tietokoneissa on järkevää käyttää laitelisenssimallia, koska tietokoneilla on useita käyttäjiä, eikä jokaiselle käyttäjälle ole järkevää tai edes mahdollista hankkia käyttäjälisenssiä.

Kun käyttäjä ottaa yhteyttä etäpalvelimeen, selvittää palvelin etätyöpöydän käyttöoikeuslisenssin tarpeellisuuden. Etätyöpöytäistunnon isäntä pyytää tarvittaessa lisenssiä Etätyöpöydän lisensointipalvelimelta asiakkaan puolesta. Mikäli sopiva lisenssi on käytettävissä, myönnetään lisenssi yhteyttä ottavalle käyttäjälle, minkä jälkeen käyttäjä saa yhteyden etäpalvelimeen.

Etätyöpöydän yhdyskäytävä

Etätyöpöydän yhdyskäytävä mahdollistaa yrityksen sisäisen verkon palvelujen käyttämisen etäkäyttäjille mistä tahansa Internetiin yhteydessä olevasta laitteesta, joka pystyy käyttämään etätyöpöytäyhteysohjelmaa (Microsoft TechNet 2009). Nämä

verkkopalvelut voivat olla etäpalvelimia, etäohjelmia tai työasemia, joissa etätyöpöytä on otettu käyttöön.

Etätyöpöydän yhdyskäytävä käyttää RDP-over-HTTPS:ää salatun ja turvatun yhteyden luomiseen etäkäyttäjien ja yrityksen sisäisen verkon palvelujen välille (Microsoft TechNet 2009). Yhdyskäytävän avulla käyttäjien ei tarvitse käyttää VPN-ohjelmaa yhteyden turvaamiseksi. Tämän ansiosta yrityksen verkon palvelujen käyttäminen on etäkäyttäjälle yksinkertaisempaa.

Etätyöpöydän yhdyskäytävän hallintatyökalun avulla yhdyskäytävälle voi asettaa käytäntöjä, joissa on määritelty käyttäjät tai käyttäjäryhmät, joilla on oikeus käyttää kyseessä olevia palveluja. Lisäksi voidaan määritellä ne resurssit, joita etäkäyttäjät saavat käyttää. Muita määrityksiä ovat muun muassa laitteiden uudelleenreitityksen salliminen tai kieltäminen sekä käytettävät tunnistautumismenetelmät, kuten salasanan, älykortin tai molempien käyttäminen.

Etätyöpöytäistunnon välittäjä

Usein etäpalvelimia on useampia palvelimien kuormituksen tasaamiseksi. Varsinkin isommissa ympäristöissä on tarpeellista käyttää useampaa etäpalvelinta, jotta yhden palvelimen kuorma ei kasvaisi liian korkeaksi. Etäpalvelimen liian korkea kuormitus saattaa heikentää oleellisesti etäpalvelun tasoa tai jopa katkaista palvelun kokonaan.

Useamman etäpalvelimen ryhmässä eli etäpalvelinfarmissa etätyöpöytäistunnon välittäjä vastaa siinä olevien etäpalvelimien tasaisesta kuormituksesta. Kun etäkäyttäjä ottaa yhteyttä etäpalveluihin, etätyöpöytäistunnon välittäjä käy tarkistamassa palvelimien kuormituksen ja ohjaa käyttäjän etäpalvelupyynnöt vähimmällä kuormalla olevaan etäpalvelimeen.

Etätyöpöydän web-littymä

Tällä palvelulla tarjotaan etäkäyttäjille etäohjelmistoja ajettavaksi joko selaimen kautta tai omina etäohjelminaan (Microsoft TechNet 2009).

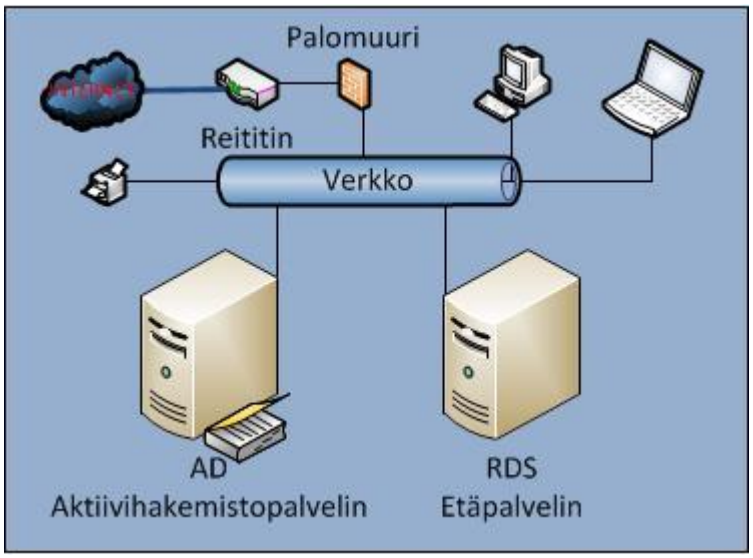
2.2 Tyypillinen etäympäristö

Suuri osa yrityksistä Suomessa ovat pieniä tai keskisuuria. Varsinkaan pienillä yrityksillä ei ole resursseja tai tarvetta rakentaa kovinkaan suuria palvelinjärjestelmiä. Tästä syystä valtaosassa pienten yritysten etäjärjestelmissä käytetään yhtä tai kahta

palvelinta. Yhden palvelimen järjestelmässä kaikki yrityksen palvelut ovat yhdessä palvelimessa. Tällä tavalla yritys saa pienellä investoinnilla paljon palveluja käyttöönsä.

Kahden palvelimen ympäristössä palvelimien roolit on jaettu niin, että yhdessä palvelimessa on yrityksen tärkeimmät palvelut eli aktiivihakemistopalvelu, käyttäjätietokanta ja tiedostojenjakopalvelu. Toisen palvelimen rooli on toimi etäpalvelimena, joka mahdollistaa yrityksen resursseja käytettäväksi verkkoon. Kuvan 1 mukaisessa pienyrityksen tyypillisessä IT-infrastruktuurissa AD-palvelin sisältää yrityksen tärkeimmät palvelut. Sen tehtävänä on toimia yrityksen käyttäjätilien hallintapalvelimena sekä tarjota työasemille käytettäväksi keskitetty paikka tiedostojen tallennukselle. RDS-palvelimen tehtävä on tarjota AD-palvelimen palveluja etäkäyttäjille verkon yli.

Kuva 1: tyypillinen pienyrityksen IT-infrastruktuuri



Hieman isommissa yrityksissä usein on käytettävissä useampi palvelin, jolloin palvelinten rooleja voidaan jakaa. Tällä tavoin saadaan yhteen palvelimeen koostuvaa kuormaa jaettua useammalle palvelimelle, joka tehostaa verkon toimintaa. Parhaimmassa tapauksessa kaikki roolit on mahdollista jakaa useammalle palvelimelle, mutta tällaista ympäristöä käytetään yleensä vain suurissa yrityksissä, joissa on ensisijaisen tärkeää eliminoida verkon pullonkaulat.

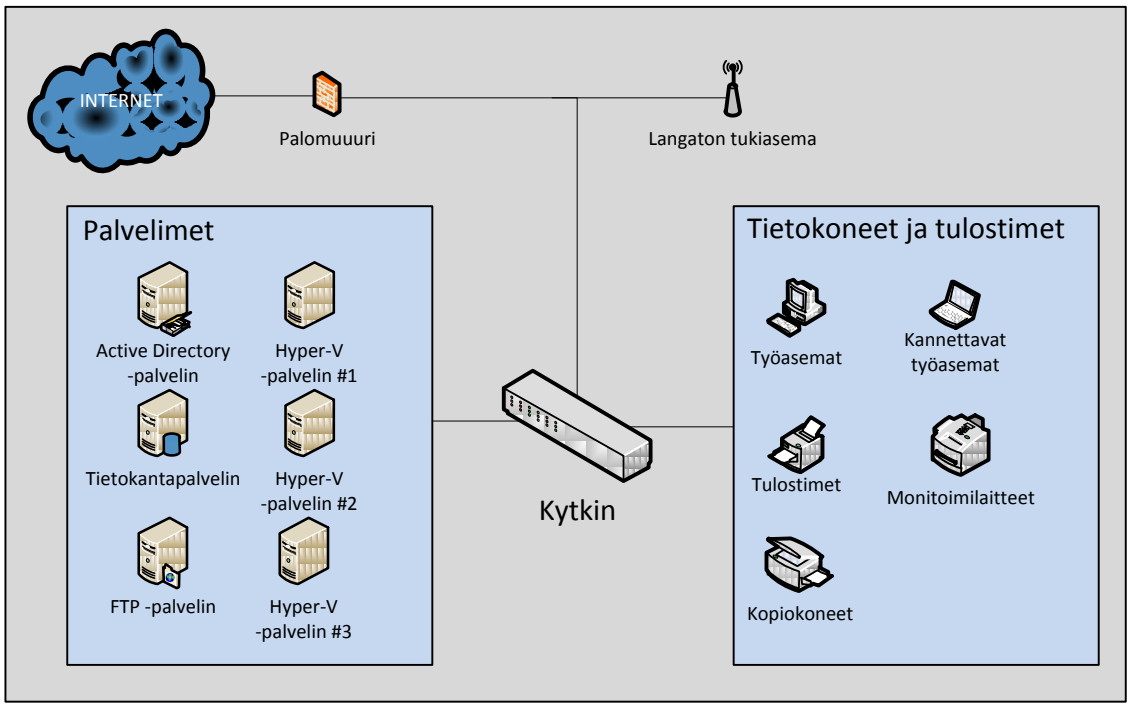
Tässä dokumentissa kuvataan ensin etätyöpöytäpalvelun asennus. Sen jälkeen käydään läpi etätyöpöytäpalvelun tärkeimmät asetukset, jotta etätyöpöytäpalvelu olisi käytettävissä.

