

Työpöytien virtualisointi
Laurea-ammattikorkeakoulussa



Forsell Teppo, Rossi Tuukka

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Työpöytien virtualisointi Laurea-ammattikorkeakoulussa

Teppo Forsell, Tuukka Rossi
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Tammikuu 2011

Teppo Forsell, Tuukka Rossi

Työpöytien virtualisointi Laurea-ammattikorkeakoulussa

Vuosi 2010 Sivumäärä 122

Työpöydän virtualisoinnilla tarkoitetaan käyttäjän käyttöjärjestelmän siirtämistä palvelimelle paikallisen asennuksen sijasta. Käyttäjän päätelaitteelle välitetään näyttökuva sekä hiiren ja näppäimistön painallukset verkon yli. Keskittämällä käyttöjärjestelmät palvelinsaliin saavutetaan merkittäviä hyötyjä ylläpidon näkökulmasta, kuten ympäristön hallinta yhdestä sijainnista.

Opinnäytetyön tarkoituksena on tuottaa tietoa Laurean IT-palveluille siitä miten työpöytävirtualisointia voitaisiin hyödyntää opetus- ja laboratorioympäristöissä. Tavoitteena oli selvittää, mitä asioita tulee ottaa huomioon työpöytävirtualisoinnin käyttöönotossa.

Työpöytävirtualisointi on yleistynyt ja kehittynyt vauhdilla palvelinvirtualisoinnin jalanjäljissä. Monet ammattikorkeakoulut ovat testanneet ja ottaneet käyttöön VDI-ympäristöjä. Laurea IT-palvelut tarvitsivat tietoa eri ratkaisuvaihtoehdoista, teknologioista ja siitä, kuinka työpöytävirtualisointia voitaisiin hyödyntää sen ylläpitämässä ympäristössä. Opinnäytetyö toteutettiin yhdessä Laurea IT-palveluiden kanssa, joka tarjosi projektille tarvittavat tilat ja laitteet.

Työssä tehtiin testiympäristöt, joiden avulla arvioitiin teknologioiden soveltuvuutta käyttötarkoitukseen. Testiympäristöjen asennukset dokumentoitiin, jotta niitä voitaisiin hyödyntää myöhemmin pohjana toteutusympäristön suunnittelussa. Eri vaihtoehtojen avaamista varten esiteltiin yleisimmät virtualisoinnin muodot sekä Microsoftin, VMwaren ja Citrixin työpöytä- ja sovellusvirtualisoinnin ratkaisut.

Työn tuloksena saatiin selvitys asioista, joihin tulee kiinnittää huomiota toteutusympäristön suunnitteluprojektissa. Testauksen pohjalta tehtiin arviointi VMwaren ja Microsoftin teknologioiden soveltuvuudesta Laurean opetus- ja laboratorioympäristöihin. Lopuksi työssä esiteltiin jatkokehitysehdotus ratkaisuiden hyödyntämisestä IT-palveluille.

Opinnäytetyö on luonteeltaan tapaustutkimus ja siinä hyödynnetään lähestymistapana konstruktivistista tutkimusotetta. Konstruktiona on testiympäristöjen luominen ja erilaisten ratkaisumallien toimivuuden osoittaminen käytännössä.

Asiasanat: työpöytä, virtualisointi, VDI

Teppo Forsell, Tuukka Rossi

Desktop virtualization at Laurea University of Applied Sciences

Year	2010	Pages	122
------	------	-------	-----

Virtual Desktop Infrastructure (VDI) means that the user's operating system is installed on a server instead of a local machine. In this scenario the data transmitted from the server to user's terminal device is the screen image, mouse movements and keystrokes. System administrators can achieve significant benefits by moving operating systems to the data center, such as centralized management and data security.

The purpose of the research is to provide information to Laurea IT services how desktop virtualization could be used in teaching and laboratory environments. The objective was to discover what issues have to be considered before migrating to desktop virtualization.

Server virtualization has been a remarkable success in the last decade. Desktop virtualization has evolved and spread rapidly after commonly used server virtualization. The next big step in virtualization is the VDI environments mentioned above. Many Finnish universities of applied sciences have tested and introduced their own VDI environments. Laurea IT services is also interested in these possibilities and offered necessary resources for this project.

This research presents the most common forms of virtualization as well as Microsoft and VMware's VDI test environments for evaluating their technological compatibility against Laurea's needs. The test environment installations were documented that they could be used as a basis for the later implementation project.

The result of the research is a report on matters, which should be considered as a part of the implementation project. Test environments offered information about how the chosen solutions meet different studying environments requirements. At the end of this thesis a proposal is presented from the Laurea IT services point of view concerning how they could exploit virtualization in future.

The thesis is a case study and it is based on constructive research approach. In this case construct is creating test environments and proofing their compatibility in practice.

Key words: desktop, virtualization, VDI

Sisällys

Termit ja lyhenteet	6
1 Johdanto.....	8
1.1 Opinnäytetyön tavoite ja menetelmät	9
1.2 Työn rajaus	10
1.3 Työn tilaaja	10
2 Virtualisointi	11
2.1 Palvelinten virtualisointi	13
2.2 Sovellusvirtualisointi	16
2.2.1 Microsoft App-V	17
2.2.2 VMware ThinApp.....	18
2.2.3 Citrix XenApp	19
2.3 Tallennusvirtualisointi	20
2.4 Verkon virtualisointi.....	22
2.5 Työpöydän virtualisointi (VDI)	23
2.5.1 Microsoft VDI	23
2.5.2 VMware View 4.....	27
2.5.3 Citrix XenDesktop 4	33
2.6 Esityskerroksen virtualisointi	37
3 Testiympäristöt.....	38
3.1 Testiympäristö 1, Microsoft VDI	39
3.2 Testiympäristö 2, VMware View 4	44
4 Testaus.....	45
4.1 Johtopäätökset	48
4.2 Kehitysehdotukset	48
5 Huomioitavia asioita virtualisointiprojektissa	49
5.1 Tallennus	49
5.2 Tietoturva	50
5.3 Tiedonsiirto	51
5.4 Lisensointi ja kustannukset	51
5.5 Käyttökokemus ja lisälaitteet	52
6 Yhteenveto	52
Lähteet	54
Kuvaluettelo	58
Liite 1 Microsoft VDI-ympäristön asennus	60
Liite 2 SCVMM 2008 R2	81
Liite 3 VMware View 4.0 asennus	90

Termit ja lyhenteet

Active Directory on Microsoftin käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoja esim. käyttäjistä ja tietokoneista.

AMD-V on AMD:n x86-prosessorille, jossa on virtualisointi tuki.

APP-V eli Microsoft Application Virtualization on Microsoftin ratkaisu ohjelmistojen virtualisointiin.

Connection Broker - Ohjelmisto työpöytävirtualisoinnissa, joka yhdistää loppukäyttäjän virtuaalisiin työpöytiin.

DHCP on verkkoprotokolla, jonka päätehtävänä on antaa IP-osoitteita lähiverkkoon kytkeytyville laitteille.

DNS on internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.

Domain Controller --palvelin toimii toimialueen ylläpitäjänä ja sen päätehtävänä on ylläpitää toimialueen tietokantaa resursseista ja tunnistaa sinne kirjautuvat käyttäjät.

FQDN Fully Qualified Domain Name on domain-nimi, joka kertoo tarkan sijainnin DNS hierarkiassa.

I/O Input/Output, tallennusratkaisuissa sillä kuvataan luku ja kirjoitusoperaatioita.

ISO 9126 on kansainvälinen ohjelmistojen laatuja arviointiin määritelty standardi.

ICA, Citrixin kehittämä etäyhteysprotokolla.

Intel VT nimitys Intelin x86-prosessorille, jossa on virtualisointi tuki.

Internet SCSI (iSCSI) eli Internet Small Computer System Interface on standardi tiedon välittämiseksi tietokoneen ja oheislaitteiden välillä.

ISO image on arkistotiedosto, johon on tallennettu esimerkiksi käyttöjärjestelmän levykuva.

LAN, Local Area Network on rajoitetulla alueella toimiva lähiverkko.

LUN eli Logical Unit Number on yksilöllinen tunniste jonka avulla tunnistetaan looginen yksikkö tallennusjärjestelmissä.

NLA Network Level Authentication on RDP ohjelman käyttämä autentikointiteknologia, jolloin käyttäjän tulee tunnistautua ennen kuin yhteys muodostuu clientilta palvelimelle.

PCoIP on Teradecin valmistama protokolla joka mahdollistaa etäyhteyden tietokoneeseen tai palvelimeen esim. LCD monitorista jos laitteessa on PCoIP prosessori.

RDC 7.0 eli Remote Desktop Connection 7.0 on Microsoftin RDP protokollaa käyttämä etäyhteysohjelma, jonka avulla käyttäjä voi ottaa etäyhteyden toiselle tietokoneelle.

RDP Microsoftin kehittämä etäyhteysprotokolla, tarjoten graafisen käyttöliittymän etäkoneesta.

RDS eli Remote Desktop Services (entinen Terminal Services) avulla lähiverkon tietokoneet voivat käyttää etäyhteydellä palvelimen työpöytää, ohjelmia, sekä palveluita.

RemoteAPP on Remote Desktop Connection ohjelmiston versioiden 6.1 tai uudempien ominaisuus, jonka avulla voidaan ottaa etäyhteys sovelluksiin ilman että muodostetaan yhteyttä virtuaaliseen työpöytään.

SSL on salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.

VDI eli Virtual Desktop Infrastructure tarkoittaa teknologiaa jolla käyttäjälle toimitetaan palvelimelta ajettava virtuaalinen työpöytä.

VECD Lisenssi datakeskuksesta käytettäville virtuaalisille työpöydille

VHD, Virtual Hard Disk on Microsoftin formaatti virtuaalikoivalevyille.

VMM, Virtual Machine Monitor (tunnetaan myös nimellä Hypervisor) on virtualisointiohjelma, jonka avulla voidaan ajaa useita käyttöjärjestelmiä yhdeltä fyysiseltä koneelta.

Windows Hyper-V, tunnettiin aiemmin nimellä Windows Server Virtualization. Hyper-V on varsinkin palvelimille suunnattu virtualisointitekniikka.

X86 on yleinen termi Intelin kehittämälle suoritinarkkitehtuurille.

1 Johdanto

Yrityksillä on jatkuva tarve kehittää liiketoimintaa ja miettiä keinoja, joilla asioita saataisiin suoritettua entistä kustannustehokkaammin samoilla resursseilla. Nykypäivän vaatimukset dynaamisista ja tehokkaasti hallittavista IT-ympäristöistä ovat olleet omiaan vauhdittamaan perinteisten työasemaympäristöjen kehitystä. Muutosta vie eteenpäin entistä globaalimmaksi muuttuva maailma ja etätyön yleistymisen. Ihmisille ei riitä tulevaisuudessa enää pääsy yrityksen sähköposteihin kotoa käsin vaan oman työpöydän on seurattava mukana. Osa yrityksistä on siirtänyt jo nyt käyttäjien työpöytiä palvelimelle turvaan tietoturvallisuussyistä. Kannettavan tietokoneen voi varastaa matkan päällä, mutta palvelimella tiedot ovat turvassa, mikäli ympäristö on muuten toteutettu asianmukaisesti. Tietoturvallisuuden lisäksi toinen tärkeä osa-alue on hallittavuus. Ylläpidon toimintaa pystytään tehostamaan yhtenäisesti hallitulla ympäristöllä ja minimoimaan paikallisesti tehtävien asennusten määrää. Samalla palvelutasoa voidaan kehittää ja käyttäjille pystytään tarjoamaan entistä joustavampi tapa tehdä työtä.

Virtualisointi on yleistynyt vauhdilla viimeisen kymmenen vuoden aikana, kun palvelimia on alettu virtualisoimaan entistä enemmän. Organisaatioilla on ollut perinteisesti käytössä paljon fyysisiä palvelimia ympäristöissään, jotka vievät paljon tilaa ja kuluttavat paljon energiaa. Palvelinten virtualisoinnin avulla on saavutettu säästöjä esimerkiksi laitekannan pienenemisestä johtuvan energiankulutuksen alentumisena ja sitä myötä laitteiden käyttöastetta on hyödynnetty aiempaa tehokkaammin. Verkon ja tallennuksen virtualisointi on myös yleistynyt palvelinten virtualisoinnin rinnalla.

Seuraava suuri askel on työpöytävirtualisoinnin yleistyminen. Työpöytiä virtualisoidessa käyttäjien työpöydät ja tiedostot sijaitsevat palvelimilla. Tämä mahdollistaa joustavamman työskentelyn käyttäjälle, kun työpöytä ei ole enää sidottu yhteen työasemaan. Yleensä vaatimuksena on vain toimiva verkkoyhteys. Työpöytien hallinnoiminen helpottuu kun tiedot ovat keskitetyksi palvelimilla, näin tarvittavat muutokset ja asetukset saadaan hyvinkin nopeasti tehtyä suurelle massalle.

Monet ammattikorkeakoulut tekevät parhaillaan kartoituksia ja pilottihankkeita työpöytävirtualisoinnin parissa. Laurean IT-palvelut on osaltaan kiinnostunut näiden teknologioiden hyödyntämisestä omassa ympäristössään ja tarvitsee tietoa siitä, mitä erilaisia ratkaisuvaihtoehtoja on olemassa sekä kuinka niitä voitaisiin hyödyntää. Virtualisointi tuo lukuisia mahdollisuuksia niin suurille organisaatioille kuin yksittäisille käyttäjille. Opetuskäyttöön ja laboratorioympäristöihin virtualisointi tarjoaa hyvän mahdollisuuden testailuun ja kokeiluun järjestelmänvalvojan oikeuksin, ilman huolta pysyvistä vahingoista.

Laurea-ammattikorkeakoulussa on lukuisia koulutusaloja, paikallisyksiköitä ja opetusympäristöjä. Erilaisten ympäristöjen hallinnoiminen tuottaa ylläpidolle ylimääräistä työtä ja vie paljon aikaa, esimerkiksi liiketalouden opiskelijoiden tarpeet eroavat huomattavasti tietojenkäsittelyn opiskelijoista käytettävien ohjelmien sekä työasemien käyttäjäoikeuksien puolesta. Suurimmalle osalle oppilaista riittää käyttäjätason oikeudet työasemaan, mutta kaikki ohjelmien asennusta tai järjestelmän muokkausta vaativat opetusjaksot edellyttävät korkeampia oikeuksia. Aikaisemmin näihin haasteisiin on vastattu sisäverkosta eristetyillä ympäristöillä ja helposti vikaantuvilla vaihtolevyillä. Virtualisoinnin avulla opiskelijoille voitaisiin tarjota keskitetysti opintojakson mukaisesti räätälöidyt ympäristöt ja tuottaa ne ylläpidon kannalta tehokkaalla tavalla.

1.1 Opinnäytetyön tavoite ja menetelmät

Opinnäytetyön tarkoituksena on tuottaa tietoa Laurean IT-palveluille miten työpöytävirtualisointia voitaisiin hyödyntää Laurea-ammattikorkeakoulun opetus- ja laboratorioympäristöissä. Tavoitteena on selvittää, mitä asioita tulee ottaa huomioon työpöytävirtualisoinnin käyttöönotossa. Työssä tehdään testiympäristöt, joiden avulla voidaan arvioida teknologioiden toiminnallista laatua, luotettavuutta, käytettävyyttä, ylläpidettävyyttä sekä siirrettävyyttä. Testiympäristöjen asennukset dokumentoidaan, jotta niitä voitaisiin hyödyntää myöhemmässä vaiheessa pohjana toteutusympäristöille.

Työ on luonteeltaan tapaustutkimus ja siinä hyödynnetään lähestymistapana konstruktivistista tutkimusotetta. Työssä toteutetaan uusi ratkaisu luomalla konstruktio. Tässä tapauksessa konstruktio on testiympäristöjen luominen ja erilaisten ratkaisumallien toimivuuden osoittaminen käytännön ympäristössä. Työstä saatavaa informaatiota voidaan myös hyödyntää jatko-tutkimuksissa, mikä osaltaan tukee tapaustutkimuksen piirteitä. Testiympäristöt ja niiden asennusdokumentaatiot tuovat haluttua lisäinformaatiota työn tilaajalle. Lähestymistavan valinnassa voidaan myös hyödyntää luovuutta ja poimia kustakin lähestymistavasta ne piirteet, jotka parhaiten sopivat omaan kehittämistyöhön. Yleisimmistä tutkimusmenetelmistä konstruktioivinen tutkimusote soveltuu yksistään parhaiten opinnäytetyöhömmä. Tiedon keräämiseen hyödynsimme havainnointia ja benchmarkingia. Osallistuimme useisiin eri toimijoiden järjestämiin tapahtumiin, osana aiheeseen perehtymistä. Aiheeseen suoraan liittyneistä tapahtumista voidaan mainita AMK-virtualisointipäivät, AMK VDI - seminaari CSC, Atea Focus 2010 ja Citrix live virtualization - tapahtumat sekä palaverit Microsoftin edustajan kanssa. Havainnointiin käytämme myös omia kokemuksiamme ylläpidosta Laurea IT-palveluiden työsuhteen ajalta. (Ojasalo, Moilanen & Ritalahti 2009, 67.)

1.2 Työn rajaus

Työssä esitellään alan isoimpien yritysten ratkaisut työpöytä- ja ohjelmistovirtualisoinnista (Microsoft, VMware, Citrix), sekä kerrotaan yleisimmistä virtualisoinnin muodoista. Microsoftin ja VMwaren ratkaisusta rakennetaan testiympäristöt. Laurean IT-palvelut on jo testannut Citrixin tuotteilla virtualisointia, joten se jäi testauksen ulkopuolelle. Työ on rajattu koskemaan Laurean sisäverkossa olevia kiinteitä työasemia, joiden palveluita tulnaisiin käyttämään paikallisesta lähiverkosta käsin. Rajauksen ulkopuolelle jäävät tarkat kustannuslaskelmat lisenssiehtojen jatkuvien muutosten ja vallitsevien sopimusehtojen vuoksi. Testiympäristöjen ulkopuolelle rajataan tuotantoympäristön toteutukseen liittyvät ratkaisut tallennusjärjestelmien ja verkon virtualisoinnista. Ratkaisusta kerrotaan yleisellä tasolla, jotta työ pysyisi tavoitteiden mukaisessa mittakaavassa.

1.3 Työn tilaaja

Tämän työn tilaajana toimii Laurea-ammattikorkeakoulu. Työ tulee toimeksiantona Laurea-ammattikorkeakoulun IT-palveluiden suunnittelija Jarmo Tapiolta. IT-palvelut vastaa Laurean tietojärjestelmien ja ohjelmistojen asennuksista sekä ylläpidosta.

Laurea-ammattikorkeakoulu toimii osakeyhtiömuotoisena (Laurea-ammattikorkeakoulu Oy). Omistuspohja on 97-prosenttisesti kunnallinen. Laurea-ammattikorkeakoulun henkilöstöön kuuluu noin 500 työntekijää, sekä noin 700 vierailevaa luennoitsijaa. Laurea on Suomen kolmanneksi suurin ammattikorkeakoulu (aloituspaikkojen määrän perusteella) ja tällä hetkellä Laureassa opiskelee n. 8000 opiskelijaa, päätoimisia opettajia on n. 300. Laurean liiketoimintaa on koulutuksen tuottaminen ammattikorkeakouluopiskelijoille. Koulutus jakautuu eri koulutusaloille, joita on yhteensä kuusi. (Laurea numeroin 2009.)

Laurean koulutusalat:

- luonnontieteiden ala
- luonnonvara- ja ympäristöala
- matkailu-, ravitsemis- ja talousala
- sosiaali-, terveys- ja liikunta-ala
- yhteiskuntatieteiden, liiketalouden ja hallinnon ala

Kaikki opetus on ammattikorkeakoulupohjaista. Osa koulutusaloista opetetaan useammassa kuin yhdessä toimipisteessä, kun taas osa koulutusaloista on lokalisoituneita pelkästään yhteen toimipisteeseen. Koulutusta antavia paikallisyksiköitä Laurealla on seitsemän.

2 Virtualisointi

Virtualisointia on vaikeaa määrittää yhdellä tavalla tai yleispätevästi kaikille eri tavoille, joilla sitä voidaan toteuttaa. Dittner & Rules (2009) mukaan: "A framework or methodology of dividing the resources of computer hardware into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning". Virtualisoinnin avulla voidaan erottaa tietojenkäsittelyn resursseja kerroksiksi, jotka on eristetty toisistaan.

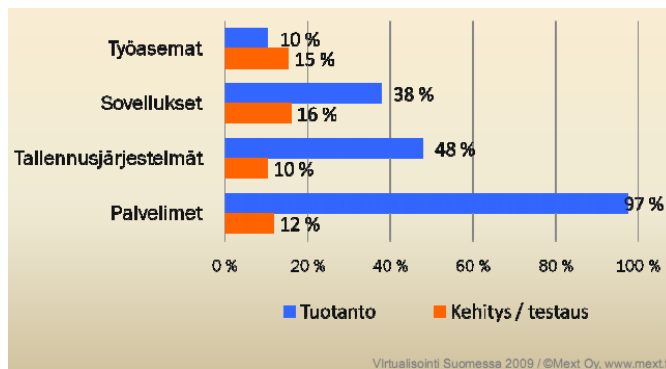
Virtualisoinnilla on jo pitkä historia takanaan, jonka IBM aloitti 1960-luvulla keskustietokoneillaan. Alkujaan virtualisoinnin ei ollut tarkoitus olla yksinoikeudella valmistettu teknologia rajoittuen vain muutamaiin valmistajiin ja erittäin kalliisiin laitteistoihin. Sen sijaan virtualisoinnin tarkoitus oli olla ilmainen ja vapaasti käytettävissä kaikille halukkaille, sekä kyettävä toimimaan x86 -pohjaisilla laitteistoilla. Nykypäivänä virtualisoinnin hyödyntäminen ei ole laitteisto- ja kustannuskysymys vaan siitä on tullut teknologia, joka on kaikkien hyödynnettävissä. Käytännössä suurin osa IT-alan yrityksistä hyödyntää virtualisointia jossain muodossa, siitä on tulossa yksi keskeisistä ympäristöjen rakennuspalikoista. Virtualisointi on muuttanut ja tulee vielä tulevaisuudessa muuttamaan näkökulmiamme siitä, kuinka voidaan hallinnoida järjestelmiä, verkkoja, tallennusta, turvallisuutta, käyttöjärjestelmiä ja sovelluksia. Tässä osiossa kerromme yleisimmistä tavoista virtualisoida (kuva 1) ja esittelemme VMwaren, Citrixin ja Microsoftin työpöytä-, esityskerros- ja sovellusvirtualisoinnin ratkaisut niiden perässä. (Ruest & Ruest 2009, XV.)



Kuva 1: Virtualisoinnin kohteita (Ruest & Ruest 2009, 26)

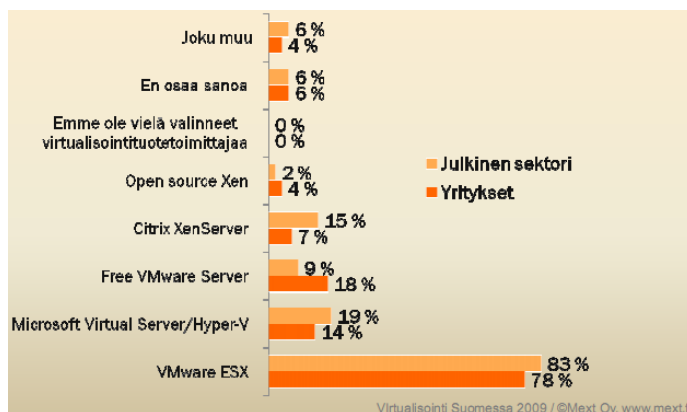
Kumppanimarkkinointipalveluita tarjoava Mext Oy suoritti syyskuussa 2009 tutkimuksen siitä, miten virtualisointia on hyödynnetty suomalaisissa yrityksissä. Selvityksessä oli mukana 208 yli 100 henkeä työllistävää yritystä. (Virtualisointi suomalaisissa organisaatioissa 2009.)

Kuten kuvasta 2 selviää, suosituin muoto on palvelinten virtualisointi, jota selvityksessä olleista yrityksistä 97 % käytti tuotantoympäristöissä. Muista ratkaisuista suosituimpia ovat tallennus- 48 % ja sovellusvirtualisointi 38 %. Tulevaisuudessa erilaiset VDI-ratkaisut ovat kasvava trendi. Tänä päivänä selvityksen mukaan sitä käyttää 10 % selvityksessä olleista yrityksistä. Kehitysympäristöissä eniten testattavina onkin sovellusvirtualisoinnin (16 %) kanssa juuri työasemien virtualisointi, jota 15 % tutkimuksessa olleista organisaatioista testaa järjestelmiinsä.



Kuva 2 Mext virtualisointi Suomessa (Virtualisointi suomalaisissa organisaatioissa 2009)

Mextin suorittamasta selvityksestä selviää (kuva 3), että palvelinten virtualisoinnissa selvästi suosituimmat tuotteet ovat VMwaren ratkaisuja. Kaupallisella ESX:llä on noin 80 % osuus ja ilmaisella Free VMware Serverilläkin kolmanneksi suurin osuus. VMwaren jälkeen Citrixin Xen-Serverin ja Microsoftin Virtual Server/Hyper-V:n osuus on selvästi vähemmän, kuitenkin molemmat ovat laajasti käytettyjä ja tunnettuja ratkaisuja.