3 Suunnitelma

Projektissa rakennetaan etäkäyttöympäristö yrityksen Nova Solutions Oy:n ylläpito-osaston testiympäristöön. Testiympäristöön rakennettua etäjärjestelmää tullaan käyttämään uusien etäkäyttöominaisuuksien testaamiseen ennen ko. ominaisuuksien käyttöönottamista Nova Solutions Oy:n tuotantojärjestelmässä.

Testiympäristö on luotu virtuaalipalvelimilla, jolloin uusien palvelimien lisääminen jälkeenpäin on helppoa ja nopeaa. Olemassa olevaan verkkoinfrastruktuuriin, joka on kuvattu kuvassa 2 luodaan uusi virtuaalipalvelin Hyper-V -palvelin #2:een. Palvelimen käyttöjärjestelmänä käytetään Microsoft Windows Server 2008 Standard R2:a, joka mahdollistaa Microsoftin uusimman etätyöpöytäpalvelun käytön.

Kuva 2: Nova Solutions Oy verkkoinfrastruktuuri



Hyper-V -palvelin #2:n käyttöjärjestelmänä on Microsoft Hyper-V Server 2008, joka on itsenäinen virtuaalikoneita varten räätälöity käyttöjärjestelmä. Microsoft Hyper-V Server on vapaasti ladattavissa Microsoftin kotisivuilta.

Hyper-V Server 2008:aan asennetaan Microsoft Windows Server 2008 Standard R2, joka liitetään yrityksen toimialueeseen. Palvelimeen asennetaan tämän jälkeen etätyöpöytäpalvelu ja siitä konfiguroidaan käyttöön perusominaisuudet: Etätyöpöydän

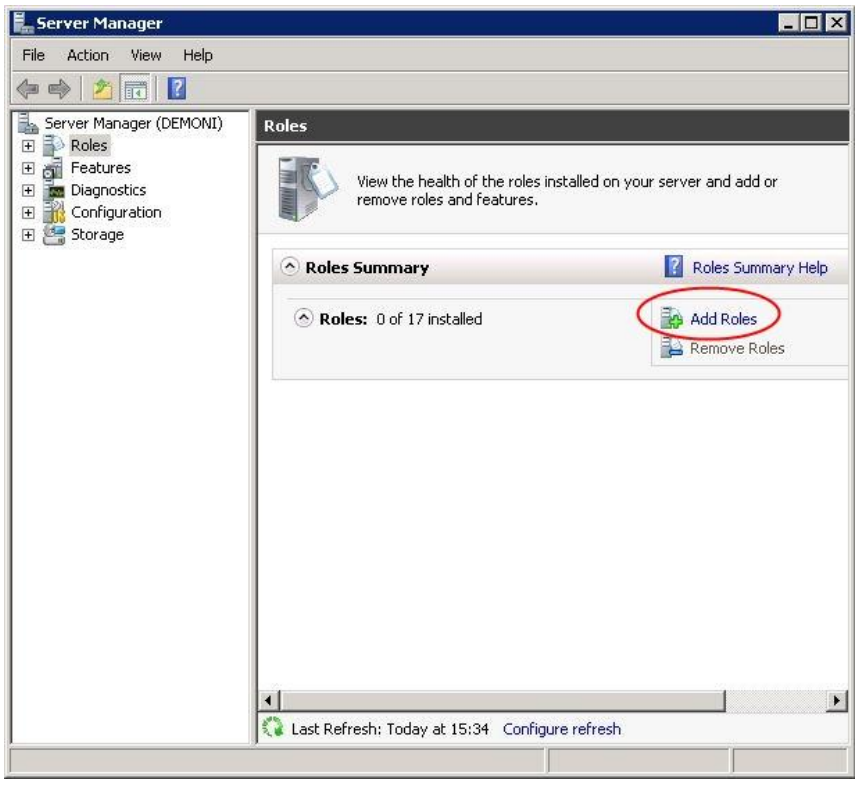
istunnon isäntä, yhdyskäytävä sekä palvelun web-liittymä. Etätyöpöydän istunnon välittäjä -palvelu jätetään tässä vaiheessa ottamatta käyttöön. Sen käyttämiseksi täytyy luoda lisää palvelimia. Kyseisellä ominaisuudella ei ole testiympäristössä tällä hetkellä tarvetta.

4 Etätyöpöytäpalvelun asennus

Etätyöpöytäpalvelun komponentit ovat valmiina Windows Server 2008 R2:ssa. Palvelut täytyy ottaa ensimmäisellä kerralla käyttöön. Tässä kappaleessa käydään läpi palvelujen asennus. Myöhemmässä vaiheessa käydään läpi myös kyseisten palvelujen asetusten määrittäminen.

Etätyöpöytäpalvelu (tai "rooli", eng. Role) voidaan asentaa palvelimen hallintatyökalulla (kuva 3). Roolin asennus aloitetaan valitsemalla *Add Role*. Palvelimen hallintatyökalulla voidaan myös poistaa palvelimeen asennettuja rooleja valitsemalla *Remove Roles*.

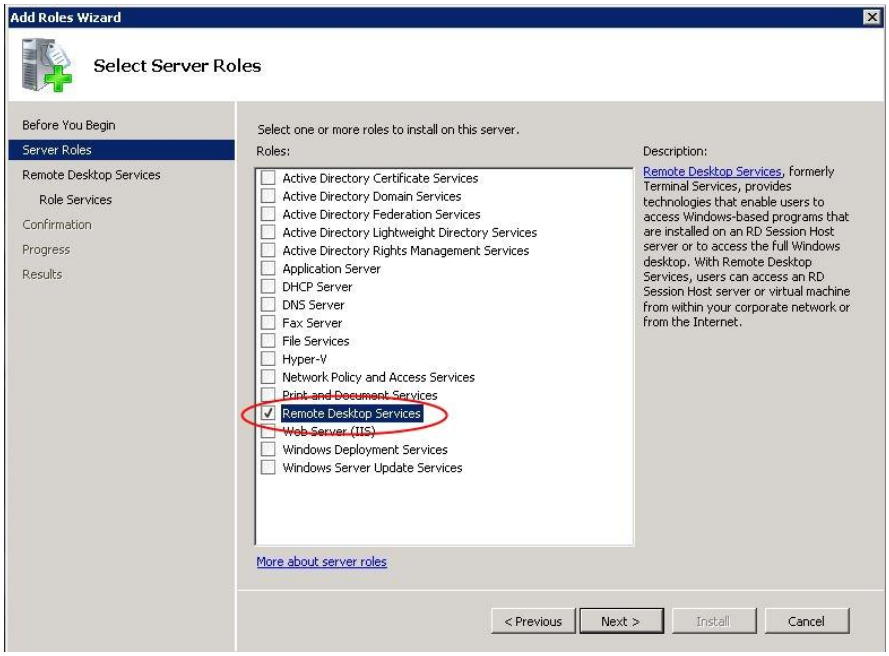
Kuva 3: Roolin asennus Server Manager -ohjelmassa



Tietoturvasyistä ennen palvelinroolien asentamista on syytä varmistaa, että järjestelmänvalvojatilin salasana on turvallinen ja täytää yrityksen sille määrittämät edellytykset. Myös palvelimen verkkoasetusten täytyy olla määritettynä oikein, mm. kiinteä IP-osoite palvelimella pitää olla käytössä.

Etätyöpöytäpalvelu valitaan palvelinroolien listauksesta (kuva 4). Palvelimelle asennettavia rooleja on kaiken kaikkiaan 17 kappaletta. Tässä tapauksessa halutaan asentaa nimenomaan etätyöpöytäpalvelu.

Kuva 4: Palvelinroolit



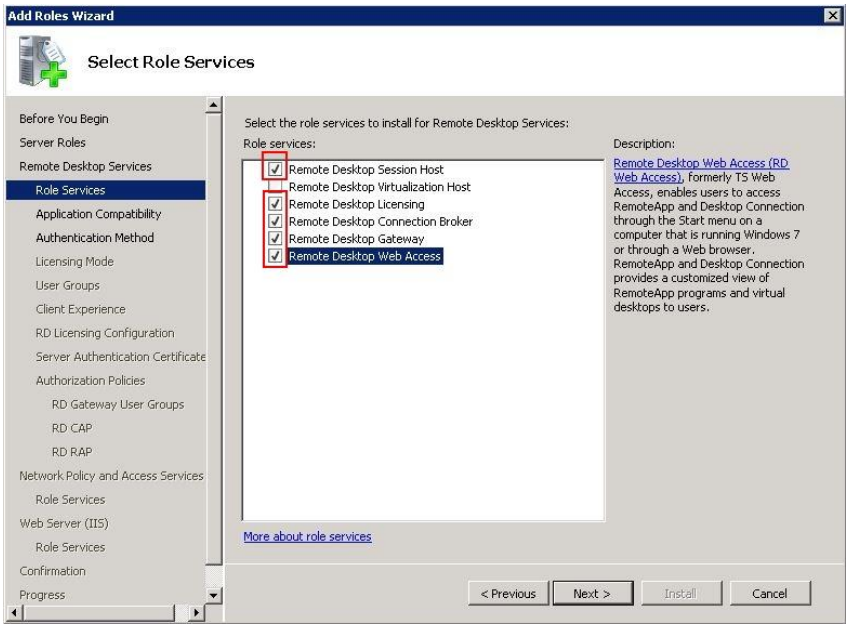
Osa etätyöpöytäpalvelun toiminnoista tarvitsee myös rooleja Network Policy and Access Services (NPAS) sekä Web Server (IIS), mutta palvelin lisää nämä roolit etätyöpöytäpalvelun asennuksen aikana mikäli näin halutaan (kuvat 5 ja 6).