Kuva 3: Käytetyimmän virtualisointi ratkaisut (Virtualisointi suomalaisissa organisaatioissa 2009)

2.1 Palvelinten virtualisointi

Palvelinten virtualisointi on yksi yleisimmistä ja tunnetuimmista tavoista virtualisoida. Nykypäivänä monissa datakeskuksissa palvelimet hyödyntävät vain 10-15 % niiden täydestä kapasiteetista. Toisin sanoen 85-90 % niiden kapasiteetista on käyttämättä. Vähän kuormitettu palvelin vie silti tilaa, tarvitsee jäähdytyksen, tuottaa lämpöä ja käyttää paljon sähköä. Alikuormitettu palvelin aiheuttaa korkeita käyttökustannuksia, mikä on puhtaasti resurssien haaskaamista. Palvelinten virtualisoinnilla voidaan tarttua tähän epäkohtaan ja yhdistää yksi fyysinen laitteisto tukemaan useaa virtuaalista käyttöjärjestelmää. Virtualisoinnin avulla saavutetaan säästöjä kokonaisvaltaisesti. Ylläpito ja laitteistokustannukset alenevat fyysisten laitteiden määrän pienentyessä, koska ympäristössä on vähemmän vikaantuvia laitteita, jotka vaativat huolenpitoa. Muihin hyötyihin voidaan laskea varmuuskopioinnin helpottuminen, vikatilanteista palautuminen, sekä järjestelmien siirtäminen lennossa toiseen sijaintiin. (Golden 2009, 4.)

”Virtualisoinnin avulla voidaan yksittäisessä tietokoneessa ajaa useita eri käyttöjärjestelmiä samanaikaisesti. Kaikilla näillä eri järjestelmillä on kuitenkin pääsy samaan laitteistoon, mutta jokainen toimii omassa virtuaalisessa tietokoneessaan; tämä virtuaalinen tietokone emuloi tietokoneen laitteistoa (prosessoria, muistia, näytönohjainta, verkkoliitintä, kiintolevyjä ja muita massamuisteja). Virtuaalisessa tietokoneessa suorituksessa olevat järjestelmät ovat virtuaalikoneita tai virtuaalipalvelimia (Virtual Machine, VM). Virtuaalipalvelin tallennetaan omaan tiedostoonsa (.vhd) paikallisessa tietokoneessa, verkkoasemassa, tai tallennusjärjestelmässä.” (Kivimäki 2009, 1201.)

Päällimmäisellä tasolla palvelinten virtualisoinnissa on kaksi näkökulmaa, ohjelmistopohjainen ja rautapohjainen virtualisointi. Ohjelmistopohjaisessa ratkaisussa virtualisoitua käyttöjärjestelmää ajetaan virtualisointiohjelman (VM monitor) avulla isäntäkäyttöjärjestelmän (host) päällä, kuten kuvasta 4 selviää. Isäntäkäyttöjärjestelmä hallitsee fyysisen laitteiston ja sovelusten välistä tiedonsiirtoa, sekä VM monitoria. Virtuaalikoneiden luonti ja niiden pääsy laitteistoon tapahtuu VM monitorin kautta. Vieraskoneen (guest) luomisessa tehdään koneen asetukset sisältävä tiedosto, jonka avulla virtuaalikone käynnistetään. (Kivimäki 2009, 1201.)

Rautapohjaisessa ratkaisussa virtuaalikoneita suoritetaan ohuella kerroksella erityistä käyttöjärjestelmäohjelmistoa, joka keskustelee suoraan palvelimen laitteiston kanssa ja korvaa perinteisen isäntäkäyttöjärjestelmän. Rautapohjaisessa virtualisoinnissa käytettävää ohjelmistoa kutsutaan hypervisoriksi. Ohjelmiston tarkoituksena on näyttää isäntäkoneen laitteisto virtualisoiduille käyttöjärjestelmille. Hypervisorin avulla luodaan vieraskoneet ja se hallinnoi näiden pääsyä isäntäkoneen (host) prosessoriin, keskusmuistiin, sekä käsittelee syöttö- ja tulostustoimintoja, sekä tiedonsiirtoa virtuaalikoneiden ja fyysisen laitteiston välillä. Hyper-

visorin etuna perinteisiin VM monitor -tyyppisiin ratkaisuihin on parempi suorituskyky ja luotettavuus, koska se ei sisällä täyden käyttöjärjestelmän kaikkia ominaisuuksia vaan se on tehty nimenomaan virtualisointikäyttöä varten. (Kivimäki 2009, 1201.)

Ohjelmistopohjaista virtualisointia käytetään yleensä testi- ja kehitysympäristöissä. Tämä malli soveltuu oheisiin tarkoituksiin mainiosti, koska se on yksinkertainen ja usein myös ilmainen tapa. Esimerkkejä ilmaisista ohjelmistopohjaisista ratkaisuista ovat Microsoft Virtual PC, VMware Player ja VMware Virtual Server. Kaupallisista versioista mainittakoon VMware Workstation ja Microsoft Virtual Server 2005. Haittapuolina tekniikassa on sen resurssien kulutus. Malli perustuu käyttöjärjestelmän päälle asennettavaan virtualisointikerrokseen, joka emuloi fyysistä laitteistoa. Näin ollen palvelimen resursseja kuluttavat isäntäkäyttöjärjestelmä ja sen päälle asennetut virtuaalipalvelimet, joten osa järjestelmän resursseista menee hukkaan. Toisaalta virtuaalisointiohjelmiston asentaminen on hyvin yksinkertaista ja nopeaa, mikä sopii hyvin testiympäristöihin. Ohjelmistopohjainen virtualisointi soveltuu ainoastaan niihin käyttökohteisiin, joissa voidaan hyväksyä matalan palvelutason kriteerit. Ohjelmistopohjaisessa mallissa isäntäkäyttöjärjestelmän uudelleenkäynnistykset ja muut huoltotoimenpiteet aiheuttavat palvelukatkoja koko järjestelmän laajuudessa. Ohjelmistopohjaisen virtualisoinnin rajoitteista johtuen tuotantoympäristöissä käytetään rautapohjaista virtualisointia (bare metal). (Ruest & Ruest 2009, 32-33.)



Kuva 4: Ohjelmistopohjainen virtualisointi

Rautapohjaisessa (bare metal) mallissa hyödynnetään laitteiston päälle sijoitettavaa virtualisointikerrosta (hypervisor), mikä ei vaadi isäntäkäyttöjärjestelmää toimiakseen (kuva 5). Bare metal -virtualisoinnilla tarkoitetaan arkkitehtuuria, jossa simuloidaan täysin alla olevaa laitteistoa. Käytännössä nopeus on lähes samaa luokkaa kuin fyysistä palvelinta käytettäessä. Hypervisor voi olla valmiiksi asennettuna palvelimen laitteistoon tai se voidaan asentaa erikseen. Kerroksen päällä ajettavat koneet vievät vain pienen osan fyysisen laitteen resursseista. Tämä mahdollistaa useampien palvelimien suorittamisen samalla laitteistolla. Alustan vi-

kasietoisuus paranee, koska alla ei ole erikseen ylläpidettävää käyttöjärjestelmää. Toistaiseksi rautapohjainen virtualisointi on paras tapa toteuttaa virtualisointia tuotantoympäristöissä. Tämän tyyppisessä ratkaisussa etuna on tietoturvallisuus sekä että asennettavat käyttöjärjestelmät eivät vaadi muutoksia. Jokainen kone on täysin eristetty toisistaan ja ne eivät näy toisilleen. Huonoina puolina ovat raudan ja ohjelmiston laitteistovaatimukset. Esimerkkejä rautapohjaisista virtualisointialustoista ovat VMware ESX/ESXi ja Microsoft Hyper-V Server. (Ruest & Ruest 2009, 33.)



Kuva 5: Vieraskoneet suoraan virtualisointikerroksen päällä

Palvelinten virtualisointia voidaan käsitellä monella tasolla ja käytettävästä alustasta riippuen on olemassa erilaisia arkkitehtuureja, joilla sitä voidaan toteuttaa. Seuraavissa kappaleissa käsittelemme lyhyesti para- ja natiivivirtualisointia, jotka ovat yleisimpiä arkkitehtuureja ylempänä esitellyn bare metal vaihtoehdon lisäksi (full virtualization).

Paravirtualisointi tarjoaa osittaisen simulaation alla olevasta laitteistosta käyttöjärjestelmälle. Paravirtualisoinnin kerrokset näkyvät kuvassa 6. Useimmat laitteiston ominaisuudet toimivat emuloituina. Pääominaisuutena on osoiteavaruuden virtualisointi, tämä mahdollistaa jokaiselle virtuaalikoneelle oman uniikin osoiteavaruuden. Paravirtualisointi on helpompi toteuttaa kuin täysivirtualisointi, kun täyttä laitteistotukea ei ole saatavilla. Paravirtualisoitu kone on yleensä tehokkain verkolle ja levy I/O:lle. Huonoina puolena ovat että käyttöjärjestelmät paravirtualisoiduilla koneilla vaativat merkittäviä muutoksia. Heikkoutena on myös, etteivät virtuaaliset koneet ole hyvin taaksepäin yhteensopivia, eivätkä kovin siirreltäviä. Paravirtualisointi vaatii pääsyn vieraskäyttöjärjestelmän lähdekoodiin. Tämä on mahdollista vain avoimen lähdekoodin käyttöjärjestelmille, kuten Linux. Esimerkkinä paravirtualisointia tukevista tuotteista on avoimeen lähdekoodiin perustuva Citrixin XenServer. (Dittner & Rule 2007, 22.)



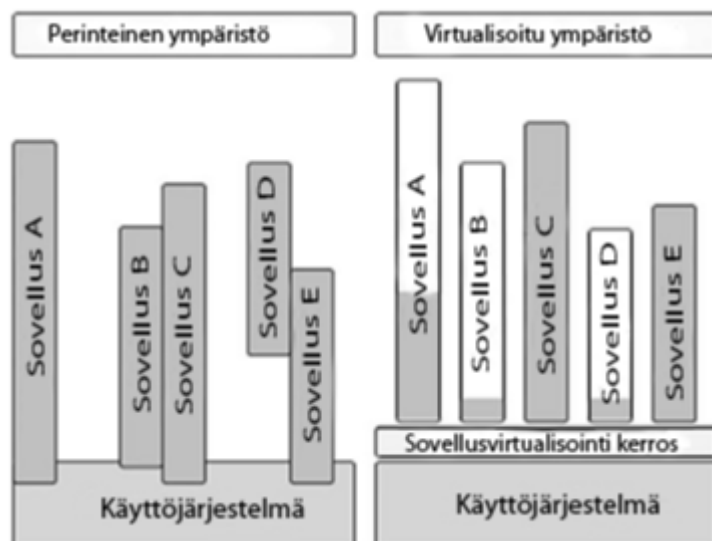
Kuva 6 Paravirtualisointi kerrokset

Natiivivirtualisointi on uusin x86-alustalle olevista virtualisointiteknologioista. Teknologia on tunnettu myös nimellä hybridivirtualisointi. Se on yhdistelmä täysvirtualisoinnista ja paravirtualisoinnista täydennettynä I/O kiihdytysteknologioilla. Natiivivirtualisointi vaatii prosessorilta laitteisto-ohjatun kiihdytyksen tuen ja hyödyntää x86-pohjaista laitteistovirtualisointia, kuten Intel VT (Intel) ja AMD-V (AMD). Vieraskäyttöjärjestelmä näkee fyysisen prosessorin suoraan ja näin toimii huomattavasti tehokkaammin. Vieraskäyttöjärjestelmä voidaan asentaa ilman siihen tehtyjä huomattavia muutoksia. (Dittner & Rule 2007, 51-52.)

2.2 Sovellusvirtualisointi

Sovellusten virtualisointi on yksi nopeimmin kasvava virtualisointitapa. Sen ajatuksena rikkoa ohjelmiston ja käyttöjärjestelmän välinen yhteys (Kuva 7), tällöin ohjelmistojen keskeiset ongelmatilanteet jäävät pois. Sovellusvirtualisointi tuo merkittäviä etuja järjestelmän ylläpitäjille ja suunnittelijoille. Sovellusten virtualisoinnissa ohjelmien väliset ristiriidat poistuvat, sekä käyttäjille pystytään tarjoamaan joustavammin heidän tarvitsemansa ohjelmat. Yksittäiset sovellukset eivät häiritse millään tavoin muita sovelluksia tai käyttöjärjestelmää, vaan ovat jokainen toisiltaan näkymättömissä, kuten kuviosta 6 selviää.

Ylläpidon kannalta sovellusten hallinnoiminen helpottuu, kun paketoitujen ohjelmien voidaan ottaa käyttöön ja pois käytöstä keskitetysti sekä käyttäjäkohtaisesti. Mikäli tulee tarvetta päivittää tai muuttaa sovelluksen asetuksia ylläpitäjän ei tarvitse muuttaa kuin yhden paketin asetuksia, jolloin kaikki käyttäjät saavat suoraan päivitetyn ohjelmiston automaattisesti käyttöönsä. Suurimpia toimijoita sovellusvirtualisoinnin ratkaisuihin ovat Microsoft App-V, Citrix XenApp ja VMware ThinApp. Pienemmistä mainittakoon InstallFree ja Symantec. (Dittner & Rule 2007, 25-26; Ruest & Ruest 2009, 33.)

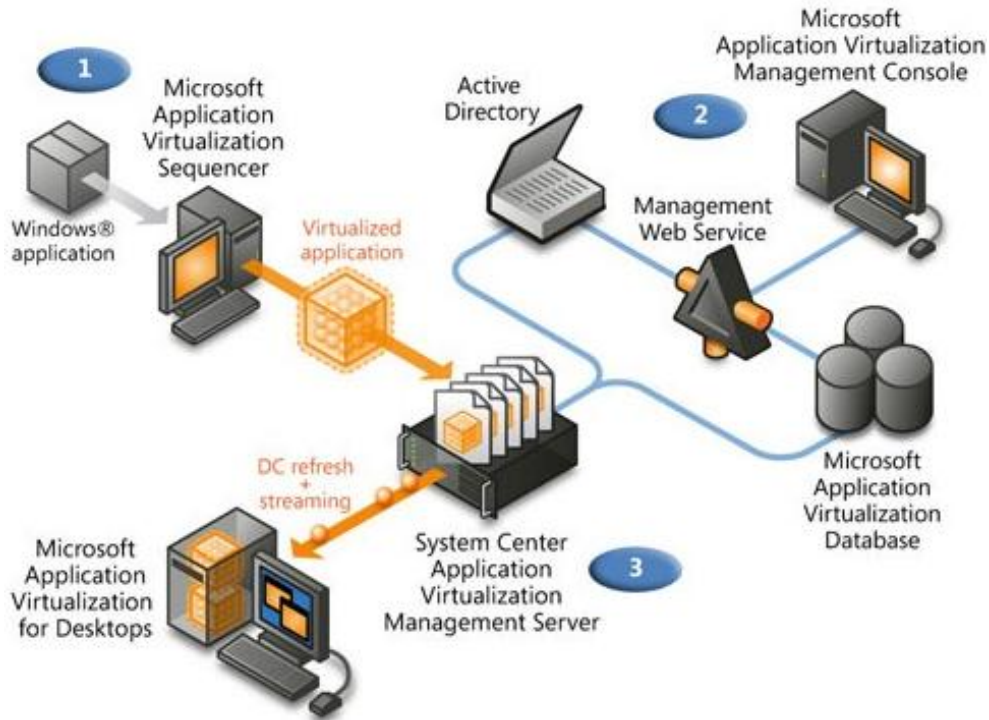


Kuva 7: Perinteisen ja virtualisoidun sovellusten riippuvuudet toisistaan

2.2.1 Microsoft App-V

Microsoftin tarjoama sovellusvirtualisointi tunnetaan nimellä Application Virtualization (aiemmin SoftGrid), jonka uusin versio on 4.6. Ylläpidollisesti App-V tuo selviä etuja keskitetyssä hallinnassa ja sovelluksen elinkaaren seurannassa. Uusin versio toi mukanaan merkittäviä uudistuksia Microsoftin sovellusvirtualisointiratkaisuun kuten tuen 64 bittisille ohjelmitoille ja käyttöjärjestelmille. Microsoft Office 2010 ja App-V 4.6 on suunniteltu toimivan saumattomasti yhdessä. Esimerkiksi aikaisempia Office versioita on ollut hankalampi virtualisoida niiden hajautetun rakenteen ja keskinäisten yhteyksien vuoksi. (Desktop Virtualization 2010; Application Virtualization Whitepapers 2010.)

App-V tarjoaa sovellukset työpöydille, palvelimille ja kannettaville tietokoneille. Käyttäjälle tulee näkyviin vain ne sovellukset joihin hänellä on oikeus ja hänellä on aina uusin versio käytettävissään, kun kone automaattisesti avaa palvelimelta oikean version sovelluksesta. App-V mahdollistaa myös sovellusten käyttämisen offline-tilassa, kun koneella ei ole yhteyttä verkkoon ja palvelimeen josta sovellus käyttäjälle lähetetään. Kuvassa 8 on näkyvissä App-V:n rakennetta ja osakomponentteja. (Application Virtualization Solutions Overview and Feature Compare Matrix 2008, 17.)

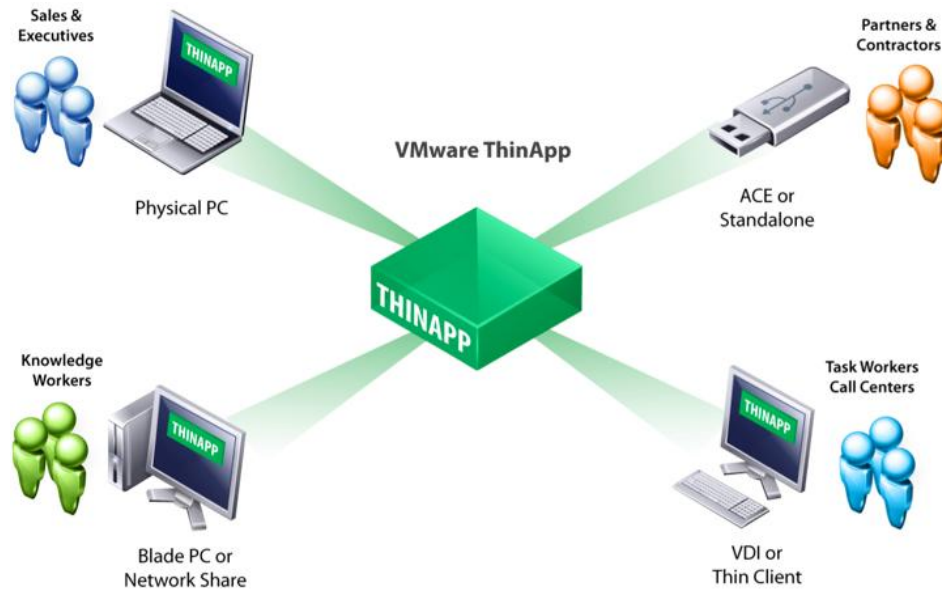


Kuva 8: Microsoft App-V:n osakomponentit (Centralized Management 2010)

2.2.2 VMware ThinApp

VMwaren sovellusvirtualisointiratkaisu ThinApp:ssa sovellukset (aiemmin Thinstall) toimivat omilla hiekkalaatikoissaan eristettynä muusta käyttöjärjestelmästä. ThinApp eroaa muista sovellusvirtualisointiratkaisuista siitä miten sovellukset toimitetaan käyttäjille. ThinApp:n avulla ohjelmisto voidaan paketoita yhteen tiedostoon, joka mahdollistaa ohjelmistojen joustavan jakelun ilman erillistä palvelinta tai työpöydälle asennettavaa asiakasohjelmaa (kuva 9). Tällä ratkaisulla ohjelmat voidaan toimittaa käyttäjille suoraan palvelimen verkkojaosta käsin tai kopioida heidän työpöydilleen. Ohjelmat voidaan käynnistää myös verkkojaosta käyttämällä pikakuvaketta, mikä viittaa palvelimilla olevaan sovelluspakettiin. ThinApp:lla luotuja sovelluksia pystytään ajamaan user-tason oikeuksilla, ilman että käyttöjärjestelmään tulee mitään asennuksista aiheutuvia muutoksia. Sovellus voidaan myös tehdä ajettavaksi USB-muistilta, tällöin ThinApp sovellus ohjaa rekisteri ja tiedostojärjestelmään tarkoitetut muutokset pc:n sijasta siirrettävälle medialle. (VMware ThinApp intro 2008, 3-4.)

ThinApp:n uusin versio on 4.5 joka toi mukanaan uudistuksina mahdollisuuden käyttää Windows 7:lla virtualisoituja sovelluksia, jotka ovat tehty Windows XP:llä tai Vistalla. Muita suuria uudistuksia on virtualisoitujen pakettien helpompi päivittäminen uudemmalle ThinApp versiolle sopivaksi. (VMware ThinApp 2010.)

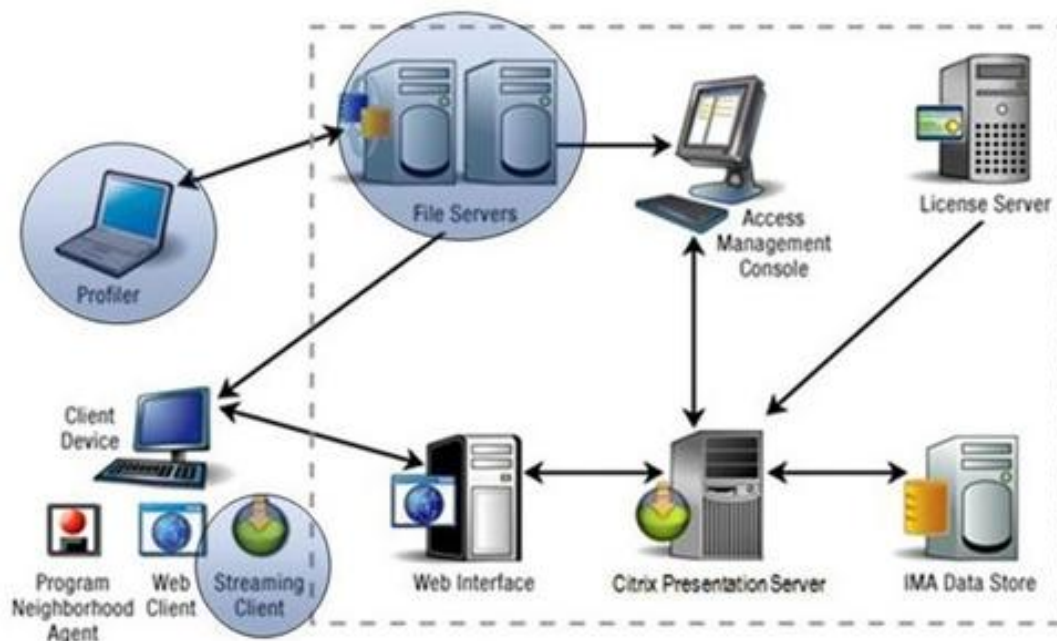


Kuva 9: VMware ThinApp sovellusten jakelu käyttäjille (VMware ThinApp made simple 2010)

2.2.3 Citrix XenApp

Citrixin XenApp yhdistää esityskerroksen ja sovellusvirtualisoinnin yhteen tuotteeseen. Tuotteen nimi muuttui vuonna 2008 Citrix Presentation Serveristä XenApp:ksi (Xen = Virtualization, App = Application), koska haluttiin nimen kuvastavan paremmin tuotteen ydintä, sovellusvirtualisointia. XenApp:n on tarkoitus tarjota sovellukset käyttäjille keskitetyltä palvelimelta, siten että käyttäjä näkisi sovellukset kuin päätelaitteelle paikallisesti asennetut. Käyttäjän päätelaitteelle voidaan toimittaa yksittäiset sovellukset palvelimelta tai esityskerrosvirtualisoinnilla sessiopohjaisen työpöydän avulla. Virtuaalisten työpöytien toimitus käyttäjälle on perusteltua, varsinkin jos suurin osa sovelluksista tarjotaan XenApp palvelimelta ja käytetään pääsääntöisesti kevytpäätteitä. Citrix XenApp ympäristö on kuvattu kuvassa 10. Uusin versio XenApp 6 (työn kirjoitus hetkellä) ilmestyi 6. Maaliskuuta 2010. Uuden version myötä on mahdollista käyttää Windows-sovelluksia Mac-tietokoneilla ja älypuhelimilla. Uudistuksena tuli myös parannuksia erityisesti Microsoft Windows Server 2008r2:lle sallien yhteiskäytön Microsoftin App-V:n kanssa. (Casselman, Kaplan & Reeser 2009, 103; Introducing Citrix XenApp 2010.)

Citrixin XenApp on saatavilla neljällä eri versiolla, näin on pyritty tarjoamaan jokaisen organisaation tarpeita vastaava paketti. Pk-yrityksen tarpeisiin on suunniteltu avaimet käteen ratkaisu, XenApp Fundamentals. Muina versiona on XenApp Advanced ja Enterprise sekä kaikkein kattavin versio XenApp Platinum. (XenApp editions 2009.)

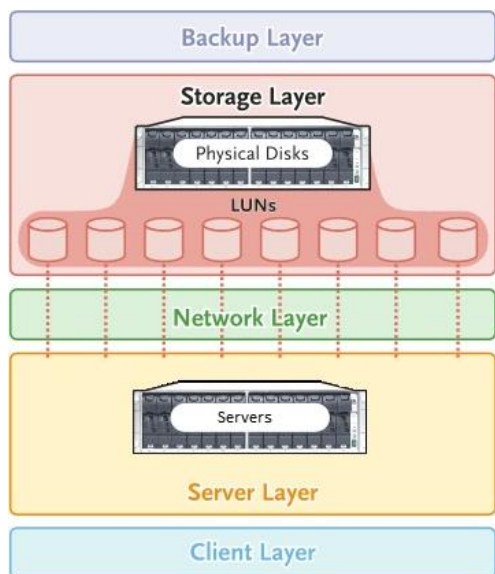


Kuva 10: Kuvauk Citrix XenApp ympäristöstä (Citrix XenApp 2010)

2.3 Tallennusvirtualisointi

Tallennusvirtualisointia käytetään kun halutaan yhdistää useiden fyysisten laitteiden tallennustilat näkymään yhtenä varastona. Varastointi voidaan suorittaa eri muodoin kuten DAS (direct attached storage), NAS (network attached storage) tai SAN (storage area networks) ja ne voidaan yhdistää erilaisin protokollin, esim. FibreChannel, Internet SCSI (iSCSI). Tallennusvirtualisointi on hyvä lisä palvelinvirtualisoinnin rinnalle, jolloin infrastruktuurin tallennustilat saadaan hallintaan. (Ruest & 2009, 27.)