Kuva 5: RD Gatewayn lisäksi tarvitsemat roolit

Kuva 6: RD Web Accessin tarvitsemat roolit.

Seuraavaksi valitaan käytettävät etätyöpöytäpalvelun komponentit (kuva 7).

Kuva 7: RDS -palvelun komponentit



Komponenteista valitaan kyseisessä tapauksessa etätyöpöydän virtualisointi-isäntää (Remote Desktop Virtualization Host) lukuun ottamatta kaikki. Etätyöpöydän virtualisointi-isäntä -komponenttia ei tarvita tässä tapauksessa, minkä vuoksi se jätetään asentamatta.

Etätyöpöydän virtualisointi-isäntä on Windows Server 2008 R2:n mukana tullut uusi ominaisuus, jolla etätyöpöytäpalveluun kirjautuva käyttäjä voidaan ohjata käyttämään haluttua virtuaalitietokonetta. Virtualisointi-isäntä toimii yhdessä Hyper-V -palvelun kanssa. Hyper-V on palvelu, jolla palvelimeen voidaan asentaa virtuaalisia tietokoneita ja työasemia. Mikäli virtualisointi-isäntä halutaan asentaa, ehdottaa palvelin

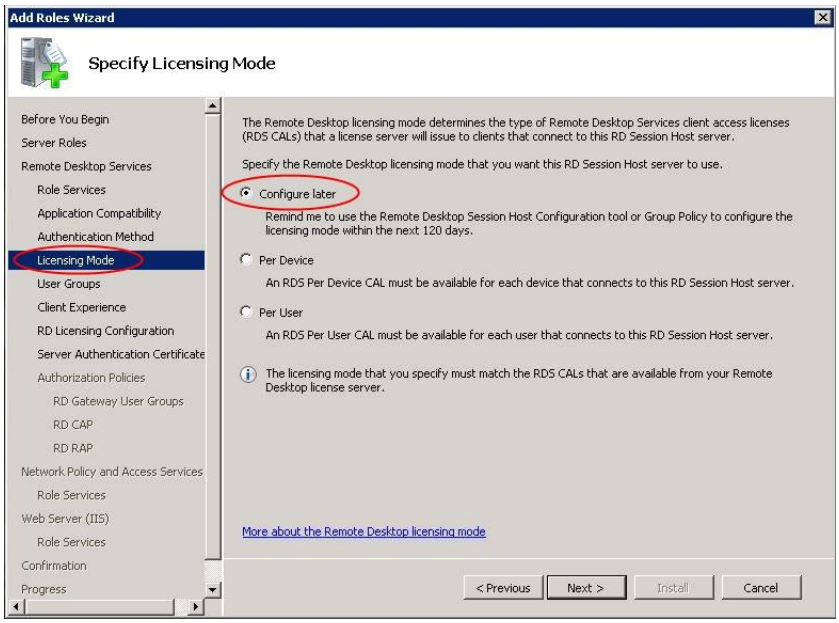
asennettavaksi myös tarvittavan Hyper-V -palvelun ja haluttaessa myös asentaa sen tässä vaiheessa.

Etätyöpöytäistunnon isäntä on suositeltavaa asentaa ennen kuin etäpalvelimelle asennetaan käyttäjille käytettäväksi haluttavia sovelluksia. Mikäli etätyöpöytäpalvelimelle on jo asennettu sovelluksia ennen etätyöpöytäistunnon isäntäpalvelun asentamista, niin kyseiset sovellukset voidaan joutua asentamaan uudelleen.

Etätyöpöytäpalvelin voidaan määrittää vaatimaan verkkotason todennusta (Network Level Authentication, NLA). Verkkotason todennus on uusi käyttäjän todennustapa, joka tuli ensimmäisen kerran käyttöön Windows Server 2008 kanssa. NLA on vanhaa todennustapaa tietoturvallisempi käytäntö, jonka käyttäminen on tioteturvasyistä suositeltavaa, mikäli sen käyttäminen on mahdollista. NLA:n käyttäminen vaatii Windows -käyttöjärjestelmän ja etätyöpöytäyhteysohjelman, jotka tukevat NLA:ta. Palvelimen täytyy olla vähintään Microsoft Windows Server 2008 tai uudempi, jotta NLA voidaan ottaa palvelimessa käyttöön. Työaseman käyttöjärjestelmänä täytyy olla Windows XP Service Pack 3 tai uudempi. (Microsoft TechNet 2009).

Etätyöpöytäpalvelu käyttää joko käyttäjäkohtaisia tai laitekohtaisia lisenssejä. Asennuksen tässä vaiheessa voidaan jo valmiiksi määritellä palvelimen etätyöpöydän lisensointimalli, mikäli se on jo tiedossa (kuva 8).

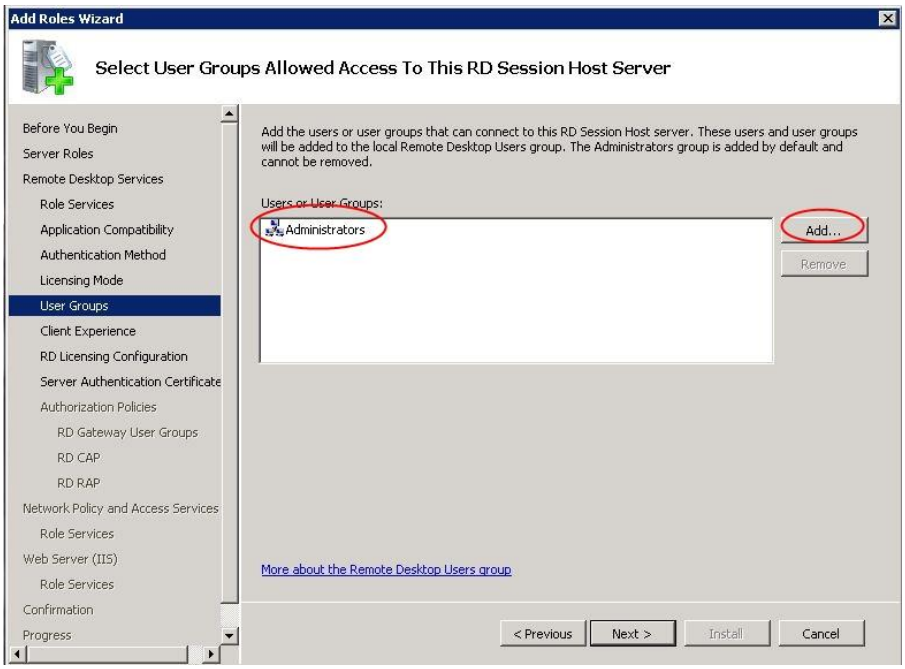
Kuva 8: RDS -palvelun lisensointimallit



Lisensointimalli valitaan myöhemmässä vaiheessa etätyöpöytäpalvelun asetusten määrittämisessä.

Etätyöpöytäpalvelulle täytyy kertoa, mitkä käyttäjäryhmät tai käyttäjät saavat ottaa yhteyttä kyseiseen etäpalvelimeen (kuva 9).

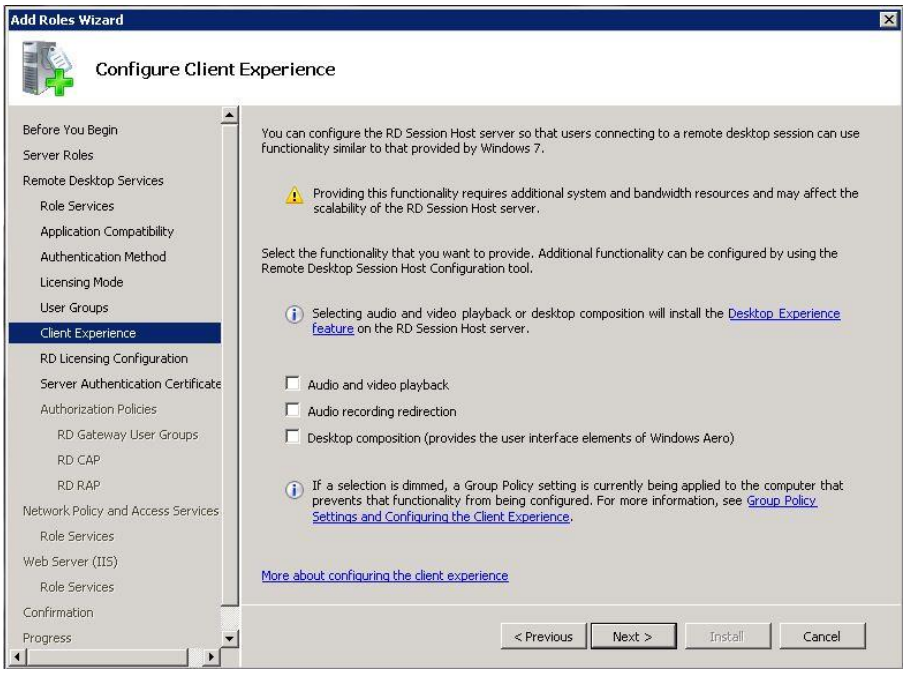
Kuva 9: Etäpalvelimen käyttöoikeus



Hyväksi todettu tapa on määrittää käyttöoikeus mieluummin käyttäjäryhmille kuin suoraan käyttäjille. Palvelimen ja palvelun ylläpitäminen on tällöin huomattavasti yksinkertaisempaa.

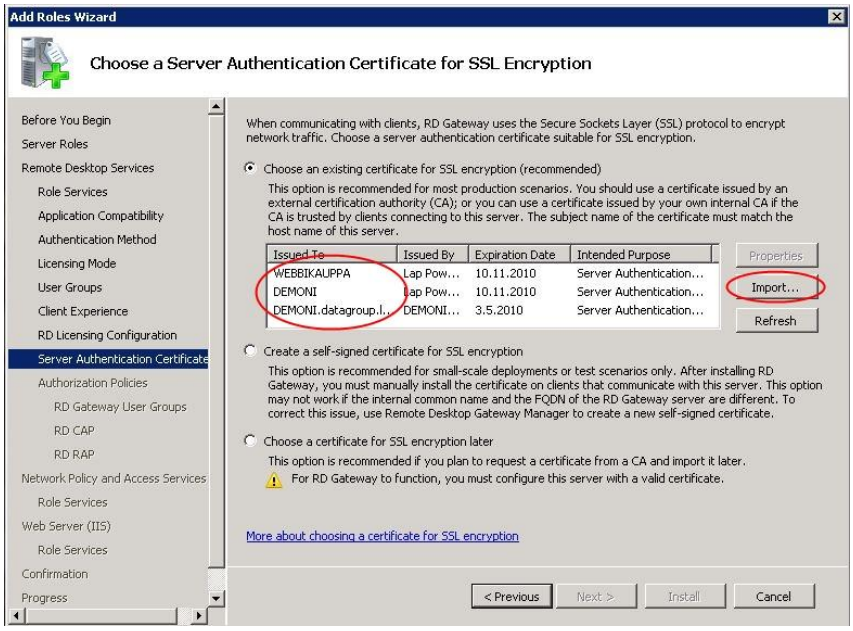
Windows Server 2008 R2 -version mukana on tullut uusi toiminto Client Experience, jossa voidaan etätyöpöytäyhteyteen ohjata myös äänitoimintoja sekä Windows Vistassa että Windows 7:ssä tutuksi tullut Windows Aeron graafisia ominaisuuksia (kuva 10).

Kuva 10: Client Experience



Etätyöpöydän yhdyskäytävä käyttää SSL -protokollaa liikenteen salaamiseksi. Jotta tämä toimisi täytyy etätyöpöytäpalvelulle määrittää, mitä SSL-varmennetta käytetään (kuva 11).

Kuva 11: Varmenne SSL-suojaukseen

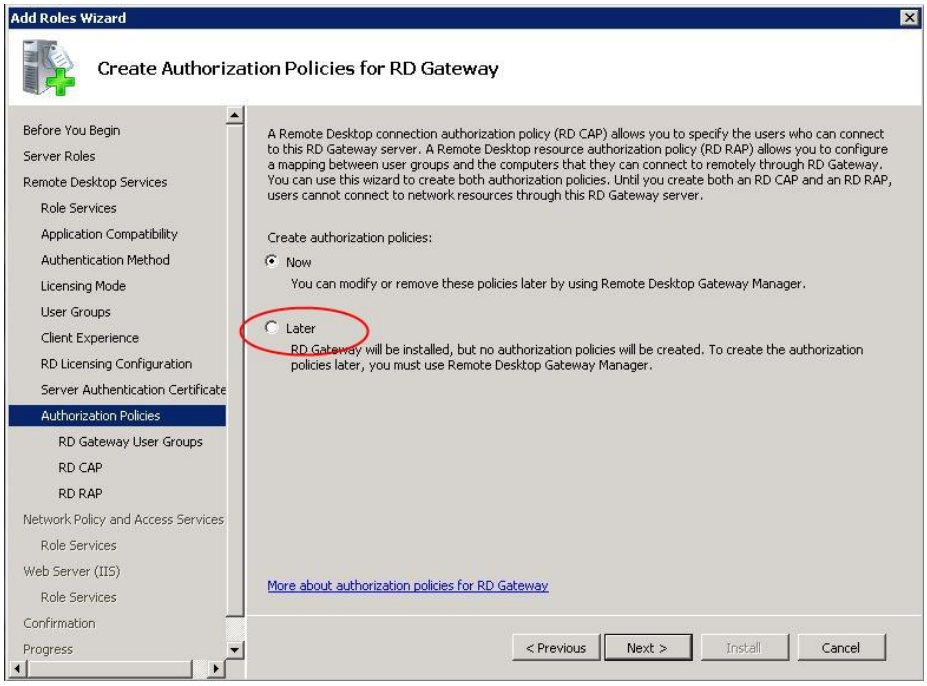


Mikäli palvelimelle on jo määritetty yksi tai useampi varmenne, voidaan halutut varmenteet valita jo tässä vaiheessa. Mikäli varmennetta ei vielä ole, niin se voidaan joko luoda asennuksen tässä vaiheessa tai valita myöhemmin.

Palvelimelle voidaan itse luoda ns. sisäinen varmenne. On kuitenkin suositeltavaa käyttää kolmannen osapuolen varmennetta. Sisäisen varmenteen käyttäminen vaatii aina varmenteen asentamisen erikseen jokaiselle laitteelle, joista etäyhteys otetaan palvelimelle. Varsinkin suurissa käyttäjämäärissä on suositeltavaa hankkia ulkopuoliselta varmenteen myöntäjätaholta varmenne. Tällöin jokaiselle etäyhteyslaitteelle ei tarvitse erikseen asentaa varmennetta.

Etätyöpöytäyhteyden auktorisointikäytännöllä voidaan määrittää, ketkä käyttäjät saavat ottaa yhteyden yhdyskäytäväpalvelimelle. Etätyöpöytäyhteyden auktorisointikäytäntö voidaan määrittää jo asennuksen aikana, tai se voidaan halutessa määrittää myös asennuksen jälkeen. Etätyöpöytäyhteyden auktorisointikäytäntö on kuitenkin luotava ennen kuin etäkäyttäjät voivat olla yhteydessä etäpalvelimeen (kuva 12).

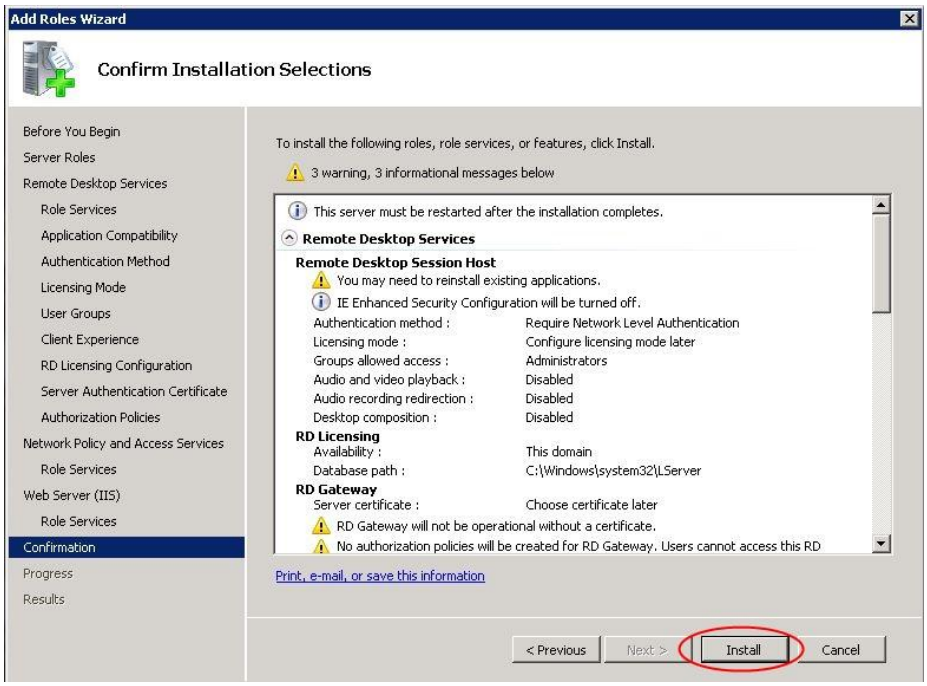
Kuva 12: Etätyöpöytäyhteyden auktorisointikäytäntö



NPAS ja IIS (www-palvelin) voidaan asentaa oletusmäärityksillä. Etätyöpöydän yhdyskäytävä ja web-liittymä tarvitsevat kyseisiä palveluja.

Etätyöpöytäpalvelun asennusvarmistus näyttää asennettavat ominaisuudet (kuva 13).

Kuva 13: RDS-palvelun asennusvarmistusikkuna



Asennus aloitetaan valitsemalla asenna (install). Asennuksen jälkeen palvelin joudutaan käynnistämään uudelleen. Uudelleenkäynnistymisen jälkeen etätyöpöytäpalvelu on asennettu. Ennen palvelun käyttämistä täytyy kuitenkin palveluun tehdään määrityksiä, joita käydään seuraavassa kappaleessa läpi.