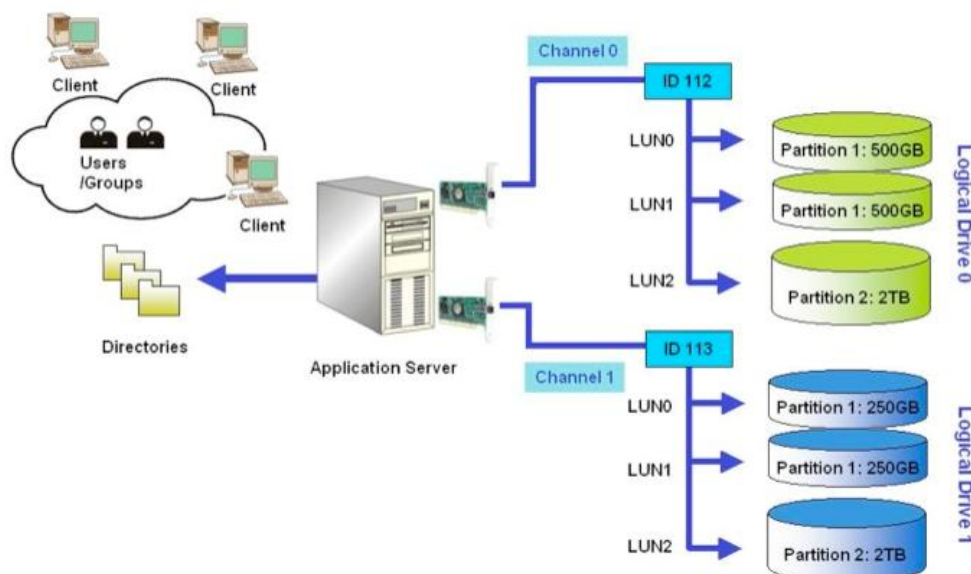
Yksinkertaisimmillaan tallennuksen virtualisointi koostuu useista fyysisistä levyasemista, jotka esitetään palvelimelle yhtenä kokonaisuutena (RAID). Tällaista kokoonpanoa voidaan pitää virtualisoituna, koska kaikki asemat ovat käytössä yhden loogisen aseman kautta. Todellisuudessa asema koostuu useista levyistä, jotka ovat samanaikaisesti käytössä. Tallennustilaa jaetaan palvelimien kesken yhdestä varastokomponentista (SAN). Varastokomponenttia käyttävät kohdejärjestelmät luulevat käyttävänsä sille määritettyä omaa fyysistä asemaa. Tallennusjärjestelmien ylläpitäjät vain määrittävät halutun määrän virtuaalista varastotilaa (LUN) kohdepalvelimille (kuva 11). Nykyiset SAN-järjestelmät voidaan liittää osaksi palvelinympäristöä ilman käyttöjärjestelmien uudelleenohjelmointia, mikä nopeuttaa käyttöönottoa. (Dittner & Rule 2007, 24-25.)



Kuva 11: Tallennusvirtualisoinnin kerroksia (Storage layer 2008.)

Uudenaikaiset levyjärjestelmät vaativat myös nopeat verkkoyhteydet voidakseen taata edistyneiden ominaisuuksien toiminnan mahdollisimman tehokkaasti esim. Live Migration ja VMware VMotion, joilla voidaan siirtää käynnissä oleva virtuaalikone palvelimelta toiselle ilman katkosta toiminnassa. (Dittner & Rule 2007, 24-25).

LUN (Logical Unit Number) on SCSI-tiedonsiirtoprotokollaan tarvittava yksilöllinen tunnistenumero(osoite) levynosiolle tai itse levyille (kuva 12). LUN tunnistetta tarvitaan esimerkiksi kun RAID-pakasta halutaan ottaa käyttöön jokin levyosio, eikä kokonaista levyä. LUN yhdistää siis käyttäjän tai sovelluksen tiedot oikeaan paikkaan tallennusjärjestelmässä. LUN Masking on toiminto, jolla pystytään rajaamaan mitä levyjä palvelin näkee tallennusjärjestelmästä. LUN Maskin on erityisen tärkeä Windows-pohjaisilla palvelimilla, sillä ne yrittävät nimetä verkossaan kaikki vapaat LUNit. Tämä saattaa aiheuttaa tiedostojen hävikkiä ja sen ettei muut käyttöjärjestelmät näe luotuja LUNeja. (Long 2006, 111; Boyles 2010, 446.)



Kuva 12: LUN näkymä tallennus järjestelmässä (LUN, 2009)

2.4 Verkon virtualisointi

Verkon virtualisointi auttaa kontrolloimaan käytössä olevaa kaistaa hajauttamalla sen yksittäisiksi kanaviksi. Tämä mahdollistaa useamman itsenäisen verkon käyttämisen yhdestä fyysisestä verkosta. Yksittäiset kanavat voidaan määrittää tiettyjen resurssien käyttöön kuten erilaisiksi projektiverkoiksi. Jokainen oma verkko on eristettynä muista ja on näin hyvin suojattu muista sisäverkoista estäen ulkopuolisten siihen liittymisen. Ylläpidon kannalta tämä tuo huomattavia etuja, kun voidaan tarjota erilaisia verkkoja eri käyttötarkoituksiin. Yksinkertaisin esimerkki verkon virtualisoinnista on virtual local area network (VLAN), mikä luo loogisen erottelun fyysisessä verkossa. Palvelinten virtualisoinnissa tuotteet mahdollistavat itsessään virtuaalisten verkkokerrosten (vSwitch) luomisen. Verkkokerroksilla voidaan luoda suojaverkkoja sekä eristää virtuaalikoneet toisistaan näkymättömiksi. (Ruest & Ruest 2009, 27.)

Virtual Private Network (VPN) on yksityinen tietoliikenneverkko, jonka avulla voidaan välittää luottamuksellista tietoa turvallisesti julkisen verkon lävitse. VPN:n avulla luodaan suojattu tunneli ja sitä hyödynnetään, kun halutaan siirtää tietoa suojaamattoman verkon yli esimerkiksi internetin läpi. VPN-yhteyksiä käytetään myös yritysten etäyhteyksien luomiseen käyttäjän ja työpaikan välille. Etäyhteyden luomiseen tarvitaan usein erillinen ohjelma. Yhteyden muodostamisen jälkeen verkko näyttää käyttäjälle samalla tavalla kuin hän olisi kytkeytyneenä paikallisesti yrityksen verkkoon, vaatimatta mitään muutoksia käyttöjärjestelmään tai verkon asetuksiin. (Dittner & Rule 2007, 25.)

2.5 Työpöydän virtualisointi (VDI)

Työpöydän virtualisoinnilla tarkoitetaan sitä, että käyttäjän käyttöjärjestelmä (guest) sijaitsee konesalissa palvelimella paikallisen asennuksen sijasta. Käyttäjälle välitetään näyttökuvaa, sekä hiiren ja näppäimistön painallukset verkon yli. Virtuaalisiin työpöytäryhmiin on mahdollista luoda kahdenlaisia työpöytiä, joko henkilökohtaisia tai poolityyppisiä. (VMware Työasema virtualisointi 2009.)

Henkilökohtaisessa (persistent) työpöytäratkaisussa käyttäjä saa aina kirjautuessaan käyttöönsä saman työpöydän, jolta on aikaisemmin kirjautunut ulos. Tällainen työpöytäratkaisu soveltuu käytettäväksi esimerkiksi tehokäyttäjälle, jonka työpöytää tulee muuttaa enemmän käyttäjäkohtaiseksi. Ratkaisu soveltuu myös hyvin ympäristöihin, joissa ei ole varaa tietojen menettämislle. Kaikki data sijaitsee palvelimella, joten koneen varastaminen tai kovalevyn rikkoutuminen ei aiheuta tietojen menettämistä. (VMware Työasema virtualisointi 2009.)

Poolityyppisessä ratkaisussa kaikilla käyttäjillä on käytössään yhden mallin mukaiset työpöydät, jotka palautuvat uloskirjautumisen yhteydessä takaisin pooliin toisten käytettäväksi. Tällainen malli soveltuu erinomaisesti kohteisiin, jossa suurelle käyttäjäryhmälle voidaan tarjota samanlaista mallia. Koulut ja kirjastot ovat esimerkkejä tämänkaltaisista kohteista. (VMware Työasema virtualisointi 2009.)

2.5.1 Microsoft VDI

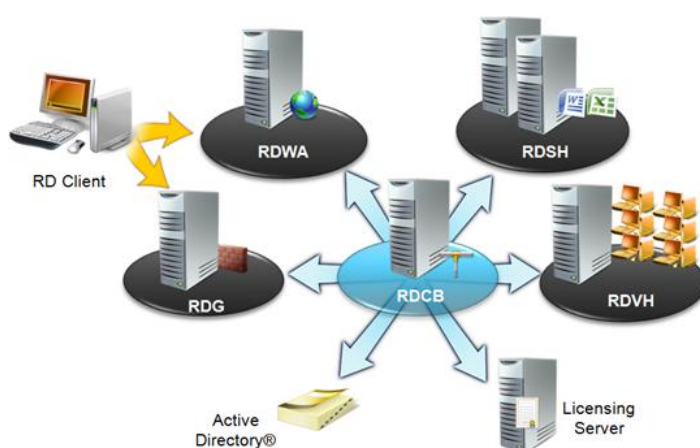
Microsoft on maailman johtavin ohjelmisto, palvelu ja ratkaisuiden toimittaja. Microsoft perustettiin vuonna 1975, pääkonttori sijaitsee Redmondissa, Washingtonissa. Työntekijöitä Microsoftilla on yli 88 000 ympäri maailmaa. Microsoftin kuuluisin tuote on Windows käyttöjärjestelmät. Muista merkittävimmistä tuotteista mainittakoon Microsoft Office, Windows Server käyttöjärjestelmät sekä System Center -ratkaisut. Uusinta kasvua Microsoft hakee mobiilipalveluista ja viihdejärjestelmistä (esim. Xbox ja Zune), sekä pilvipalveluista (cloud computing). (Facts About Microsoft 2010.)

Microsoftin uusin palvelinkäyttöjärjestelmä Windows Server 2008 R2 perustuu aiemmin julkaistuun Windows Server 2008:n. Release 2 version mukana tulee tuki työpöytien virtualisointiin (VDI) ja uudistuksia Hyper-V virtualisointitekologiaan. Uuden version myötä entisten terminaalipalvelujen nimet tunnetaan nimeltä RDS (Remote Desktop Services). Kuvassa 13 on kuvattu muutokset.

WINDOWS SERVER 2008 R2 NAME	WINDOWS SERVER 2008 NAME
Remote Desktop Services	Terminal Services
Remote Desktop Session Host (RD Session Host)	Terminal Server
Remote Desktop Virtualization Host (RD Virtualization Host)	No equivalent
Remote Desktop Connection Broker (RD Connection Broker)	Terminal Services Session Broker
Remote Desktop Web Access (RD Web Access)	Terminal Services Web Access
RemoteApp	TS RemoteApp
Remote Desktop Gateway	TS Gateway
Remote Desktop Client Access License (RD CAL)	TS CAL

Kuva 13: Remote Desktop Servicen roolipalvelut (Russel & Zacker 2010, 45-46)

Microsoftin VDI toteutus voidaan tehdä vain käyttämällä Microsoftin virtualisointi alustaa, Hyper-V:tä. Hyper-V:n käyttöönotto edellyttää Remote Desktop Virtualization Host roolia, joka on yksi Remote Desktop Servicen rooleista. RDVH:n tehtävänä on tarjota HyperV:n avulla luotuja virtuaalisia koneita käyttäjälle. RD Virtualization Host voidaan konfiguroida niin, että jokainen käyttäjä saa yhden oman virtuaalisen koneen tai vapaan työpöydän virtuaalikoneiden varannosta. Tämä määrittely tehdään RD Connection Broker palvelimella. Mikäli haluttu virtuaalikone on poissa päältä RDVH käynnistää sen kun saa käskyn RDCB:ltä. Kuvassa 14 näkyy Microsoft VDI:n komponentteja, jotka ovat esiteltyinä sen jälkeen. (Microsoft vdi overview 2009.)