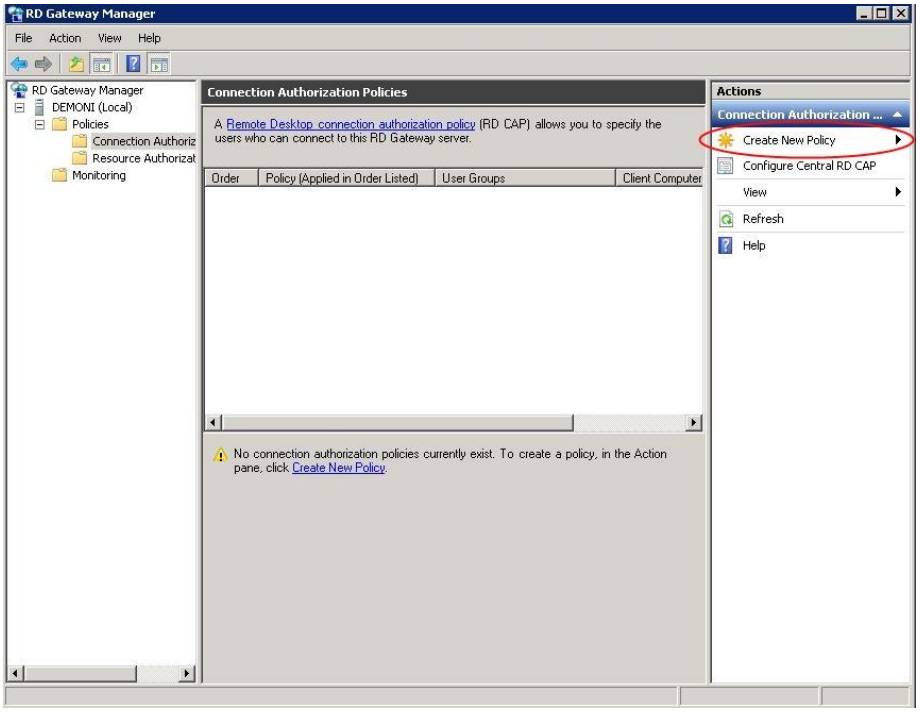
5 Etätyöpöytäpalvelun konfigurointi

Ennen kuin etätyöpöytäpalvelua voidaan käyttää, täytyy siihen tehdä tiettyjä asetuksia. Tässä kappaleessa käydään läpi kyseiset asetukset.

5.1 Yhteyden ja resurssien auktorisointikäytännöt

Ensimmäiseksi määritetään etätyöpöytäyhteyden ja etätyöpöydän resurssien auktorisointikäytännöt etätyöpöydän yhdyskäytäväpalvelimelle. Auktorisointikäytännöt määritetään etätyöpöydän yhdyskäytävän -hallintatyökalun avulla. Molemmat auktorisointikäytännöt voidaan luoda samalla kertaa käyttämällä *Create New Authorization Policies Wizard* -asennusvelhoa (kuva 14).

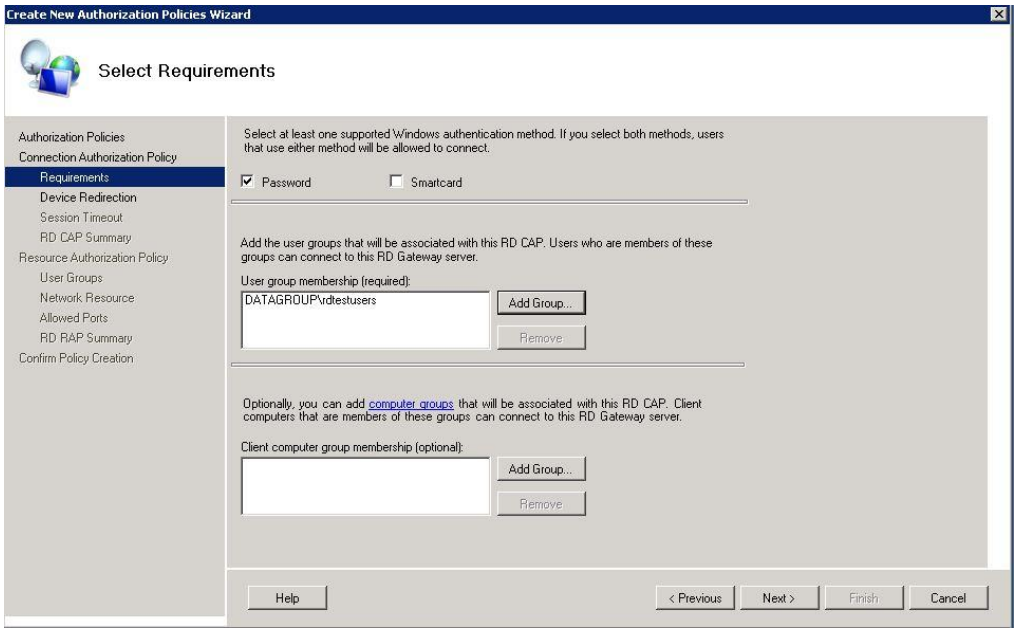
Kuva 14: Yhteyskäytäntöjen luonti



Valitaan *Create a RD CAP and a RD RAP (recommended).* RD CAP -käytännöllä valitaan ne käyttäjät, jotka saavat ottaa yhteyden etäpalvelimeen. Tähän kannattaa määrittää käyttäjäryhmittäin käyttäjät, jotka saavat ottaa yhteyden etäpalvelimeen. Tämä helpottaa palvelimen ylläpitoa, varsinkin silloin kun käyttäjiä on paljon. Jälkeenpäin uudelle käyttäjälle on helppo antaa etäkäyttöoikeus lisäämällä hänet

etäkäyttäjäryhmään. Tässä kohtaa voidaan myös halutessa määrittää ne tietokoneet, jotka saavat ottaa yhteyden etäpalvelimelle (kuva 15).

Kuva 15: RD CAP sallitut käyttäjät ja ryhmät



Device Redirection -kohdassa voidaan estää määrättyjen laitteiden reitittyminen etäyhteyteen, esimerkiksi tietoturvasyistä USB-muistitikkujen reitittymininen etäyhteyteen voidaan estää.

Session Timeout:lla voidaan määrittää istunnon aikakatkaisu, toisin sanoen milloin käyttämätön yhteys katkeaa (*Enable idle timeout*). Tämä on erittäin suositeltavaa ottaa käyttöön. Istunnon aikakatkaisulla voidaan yhteys määritetyn ajan jälkeen joko katkaista tai todentaa uudelleen ja valtuuttaa ilman, että käyttäjä huomaa mitään.

Etätyöpöydän resurssien auktorisointikäytännöllä määritetään, mihin resursseihin käyttäjät saavat kyseisellä etätyöpöydän yhdyskäytäväpalvelimella ottaa yhteyttä. Määritetään samalla tavalla kuin RD CAP:ssakin käyttäjäryhmä tai käyttäjät, joihin kyseinen RD RAP -käytäntö otetaan käyttöön. Oletuksena asennusvelho tarjoaa samoja käyttäjämäärityksiä kuin RD CAP:ssa. Halutessa eri käyttäjäryhmille tai käyttäjille voidaan määritellä erilaisia RD RAP -käytäntöjä.

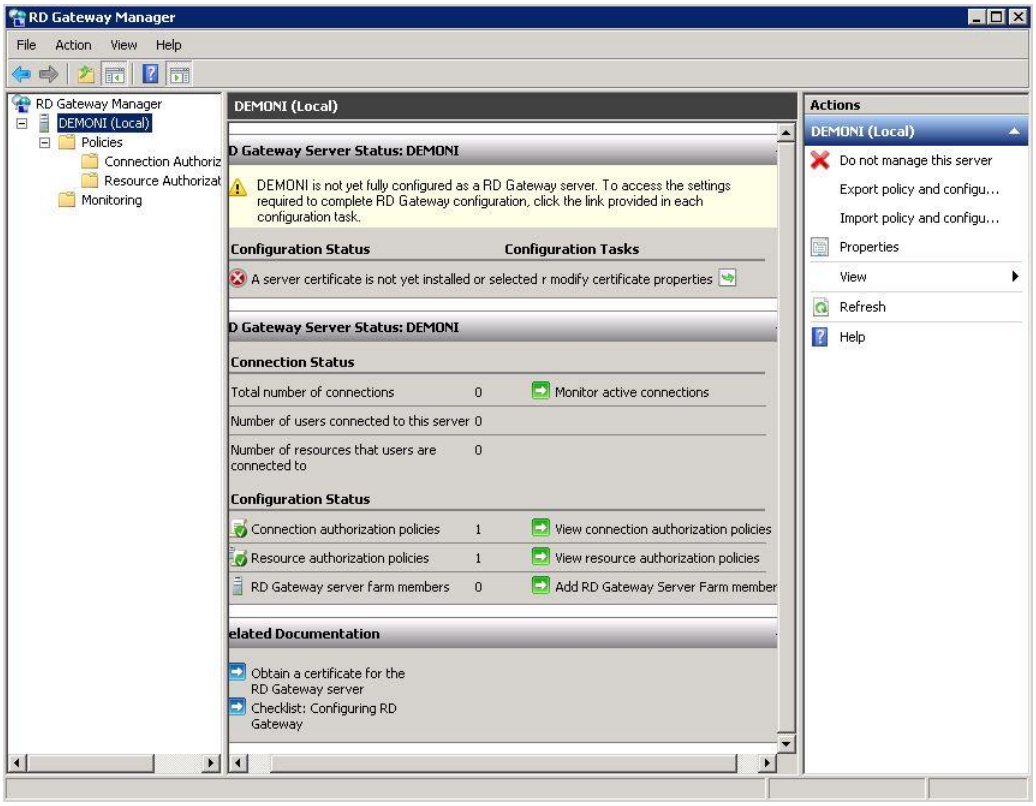
RD RAP:ssa määritetään ne palvelimet tai työasemat joihin etäkäyttäjä saa olla yhteydessä. Yksinkertaisimmillaan voidaan määrittää, että etäkäyttäjät saavat ottaa yhteyden mihin tahansa verkkoresurssiin eli tietokoneeseen tai palvelimeen. Mikäli käytössä ei ole useampia palvelimia niin tätä vaihtoehtoa voidaan käyttää.

Isommissa ympäristöissä kuitenkin on suositeltavaa rajata resurssit joita verkossa saa etänä käyttää. Määritys voidaan tehdä joko AD:n kautta tai määrittää RD Gateway-managed groupilla. Suositeltavinta on käyttää AD:n ryhmiä ylläpidollisia tehtäviä helpottavista syistä.

Oletuksena verkkoresursseihin otetaan yhteys TCP -portista 3389. Portti voidaan muuttaa, mikäli näin halutaan. Mikäli portti muutetaan, niin se on otettava huomioon palomuureja määritettäessä.

Nyt palvelimelle on määritetty RD CAP ja RD RAP -käytännöt, joilla kerrotaan palvelimelle, ketkä käyttäjät ja mihin verkkoresursseihin kyseiset käyttäjät saavat olla yhteydessä.

Kuva 16: RD Gateway Manager, RD CAP ja RAP määritettyinä



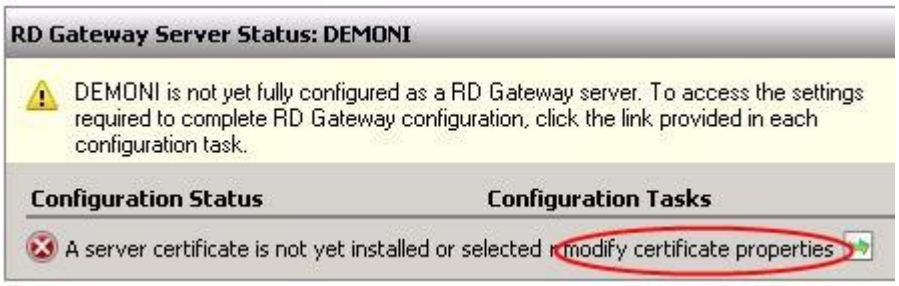
Etätyöpöydän yhdyskäytävän hallintatyökalun pääikkunasta nähdään kohdassa Configuration Status, että auktorisointikäytäntöjä on nyt yksi molempia käytössä (kuva 16).

Hallintatyökalu ilmoittaa vielä, että tarvittavaa varmennetta ei ole otettu käyttöön. Se täytyy tehdä seuraavaksi.

5.2 Etätyöpöydän yhdyskäytävän varmenne

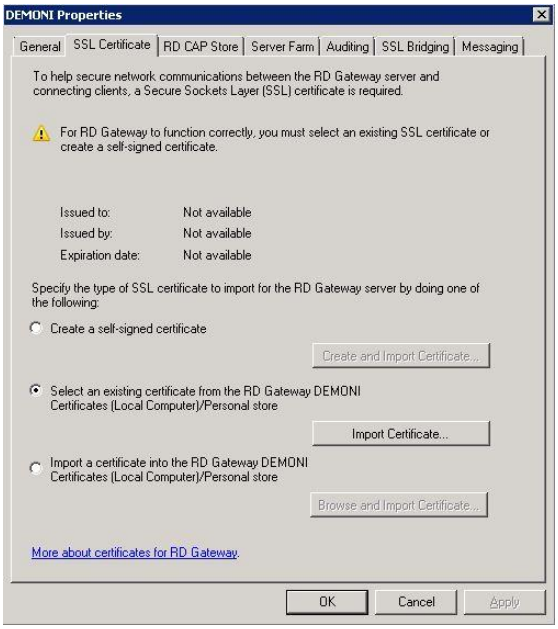
Palvelimelle täytyy määrittää palvelinvarmenne (server certificate) ennen kuin se voi toimita etätyöpöydän yhdyskäytäväpalvelimena. Varmenne voidaan ottaa käyttöön etätyöpöydän yhdyskäytävän hallintatyökalulla valitsemalla linkki *modify certificate properties* (kuva 17).

Kuva 17: RD Gateway server certificate -ilmoitus



SSL Certificate -välilehdellä voidaan luoda uusi varmenne, valita olemassa oleva varmenne palvelimen varmennesäilöstä tai tuoda aikaisemmin luotu varmenne (kuva 18). Tässä tapauksessa palvelimella on jo valmiina sopivia varmenteita, joten valitaan *Select an existing certificate...* alta haluttu varmenne.

Kuva 18: RD Gateway varmenne

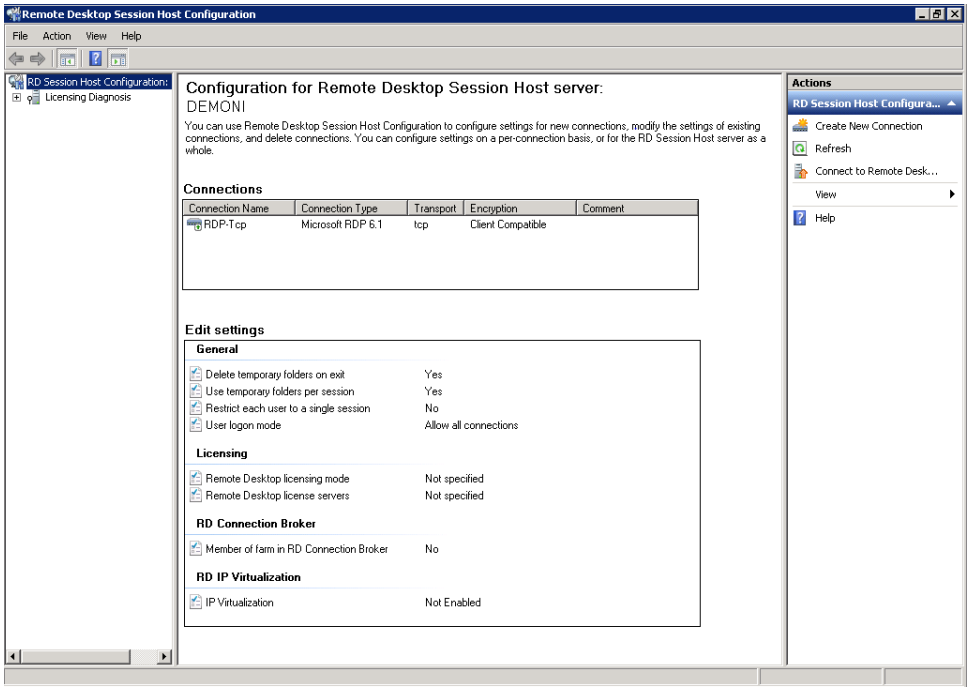


Varmenteen määrittämisen jälkeen RD Gateway -palvelu on määritelty ja toiminnassa.

5.3 Etätyöpöydän lisensointi

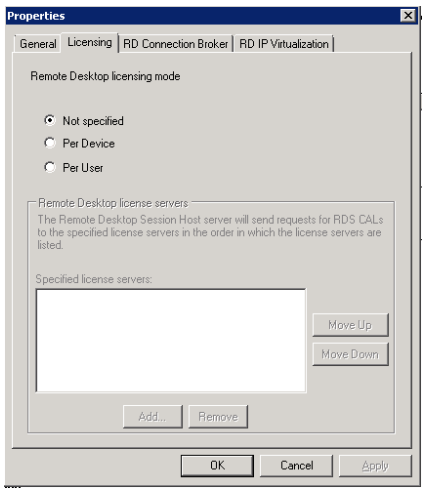
Etätyöpöytäpalvelussa voidaan käyttää lisensointimalleina joko käyttäjäperusteisia lisenssejä tai laiteperusteisia lisenssejä. Lisensointimallin voi valita etätyöpöytäistunnon isännän konfigurointityökalulla (kuva 19).

Kuva 19: RD Session Host Configuration



Lisensointimalli valitaan *Edit Settings* -alta kohdasta *Remote Desktop licensing mode*.

Kuva 20: Remote Desktop licensing mode



Valittavina ovat laite ja käyttäjä -lisensointimallit. Laitemallissa (per device) vaaditaan jokaiselta etäpalveluun yhteyttä ottavalta laitteelta oma lisenssinsä. Käyttäjämallissa (per user) vastaavasti jokaiselta käyttäjältä vaaditaan oma lisenssinsä. Eri lisensointimalleja ei voida käyttää samanaikaisesti.

Etätyöpöytäistunnon isäntäpalvelimelle kerrotaan samaisessa asetusikkunassa myös ne palvelimet, jotka toimivat lisensointipalvelimina. Palvelimia voi olla useampia. Istunnon isänstäpalvelin lähettää lisenssien vahvistuspyynnöt palvelimille siinä järjestyksessä, jossa ne listassa ovat.

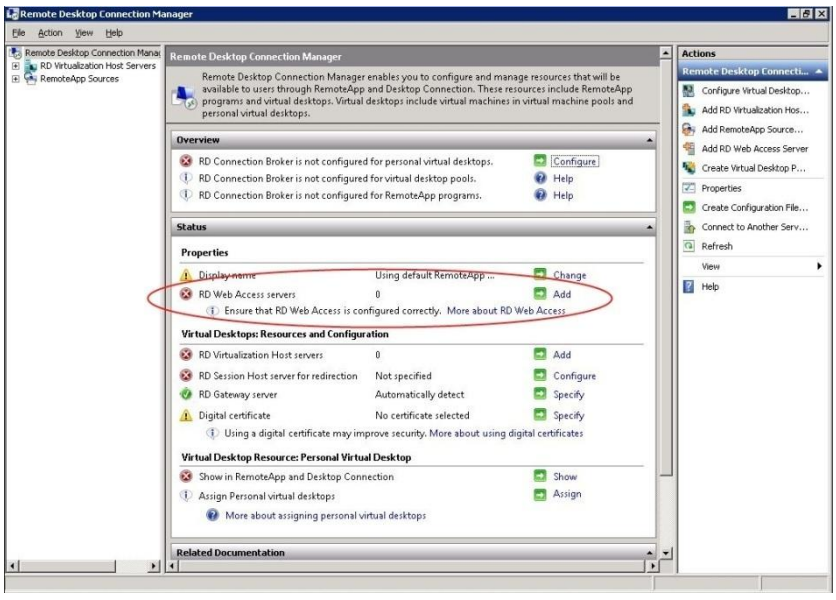
5.4 Etätyöpöydän web-liittymä ja etäohjelmat

Luvuissa 5.1-5.3 tehtyjen määritysten jälkeen käyttäjät voivat ottaa yhteyttä etäpalvelimille etätyöpöytäyhteyden asiakasohjelmalla, joka näyttää palvelimen työpöydän käyttäjälle. Kyseisen ohjelman avulla voidaan jo käyttää etäpalvelimelle asennettuja sovelluksia.