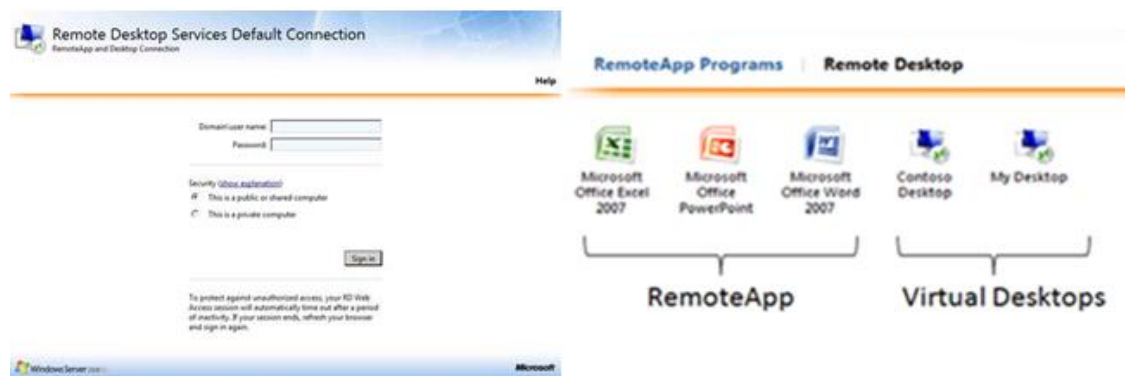
Kuva 14: Microsoft VDI komponentteja (RD Virtualization Host, 2010)

RD Connection Broker, aikaisemmin nimellä Terminal Services Session Broker, toimii tietojen välittäjänä päätelaitteen ja RDVH:n välillä varmistamaan yhteyden luomisen. Connection

Broker valmistele etätyöpöydän RDVH:n kanssa yhdistäen käyttäjän joko omalle koneelle tai yhdelle koneelle varannosta. Käyttäjän ottaessa yhteyttä koneelle joka on varannossa RDCB tarkistaa ensin onko mahdollisesti käyttäjän aikaisempi istunto katkennut. Mikäli yhteys on katkennut, käyttäjä yhdistetään takaisin aikaisempaan istuntoon. Täysin uuden istunnon alkaessa RD Connection Broker tarkistaa onko varannossa vapaana olevaa konetta toimitettavaksi käyttäjälle. (Microsoft vdi overview 2009.)

RD Session Host palvelinta käytetään ohjelmien, verkkoresurssien ja sessiopohjaisten työpöytien jakamiseen käyttäjille. RDSH-palvelinta voidaan verrata aikaisempaan Terminal Serveriin. Session Host palvelimen roolina on tässä ympäristössä toimia ainoastaan virtuaalikoneiden ohjauksessa eikä perinteisenä terminaalipalvelimenä. Server 2008R2:ssa RD Session Host rooli voidaan määritellä neljällä eri tavalla riippuen käyttötarkoituksesta. Määrittelemällä RDSH-palvelin ”virtual machine redirection” tilaan käyttäjien kirjautumistapa muutetaan sallimaan uudelleen yhdistämiset, mutta estämään uudet kirjautumiset. Asennuksen seurauksena palvelinta ei voida käyttää enää terminaalipalvelimenä. Microsoftin ratkaisussa käytetään taaksepäin yhteensopivuussyistä erillistä RDSH-palvelinta pelkän Connection Brokerin sijasta. Tällä ratkaisulla taataan RDP-clienttien toimivuus Windows Server2008R2 kanssa versiosta 5.2 alkaen. (RD Session Host 2010.)

RD Web Access avulla käyttäjät voivat käyttää etänä sovelluksia tai virtuaalisia työpöytiä internet-selaimen kautta. Selainta käytettäessä käyttäjä näkee kaikki sovellukset ja virtuaaliset työpöydät, joihin hänellä on käyttöoikeus. Windows 7 ja Server 2008 R2 uutena ominaisuutena ohjelmat voidaan lisätä käynnistä-valikkoon hyödyntämällä RD Web Access-palvelimen uutta RemoteApp and Desktop Connection Feed (RAD) toimintoa, joka on RSS-syötteen tapainen teknologia. Toiminto otetaan käyttöön lisäämällä RD Web Access -palvelimen osoite RemoteApp and Desktop Connections asetuksiin. Tarjotut ohjelmat päivittyvät automaattisesti käynnistä valikoihin, eikä niihin tarvitse kirjautua enää erikseen. Web Access tarjoaa myös vanhemmille päätekoneille väylän virtuaalisiin työpöytiin (Windows XP), kuvassa 15 on näkyvä kirjautuessa selaimen kautta. Web Access kertoo ainoastaan listan käyttäjille tarjottavista ohjelmista ja työpöydistä, joten sille on määriteltävä palvelin, jolta se noutaa tarvittavat tiedot. Lähde voidaan määritellä kahdella eri tavalla, joko RDSH jakamaan sessiopohjaisia työpöytiä ja ohjelmia tai Connection Broker tarjoamaan virtuaalisia työpöytiä. (RD Web Access 2010.)



Kuva 15: Kirjautuminen Web Access:n avulla tarjolla oleviin ohjelmiin ja työpöytiin.

Windows Server 2008 R2 ja Windows 7 myötä RDP-protokolla on saanut paljon uusia ominaisuuksia. Remote Desktop Client (RDC) 7.0 on saatavilla myös Windows XP Service Pack 3 ja Windows Vista Service Pack 1 käyttöjärjestelmille, mutta kaikista uusista ominaisuuksista pääsee hyötymään Windows 7 ja Server 2008 R2 yhdistelmällä. Kuvassa 16 selviää mitkä käyttökokemukseen vaikuttavat ominaisuudet ovat käytössä, kun asiakaskoneena on Windows 7 Enterprise, R2 tai XP(sp3) ja otetaan yhteys Windows Server 2008 R2 palvelimen. (Remote Desktop Connection 7.)

Remote Desktop Protocol 7:n mukana tulleita etäkäyttökokemusta parantavia ominaisuuksia:

- Multimedia redirectionin avulla mediatiedostot voidaan lähettää alkuperäisessä muodossa päätelaitteen raudalle purettavaksi ja renderöitäväksi.
- Multi monitor support tukee RDP 7:n myötä 16:sta näyttöä melkein millä tahansa resoluutiolla ja ne käyttäytyvät etätyöpöydillä samalla tavalla kuin paikallisesti käytettynä.
- Audio input and recording tukee päätelaitteeseen asennettuja mikrofoneja, mahdollistaa Voice over IP -sovellukset ja sitä voidaan hyödyntää esimerkiksi puheentunnistuksessa etätyöpöydillä.
- Windows Aero Glass - käyttöliittymän tuen avulla RDSH-palvelimelta saadaan samanlainen näkymä etäyhteydessä kuin paikallisen koneen istunnossa.
- Bitmap accelerationin kautta osa rikkaasta mediasta (Silverlight, Flash) ja 3D-sisältö, voidaan renderöidä isännällä ja lähettää päätelaitteelle bittikarttoina.
- Improved audio/video synchronization tähtää parempaan äänen ja videon synkronisointiin useimmissa tilanteissa.

(Technical Overview of Windows Server 2009, 13.)

Käyttökokemukseen vaikuttavat ominaisuudet	Win 7 / R2	XP sp3
Windows Media Player:n uudelleenohjaus	Kyllä	Kyllä
Kaksisuuntainen audio	Kyllä	Kyllä
Usean näytön tuki	Kyllä	Kyllä
Aero Glass-tuki	Kyllä *	Ei
Bitmap Acceleration	Kyllä	Kyllä
Kielipalkin telakointi	Kyllä	Ei
Helppo tulostus	Kyllä	Kyllä

* Ei käytettävissä yhdessä usean näytön tuen kanssa.

Kuva 16: RDP 7.0 käyttökokemusten vertailu (Remote Desktop Connection 7)

2.5.2 VMware View 4

VMware on perustettu 1998 ja sen pääkonttori sijaitsee Palo Altossa, Kaliforniassa. VMware työllistää yli 8200 työntekijää ja sen vuoden 2009 liikevaihto oli 2 miljardia dollaria. Se on viidenneksi suurin ohjelmistoyritys. VMwarella on yli 190 000 asiakasta ja 25 000 liikekumppania ja 51 000 sertifioitua asiantuntijaa. VMware on yksi suurimmista virtuaali- ja pilvipalveluiden tuottajista maailmanlaajuisesti. (VMware Overview 2010.)

vSphere on VMwaren pilvilaskentajärjestelmä, jolla voidaan muuttaa datakeskukset virtuaaliseksi pilvilaskentajärjestelmäksi. vSphere virtualisoi ja yhdistää fyysisten laitteistojen resurssit useista järjestelmistä ja tarjoaa niistä virtuaaliset resurssit datakeskukselle. Pilvilaskentajärjestelmänä vSphere hallinnoi laajalti eri palvelimien komponentteja infrastruktuurissa (kuten prosessorit, tallennustilan ja verkon), näyttäen ne yhtenäisenä dynaamisena kokonaisuutena. VMware vSphere voidaan jakaa seuraaviin komponenttikerroksiin; infrastruktuuripalveluihin, sovelluspalveluihin sekä vCenter palvelimeen ja clientteihin. Alla on esiteltynä komponentit lyhyesti. (VMware vSphere 2009.)

vSpheren infrastruktuuripalvelut voidaan jakaa kolmeen osaan; vCompute, vStorage ja vNetwork. vCompute yhdistää erillisten palvelimien tehot ja tarjoaa niitä sovelluksille. vStoragesa teknologiat mahdollistavat virtualisoitujen tallennusjärjestelmien käytön ja hallinnan. vNetwork palvelu mahdollistaa verkon virtualisoimisen pilvilaskentajärjestelmässä. Sovelluspalveluihin kuuluvat palvelut takaavat sovelluksille saatavuuden, turvallisuuden ja skaalautuvuuden. vCenter tarjoaa yhden valvontapisteen datakeskukselle. Tärkeimpinä ja olennaisimpina rooleina on käytön valvonta, suorituskyvyn seuranta ja konfigurointi. Clienttien avulla käyttäjät voivat ottaa yhteyden vSpheren datakeskukseen. Clienttina voi olla päätelaitteelle

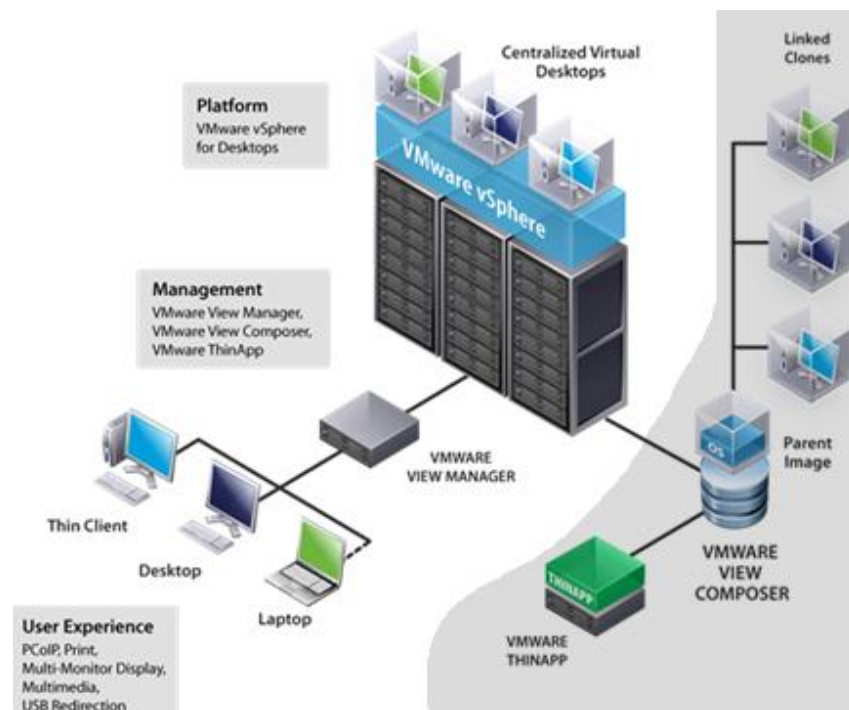
asennettua vSphere Client tai yhteys internet-selaimen kautta käyttäen Web Access - portaalia. (VMware vSphere 2009.)

vSphere on saatavilla neljällä eri versiolla; Standard, Advanced, Enterprise ja Enterprise Plus. vSphere sisältää mm. seuraavat tuotteet; ESX tai ESXi virtualisointialustan, vCenter Server hallintapalvelimen ja vShield Zones, vMotion , Storage VMotion ominaisuudet riippuen versios- ta. (VMware vSphere 2009.)

View 4 on VMwaren työpöytävirtualisointiratkaisu ja se perustuu VMwaren omalle virtu- alisointialustalle, vSphere:lle. VMware View 4:n avulla pystytään erottamaan työpöytä fyysi- sestä laitteesta ja sijainnista, sekä toimittamaan ne hallinnoituna palveluna keskitetystä si- jainnista. Ratkaisulla voidaan jakaa työpöytä käyttäjille, monilla eri päätelaitteilla ja lähes millä tahansa verkkoyhteyden yli. VMware View 4 on saatavilla Enterprise ja Premier - versioilla. Premier version mukana tulevat lisäksi seuraavat komponentit:

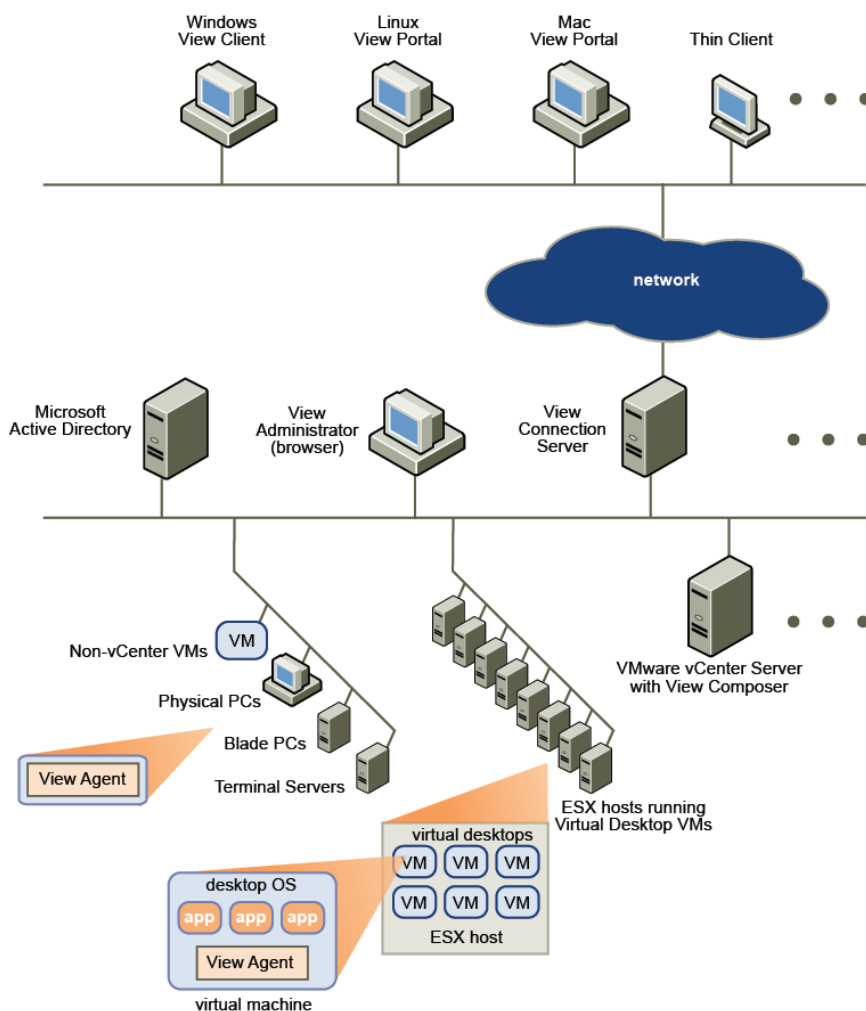
- View Composer varastoinnin optimointiin
- ThinApp sovellusten virtualisointia varten
- vShield loppupään keskitettyä virustorjuntaa ja haittaohjelmien etsintää varten
- View Client Offline Desktop (mahdollistaa työpöytien käytön offline-tilassa)

(VMware View 4.5 new features 2010.)



Kuva 17: Järjestelmän toiminta View 4 (VMware View features 2010)

VMware View Manager on keskeinen osa VMware View 4 työpöytävirtualisointia. VMware View Manager 4 sisältää seuraavat komponentit; View Connection Server, View Agent, View Client, View Portal sekä View Administrator. Seuraavissa kappaleissa on esitelty järjestelmän pääkomponentit ja niiden väliset vuorovaikutussuhteet. (VMware View 2010.)



Kuva 18: VMware View:n kuvaus (VMware View 2010, 10)

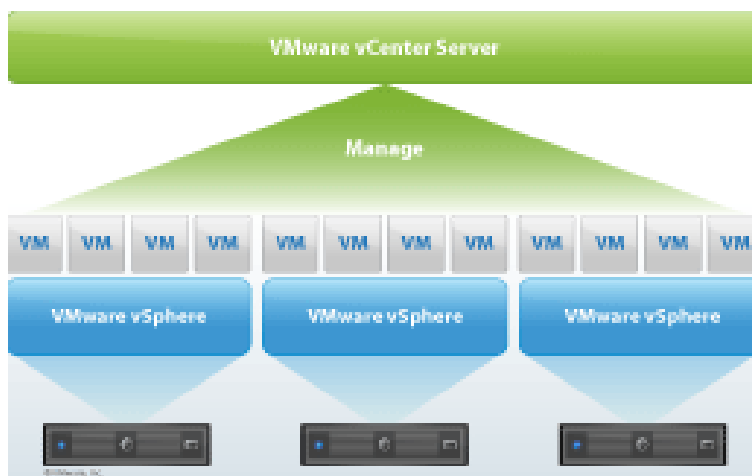
View Connection Server toimii välittäjänä (Connection Broker) asiakaspään yhteyksille. Connection Server autentikoi käyttäjän Active Directoryn kautta ja ohjaa pyynnöt sopivalle virtuaalikoneelle, fyysiselle- tai blade PC:lle tai Windows terminaalipalvelimelle. Connection Serverin tulee asentaa Microsoft Server 2003:lle ja tulee liittää Active Directoryyn. Connection Serverin ydinkomponentti on View Broker, joka on vastuussa kaikesta käyttäjien vuorovaikutuksesta View Clientin ja Connection Serverin välillä. View Brokeriin sisältyy Administration hallintatyökalu, mitä käytetään View Administrator Web clientin kautta. View Broker toimii yhteistyössä vCenterin kanssa ja tarjoaa kehittyneet ominaisuudet View työpöytien hallintaan esimerkiksi virtuaalikoneiden luonti ja virranhallinta. (VMware View 2010, 11, 49.)

View Administrator on verkkopohjainen hallintatyökalu, jonka avulla järjestelmänvalvojat voivat määrittää Connection Serverin asetuksia, jakaa ja hallinnoida View työpöytiä, valvoa käyttäjätunnistusta sekä ratkoa loppukäyttäjien ongelmia. View Administrator asentuu Connection Serverin asennuksen yhteydessä. Tämän sovelluksen avulla järjestelmänvalvojat voivat hallinnoida useita Connection Servereita ilman, että heidän täytyisi asentaa erillisiä sovelluksia sitä varten paikalliselle koneelle. (VMware View 2010, 22-23.)

vCenter Server toimii keskitettynä hallintajärjestelmänä VMware ESX-palvelimille. vCenter tarjoaa yhdistetyn pisteen, jonka kautta voidaan hoitaa virtuaalikoneiden konfigurointiin, provisiointiin ja hallinointiin liittyvät tehtävät. VMwaren vCenter palvelimen avulla järjestelmänvalvoja pystyy hallitsemaan tehokkaasti vSphere ympäristöjä (kuva 19). vCenterin avulla pystytään hallinnoimaan kaikkia fyysisiä ja virtuaalisia koneita yhdeltä Windows-alustan koneelta, johon on asennettuna VMware vSphere Client. Hallinnoiminen voidaan myös suorittaa vCenter Web Access -portaalin kautta, käyttämällä mitä tahansa web-selainta. (VMware vCenter 2009; VMware View 2010, 12-13.)

Pääominaisuuksia:

- Virtuaalikoneiden ja ympäristön reaaliaikainen seuranta. vCenteristä voi seurata kaikkia virtuaalisia laitteita, sekä niihin liittyviä fyysisiä komponentteja. Näihin kuuluvat muun muassa palvelimien laitteistot, tallennustilat, suorittimet ja verkot.
- Automaattinen vika- ja ilmoitusraporttien lähettäminen. vCenter pystyy myös aloittamaan automatisoituja korjaustoimia ongelmatilanteissa.
- Työn automatisointi. VMware vCenter sisältää vCenter Orchestrator -työkalun, jonka avulla ylläpitäjä pystyy automatisoimaan satoja erilaisia työnkuluja.
- vCenterillä pystytään hallinnoimaan yhdeltä konsolilta 300 isäntää ja 3000 virtuaalikonetta, linkitetystä tilasta voidaan hallinnoida jopa 1000 isäntää ja 10 000 virtuaalikonetta, jotka ovat jaettuna kymmenen vCenter -palvelimen kesken. (VMware vCenter 2009.)



Kuva 19: vCenterin toimintamalli (VMware vCenter 2009)

View Agent asennetaan kaikille virtuaalisille työpöydille, fyysisille laitteille ja terminaalipalvelimille, joita käytetään VMware View:n kautta työpöytinä. Agentti kommunikoi View Clientin kanssa ja tarjoaa seuraavia ominaisuuksia kuten yhteyden valvonta, virtuaalinen tulostamisen ja pääsyn paikallisesti liitettyihin USB-laitteisiin. Mikäli tarkoituksena on käyttää virtuaalikonetta työpöytänä, agentti asennetaan siihen ensimmäiseksi ja luodaan mallikone sen pohjalta. Käytettäessä luotavien koneiden pohjana mallikonetta, agentti asentuu automaattisesti kaikkiin uusiin virtuaalisiin työpöytiin. Agentti voidaan asentaa kertakirjautumismahdollisuudella (SSO). SSO:n ollessa päällä, käyttäjä kirjautuu sisään ainoastaan kerran View Connection Serveriin yhdistämisen aikana. (VMware View 2010, 22-23.)

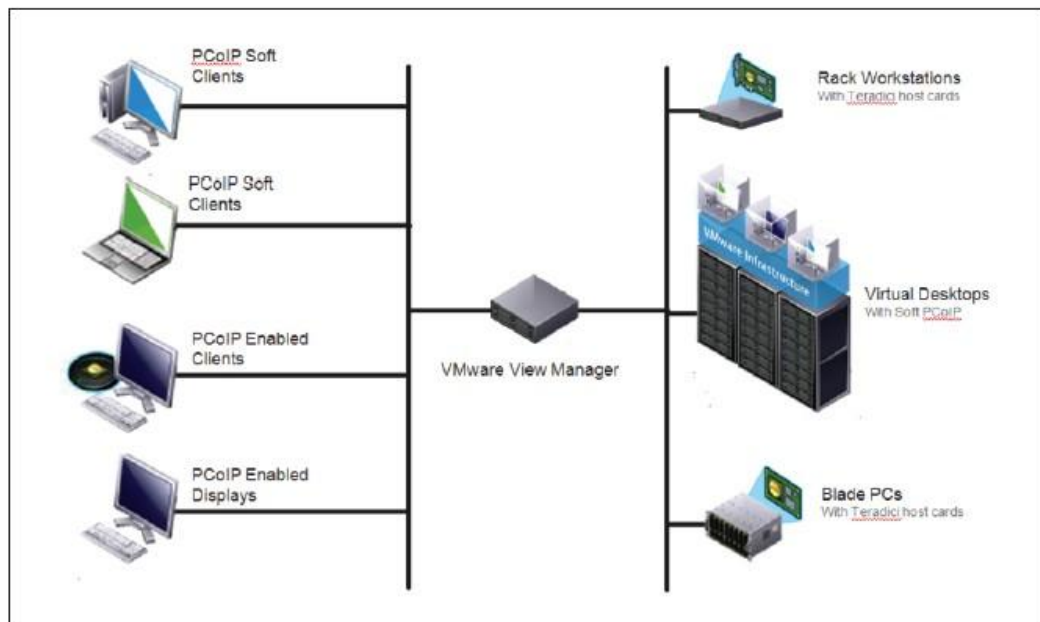
View Client on VMwaren sovellus, joka mahdollistaa Windows ja Linux käyttöjärjestelmien käyttäjille View:n virtuaaliset työpöydät. Sisäänkirjautumisen jälkeen käyttäjä voi ottaa käyttöönsä jonkin virtuaalisen työpöydän, johon hänellä on oikeus. Käyttöoikeuden varmentamiseen voidaan käyttää seuraavia menetelmiä: Active Directoryn tunnisteita (käyttäjätunnus ja salasana), RSA Secure ID (käyttäjätunnus, pin-koodi ja vaihtuva varmisteavain), älykortti PIN-koodilla. Työpöytävirtualisoinnissa etäkäyttö protokollana voidaan käyttää PCoIP:tä ja Microsoft RDP:tä. HP RGS protokollaa voidaan käyttää View työpöydille, jotka ovat HP Blade palvelimien isännöimiä. View Clientista on myös View Client with Offline Desktop -versio, joka mahdollistaa virtuaalisten työpöytien käyttämisen kun päätelaitteelle ei ole verkkoyhteyttä saatavilla. Tällöin virtuaaliset työpöydät latautuvat käyttäjän fyysiselle päätelaitteelle. (VMware View 2010, 22-23.)

View Portal on verkkopohjainen vaihtoehto View Clientille, jonka avulla käyttäjä pääsee virtuaalisille työpöydilleen käyttäen internet-selainta (Internet Explorer, Firefox tai Safari). Kirjautuminen tapahtuu menemällä selaimella View Connection Serverin URL-osoitteeseen. View Portal asentaa kaikki vaadittavat komponentit, mutta jotkin laajennukset eivät ole käy-

tössä. Merkittävämpänä puutteena USB-laitteiden tuki. Käyttäjän kirjautuessa ensimmäisen kerran View Portalille tulee hänen hyväksyä Portalin tarjoamien laajennusten asennus pääte-laitteelle. Linux koneella tulee olla lisäksi aktivoituna etätyöpöytä ja Mac OSX -koneilla Microsoft Remote Desktop Connection Client for Mac, jotta virtuaaliset työpöydät toimivat näissä käyttöjärjestelmissä. (VMware View 2010, 22-23.)