Microsoft Windows Server 2008 toi kuitenkin uutena ominaisuutena mahdollisuuden käyttää ohjelmia suoraan joko selaimen kautta tai erillisillä etäohjelmapikakuvakkeilla.

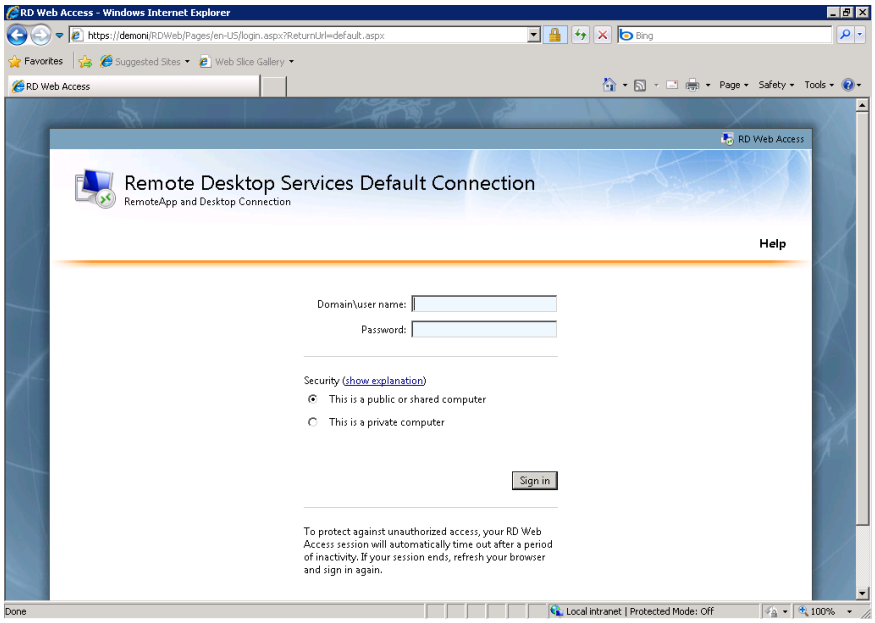
Etätyöpöytäyhteyden hallintatyökalussa (Remote Desktop Connection Manager) kerrotaan mitkä palvelimet toimivat etätyöpöydän web-liittymän palvelimina. Palvelin tai palvelimet voidaan lisätä etätyöpöytäyhteyden hallintatyökalulla (kuva 21).

Kuva 21: RD Connection Manager



Oletuksena web-liittymän osoite on https://*palvelimen_nimi*/rdweb. Kyseiseen palveluun pääsee Internet Explorer -selaimella (kuva 22).

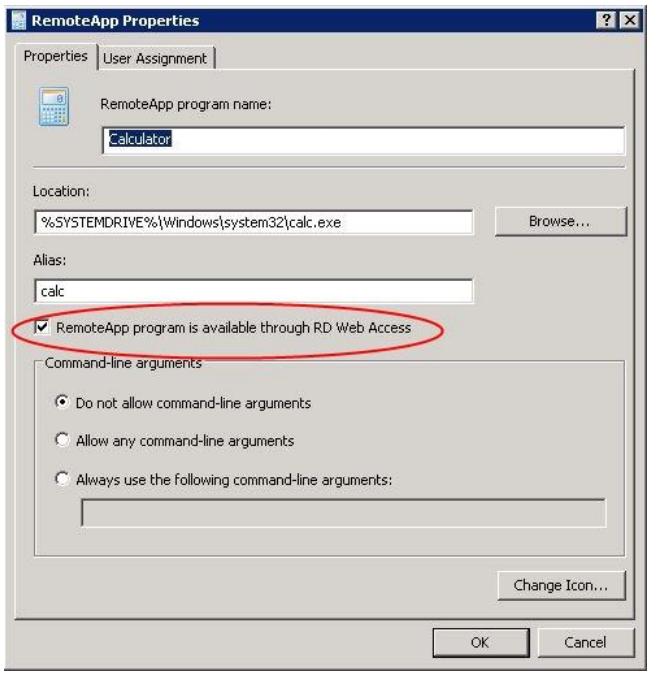
Kuva 22: RD Web Access -sivusto



Sivuston kautta voidaan jakaa käyttäjille ohjelmia käytettäväksi. Jaettavat ohjelmat määritetään etäohjelman hallintatyökalulla (RemoteApp Manager). Ohjelmat voidaan jakaa käyttäjien käytettäväksi joko web-liittymän kautta tai niistä voidaan tehdä pikakuvakkeita, joilla käyttäjät voivat käyttää ohjelmia aivan kuin ne olisi asennettu käyttäjän omalle koneelle.

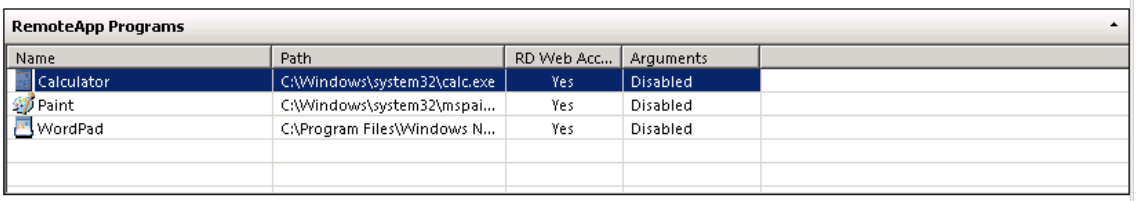
Ohjelmia saa lisättyä käyttöön valitsemalla *Add RemoteApp Programs.* Tämä avaa *RemoteApp Wizard* -velhon, jonka avulla voidaan määrittää halutut ohjelmat. Ohjelmia voidaan valita useampia kerrallaan. Ominaisuudet -painikkeen alta voi etäojelmalle antaa määrityksiä. Tämän valikon alta valitaan myös se, onko ohjelma käytettävissä web-liittymässä (kuva 23).

Kuva 23: RemoteApp Properties



Käytettäväksi julkaistut ohjelmat tulevat etäohjelman hallintatyökalun listaan näkyviin (kuva 24).

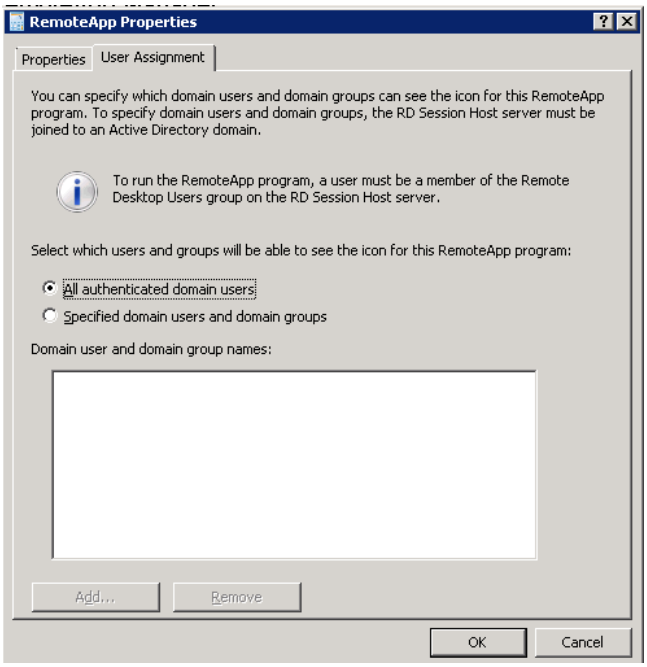
Kuva 24: Julkaistut RemoteApp -ohjelmat



Microsoft Windows Server 2008 R2:n etätyöpöytäpalvelin uutena ominaisuutena aikaisempaan on mahdollisuus määrittää mitä ohjelmia kukin käyttäjä voi käyttää tai web-liittymän kautta nähdä ja käyttää (Microsoft TechNet 2009). Aikaisemmin tämä ei ollut mahdollista suoraan vaan kyseinen ominaisuus oli käytettävä kolmannen osapuolen maksullisissa ratkaisuissa, kuten esimerkiksi Citrixin etäjärjestelmissä.

Kyseinen ominaisuus määritetään etäohjelmakohtaisesti valitsemalla halutusta etäohjelmasta ominaisuudet. Välilehdellä *User Assignment* voidaan määrittää, ketkä käyttäjät saavat kyseistä etäohjelmaa käyttää (kuva 25).

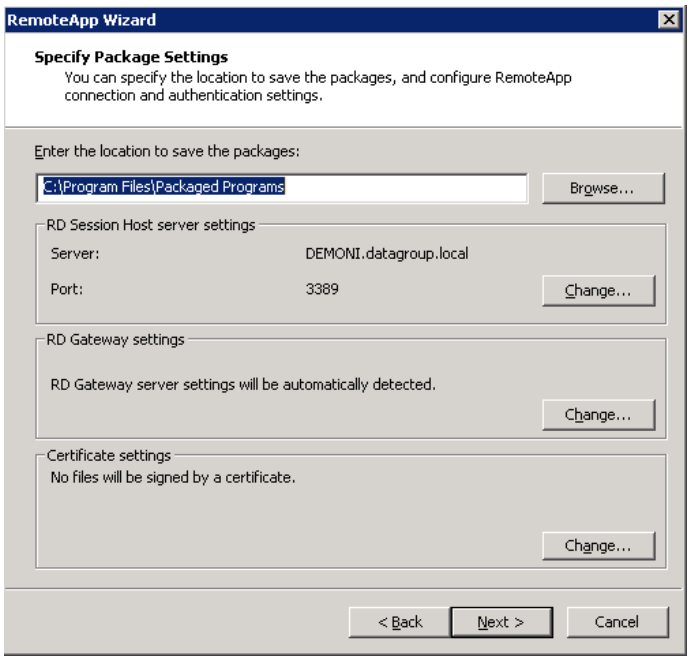
Kuva 25: RemoteApp User Assigment



Oletuksena kaikki toimialueen varmennetut käyttäjät saavat käyttää ohjelmaa. Kohdassa *Specified domain users and domain groups* voidaan määrittää käyttäjät ja käyttäjäryhmät, joille ohjelman käyttöoikeus halutaan antaa.

Etäohjelmista on mahdollista luoda myös pikakuvake (.rdp tiedosto), josta ohjelma voidaan käynnistää suoraan kirjautumatta web-liittymään. Etäohjelman pikakuvake luodaan etäohjelman hallintatyökalulla. Valitsemalla *Create .rdp file* halutusta etäohjelmasta avautuu *RemoteApp Wizard* -asennusvelho. Asennusvelho kysyy, mihin rdp-tiedostot tallenetaan. Oletuksen ne tallentuvat polkuun *c:\Program Files\Packaged Programs*. Asennusvelho haluaa tiedot RD Session Host -palvelimesta, yhdyskäytäväpalvelimesta sekä halutaanko ohjelma suojata varmenteella (kuva 26).

Kuva 26: .rdp -tiedoston luonti



Luodut etäohjelman pikakuvakkeet voi tämän jälkeen jakaa käyttäjille. Käyttäjälle ohjelman käyttö tällä tavalla on saumatonta oman käyttöjärjestelmän kanssa. Useasti käyttäjä ei edes tiedä, että ohjelmaa käytetään verkon yli palvelimelta eikä omalta koneelta.

6 Tulokset

Etätyöpöytäpalvelun asennus onnistui odotetusti eikä asennuksen aikana ongelmia ilmennyt. Asennuksen jälkeen tehtiin tärkeimmät konfiguroinnit, jotta järjestelmä saataisiin käyttäjien käyttöön.

Ensimmäiseksi määritettiin etätyöpöytäyhteyden auktorisointikäytännöllä ne käyttäjät, jotka saavat olla yhteydessä etäpalvelimeen. Etätyöpöydän resurssien auktorisointikäytännöllä taas määritettiin ne palvelimet tai tietokoneet, joihin etäkäyttäjä saa olla yhteydessä.

Etätyöpöydän yhdyskäytäväpalvelimeen ei tarvittu kolmannen osapuolen (esim. Verisign tai Thawte) allekirjoittamaa varmennetta, koska rakennettu etäjärjestelmä tulee yrityksen ylläpito-osaston sisäiseksi testaus- ja kehitysympäristöksi. Varmenteeksi valittiin palvelimen allekirjoittama varmenne (Self-signed certificate).

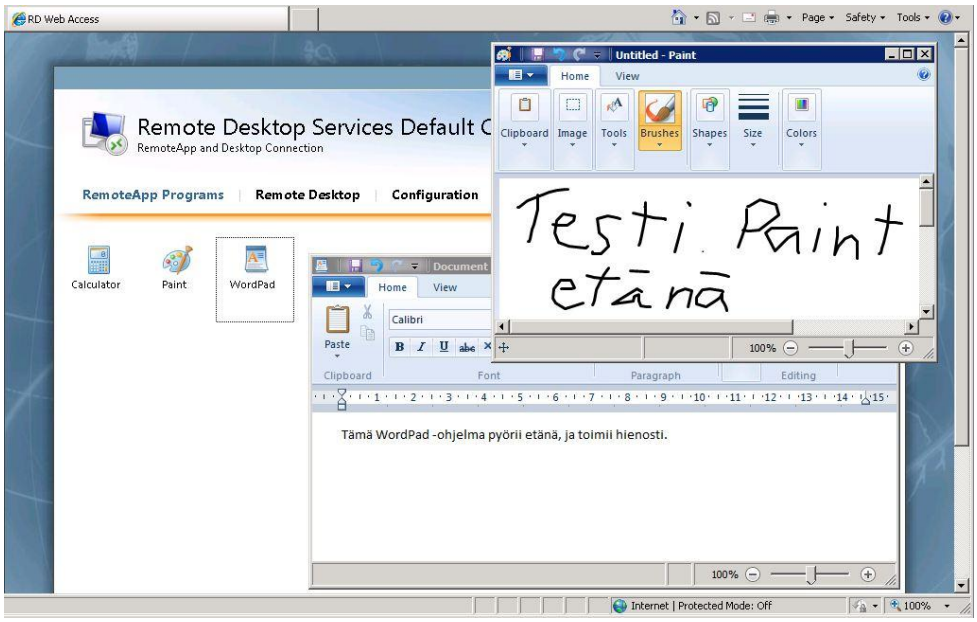
Etäpalvelimen lisenssimallilla ei itse asiassa ollut suurtakaan merkitystä, koska järjestelmän julkaisulle laajemmalle käyttäjäkunnalle ei ole tässä vaiheessa tarvetta. Lisensointimalliksi valittiin kuitenkin useimmiten käytetty käyttäjäperusteinen.

Etätyöpöydän web-liittymän käyttöönotto oli helppoa eikä ongelmia ilmennyt. Etäjärjestelmän toiminta testattiin kirjautumalla web-liittymään ja käynnistämällä sieltä muutama ohjelma (kuva 27).

Kuva 27: RD Web Access -testaus

Testausmielessä käynnistettiin ohjelmat Paint ja WordPad, jotka käynnistyivät ongelmitta ja toimivat moitteetta (kuva 28).

Kuva 28: WordPad ja Paint toimivat etänä.



Järjestelmä toimii hienosti ja tulee palvelemaan yrityksessä testiympäristönä, jossa testataan etäjärjestelmien toimintoja ennen niiden ottamista tuotantoon.

7 Yhteenveto ja pohdintaa

Microsoft on tuonut uusimmassa palvelinkäyttöjärjestelmässään Windows Server 2008 R2 mukanaan odotettuja ja huomattavia parannuksia heidän etätyöpöytäpalveluunsa. Ennen Windows Server 2008:aa käytettävissä oli lähinnä etätyöpöytäyhteys palvelimelle sekä tiedostopalvelun käyttö. Windows Server 2008 paransi huomattavasti palvelua tuomalla mukanaan mm. etäohjelmat, EasyPrinting -ominaisuuden sekä etätyöpöydän web-liittymän.

Windows Server 2008 R2:n myötä palvelun nimi muutettiin etäpäätepalvelusta etätyöpöytäpalveluksi. Lisäksi aikaisemmin tuotuja ominaisuuksia parannettiin. Muun muassa web-liittymän sisällön suodattaminen käyttäjätili- tai käyttäjäryhmäkohtaisesti on tervetullut parannus.

Tästä dokumentista jätettiin osa ominaisuuksista tarkastelematta. Kyseiset ominaisuudet ovat lähinnä keskisuurten ja suurten yritysten käyttämiä ominaisuuksia. Tärkeimpänä näistä on etätyöpöytäyhteyden välittäjä (Remote Destkop Connection Broker), joka mahdollistaa useamman etätyöpöytäistunnin isäntä -palvelimen (Remote Desktop Session Host) käytön ja istuntojen jakamisen näiden palvelimien välillä. Tämä parantaa huomattavasti palvelun tehokkuutta suuremmissa ympäristöissä, koska kaikki käyttäjät eivät ota yhteyttä vain yhteen palvelimeen.

Suuri osa tässä dokumentissa kuvatusta asennuksesta ja konfiguroinneista tehtiin testiympäristössä, jossa oli mahdollista ”kokeilu ja erehdys” -menetelmällä tutkia uusia ominaisuuksia. Tämän dokumentin avulla kyseisiä etäjärjestelmiä tullaan asentamaan asiakkaiden tuotantoympäristöön. Lisäksi uusimman etätyöpöytäpalvelun painetun materiaalin vähäisyys lisäsi haastetta tämän työn tekemiselle. Tästä johtuen lähdemateriaalina jouduttiin käyttämään lähes pelkästään Microsoftin TechNet:in artikkeleja.

LÄHTEET

Pekkola J. & Uskelin L. 2007. Etätyöopas työnantajille. Helsinki: Työministeriö. Saatavisssa myös http://www.mol.fi/mol/fi/99_pdf/fi/06_tyoministerio/06_julkaisut/10_muut/etatyoopas_tyonantajille.pdf.

Tulloch M. 2006. Overview of Terminal Services. Viitattu 13.12.2009 http://www.windowsnetworking.com -> Articles & Tutorials -> Widnows 2003 -> Overview of Terminal Services.

Russel C. & Zacker C. 2010. Introducing Windows Server 2008 R2. Redmond: Microsoft Press.

Microsoft TechNet 2009. What's New in Remote Desktop Services. Viitattu 13.12.2009 http://technet.microsoft.com/en-us/library/dd560658(WS.10).aspx.

Microsoft TechNet 2009. Overview of Remote Desktop Licensing. Viitattu 15.12.2009 http://technet.microsoft.com/en-us/library/cc725933.aspx.

Microsoft TechNet 2009. Overview of Remote Desktop Gateway. Viitattu 16.12.2009 http://technet.microsoft.com/en-us/library/cc731150.aspx.

Microsoft TechNet 2009. Configure Network Level Authentication for Remote Desktop Services Connections. Viitattu 22.12.2009 http://technet.microsoft.com/en-us/library/cc732713.aspx.

Microsoft TechNet 2009. Remote Desktop Web Access. Viitattu 30.12.2009 http://technet.microsoft.com/en-us/library/dd560668(WS.10).aspx.