VMware View Composerin asennus on valinnainen ja sitä ei ole pakko käyttää tuotantoympäristössä. Testiympäristön rajoitteiden vuoksi emme hyödyntäneet Composerin ominaisuuksia, samalla ympäristöt pysyivät Microsoftin ratkaisun kanssa samankaltaisina. Tuotantoympäristössä ominaisuus kannattaa kuitenkin ehdottomasti ottaa käyttöön, sen tarjoamien ominaisuuksien vuoksi. Composer tulee asentaa samaan järjestelmään kuin mihin vCenter on asennettu. View Composerin avulla pystytään luomaan useita virtuaalisia koneita yhdestä levykuvasta (Golden Image). Näissä koneissa perustana on aina sama pohja, jonka päälle Composer luo jokaiselle koneelle oman nimen ja IP-osoitteen. Näin jokainen tämän avulla luotu kone toimii itsenäisesti. Tämän avulla voidaan automatisoida koneiden virtualisointi suurille massoille, voidaan luoda jopa 512 koneen --linked-clone-- -pooli. View Composer --linked-clone-- -pooli vie huomattavasti vähemmällä tallennuskapasiteetilla kuin perinteisellä tavalla luotu virtuaalikoneiden pooli. Kaikkien näiden koneiden ylläpito ja päivittäminen on helpompaa ja nopeampaa, kun järjestelmänvalvojan tarvitsee tehdä muutokset vain yhdelle koneelle. Mikäli luodaan pysyvien työpöytien pooli (Persistent Desktop Pool), niin View Composer luo erillisen levyn käyttäjän datoilta ja sovelluksille, kuin missä virtuaalinen kone sijaitsee. VMware suosittelee, että tämä levy pidetään erillään muista datakeskuksista, näin käyttäjien datat saadaan helpommin varmuuskopioitua. (Understanding Clones 2010; VMware Manager 4 2009; VMware View 2010, 22-23.)

VMware View ympäristössä voidaan käyttää rauta- ja ohjelmistopohjaisia ratkaisuja (kuva 20). Ohjelmistopohjaisessa vaihtoehdossa käytetään PCoIP-pohjaista View Client-ohjelmistoa perinteisellä PC:llä tai ohutpäätteellä. Rautapohjaisessa mallissa hyödynnetään Zero Client - päätelaitteita, mitkä eivät sisällä suoritinta, normaalia käyttöjärjestelmää tai laiteohjaimia. Zero Clientit tarjoavat PCoIP-protokollan laiteohjelmatasolla hyödyntäen Teradiciin isäntäkortteja. Tällä ratkaisulla saavutetaan paras toiminnallisuus ja lähes täydellinen huoltovapaus. (VMware View 4 PCoIP 2009.)



Kuva 20: VMware päätelaitteet (VMware View 4 PCoIP 2009)

PCoIP-protokollan ominaisuuksia:

- Usean näytön tuki 1920x1200 resoluutiolle, clear-type fontit, 32-bittiset värit ja tuki neljälle monitorille
- Automaattinen näytön skaalaus, dynaaminen kuvan koon muuttaminen, pivot-toiminnon tuki
- Multimedian uudelleenohjaus seuraavilla formaateilla: VWM, WMA, AC3, MP3, MPG-1, MPG-2 ja MPG-4
- Tuki seuraaville USB-laitteille: hiiret, näppäimistöt, massamuistit, printterit, skannerit ja muut yleisimmät lisälaitteet
- Tuki isäntäpohjaiselle Flash:n renderöinnille ja mahdollisuus hallita laatua sekä kais-tankulutusta
- Kaksisuuntainen ääni korkealla laadulla

(VMware View 4 PCoIP 2009.)

2.5.3 Citrix XenDesktop 4

Citrix on IT-yritys, joka on perustettu vuonna 1989 ja päätoimisto on Fort Lauderdale, Floridassa. Työntekijöitä Citrixillä on 35 maassa yhteensä yli 4000 ja sen asiakkaina on yli 230 000 organisaatiota. Citrix tarjoaa verkkoratkaisuja, pilvipalveluita, software-as-a-service (Saas)-palveluita sekä palvelin ja työpöytävirtualisointiratkaisuja. Citrix on yksi toimialansa johtavista yrityksistä. (Citrix Desktop Virtualization 2010, 10; Products & Solutions 2010.)

Citrixin XenServer pohjautuu Xen hypervisorin, joka kehitettiin Cambridgen yliopistossa Keir Fraserin ja Ian Pratin toimesta, osana Building and open infrastructure for global distributed computing -tutkimusprojektia 1990-luvun loppupuolella. Ensimmäinen versio tuotteesta julkistettiin kansainväliselle kehittäjäyhteisölle vuonna 2003 ja vuonna 2004 julkistettiin virallisesti Xen 1.0 versio. Pian julkaisun jälkeen Ian Pratt ja useat muut teknologiajohtajat perustivat XenSource Inc.-yhtiön, tavoitteenaan muuttaa Xen hypervisor kilpailevaksi tuotteeksi yritysratkaisuille. Xen hypervisor on avoimen lähdekoodin virtualisointiratkaisu, joka tarjoaa tuen x86, x64, IA64, ARM, sekä muille prosessoriarkkitehtuureille. Ratkaisu tukee useimpia käyttöjärjestelmiä esim. Windows, Linux ja Solaris. Vuonna 2007 Citrix osti 500 miljoonalla dollarilla avoimen lähdekoodin virtualisointiratkaisuja kehittäneen XenSource ja kehitti heidän ratkaisun pohjalta oman kaupallisen tuotteen, joka tunnetaan nimellä XenServer. (What is Xen 2010; Ruest & Ruest 2009, 174; Xen.org History 2010.)

Xen Desktop on Citrixin VDI-ratkaisu, joka mahdollistaa virtuaalisten Windows työpöytien provisioinnin käyttäjille. Oletuksena järjestelmä pohjautuu yhteen levykuvaan, pitkälti samalla tavalla kuin VMwaren View -ratkaisussa. Kaikki työpöydät provisioidaan yhdestä levykuvasta ja suoritetaan siitä. Master-imagea ei kopioida missään vaiheessa. Tällä ratkaisulla voidaan säästää jopa 40 % prosenttia tallennustilassa. Citrix tuli markkinoille omalla tuotteellaan XenDesktop 2.0:lla vuonna 2008. Lokakuussa 2009 julkaistiin versio XenDesktop 4 ja vuotta myöhemmin siitä julkistettiin versio 5.0, mikä on kirjoitushetkellä viimeisin versio. (Citrix Desktop Virtualization 2010, 9; Ruest & Ruest 2009, 257.)

XenDesktop muodostui yhdistämällä ominaisuuksia XenServerin virtualisointiytimeistä XenApp:n välitysmekanismiin, sekä yrityskaupassa Ardencelta saatuihin toiminnallisuuksiin. Ardencelta saadut teknologiat mahdollistavat eroavien tiedostojen (differential files) generoinnin yhdestä master-imagesta. Tämän teknologian avulla XenDesktop:lla voidaan hallinnoida satoja tai jopa tuhansia eroaviin tiedostoihin perustuvia levykuvia, jotka perustuvat yhteen master-imageen. Tämä on erittäin tärkeä ominaisuus, koska normaalisti jokainen levykuva täytyy valmistella Sysprep-työkalulla (System Preparation Tool), ennen sen monistamista. Sysprep pyyhkii levykuvasta kaikki yksilölliset tiedot ja luo automaattisesti uudet persoonalliset tiedot, kun levykuva avataan ensimmäisen kerran. XenDesktopin kanssa tätä vaihetta ei tarvitse tehdä. Levyn monistamista varten tehdään yksi levykuva yrityksen ohjelmistoilla ja asetuksilla, josta valmistetaan kopio lukuoikeuksilla (read-only). Lukuoikeuksilla olevasta levykuvasta tulee master-image, jota XenDesktop käyttää. Käyttäjän muutokset ja asetukset tallentuvat eroavaan tiedostoon, mikä pyyhkitään tyhjäksi uloskirjautumisen yhteydessä tai tallennetaan erilliseen käyttäjätiedostoon, riippuen siitä minkälainen työpöytäpooli on käytössä. Ainoastaan master-imageen nähden tehdyt muutokset tallennetaan. (Ruest & Ruest 2009, 257.)

XenDesktop pystytään integroimaan jo käytössä olevaan Microsoftin infrastruktuuriin. Näin pystytään hyödyntämään nykyisiä laitteistoja ja tarjotaan joustavuutta uusille hankinnoille. XenDesktop tukee suurimpien valmistajien palvelinvirtualisointiratkaisuja (Citrix XenServer, Microsoft Hyper-V ja VMware ESX ja vSphere). Citrix XenDesktop ratkaisussa on tarjolla neljä eri versiota (Express, VDI, Enterprise, VDI ja Platinum). Express on ilmainen ja riisuttu versio tuotteesta, jota voidaan käyttää tuotteen arviointiin ja maksimissaan kymmenen käyttäjän ympäristöön. (Ruest & Ruest 2009, 257; XenDesktop Features and Editions, 2010.)

Seuraavassa on esiteltyä ratkaisun pääkomponentit. Desktop Delivery Controller (DDC) todentaa käyttäjät, hallinnoi käyttäjien virtuaaliset työympäristöt, sekä välittää virtuaaliset työpöydät käyttäjille. DDC valvoo työasemien kuntoa ja käynnistää ja sammuttaa niitä käyttötilanteen mukaisesti. DDC sisältää myös User Profile Manager, jolla hallinnoidaan käyttäjien personalisoituja asetuksia virtuaalisessa tai fyysisessä Windows ympäristössä. DDC:n ydinkomponentit ovat Desktop Delivery Controller, Management Console ja License Server. DDC:tä ei voi asentaa samalle palvelimelle domain controllerin kanssa. (XenDesktop Features and Editions 2010.)

Virtual Desktop Provisioning toimii virtuaalisten työpöytien käyttöönottopalveluna provisioiden uuden työpöydän käyttäjälle ”on-demand” -periaatteella määritellystä levykuvasta. Näin pystytään tarjoamaan käyttäjille aina koskematon työpöytä, kun hän kirjautuu järjestelmään sisään. Työpöytien automaattinen provisiointi yksinkertaistaa työasemien levykuvien jakelua ja tarjoaa näin keskitettyä hallintaa virtuaaliselle työpöytäympäristölle. Työpöytien provisioinnin kautta pystytään optimoimaan levyjärjestelmän tilankäyttö käyttämällä master-imageita, mitkä vähentävät tarvittavaa tallennuskapasiteettia. (XenDesktop Components 2010.)

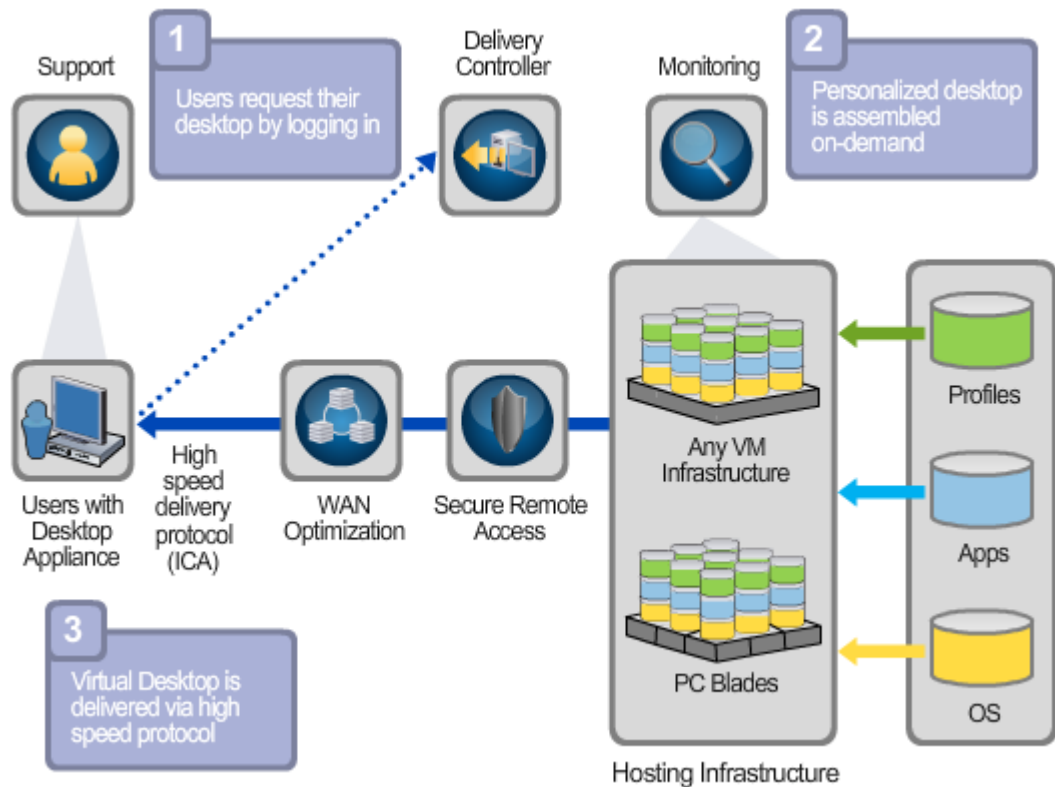
Virtual Desktop Agent on komponentti, joka asennetaan virtuaalisille työpöydille. Agentti mahdollistaa suoran yhteyden ICA-protokollan avulla käyttäjän laitteelta virtuaaliselle työpöydälle. Citrix online plug-in puolestaan on asiakaspään komponentti, joka asennetaan käyttäjän päätelaitteeseen. Online plugi:nin kautta käyttäjä saa etäyhteyden (ICA) virtuaaliseen työpöytään, johon hänelle on määritetty oikeudet. Citrix Online plug-in oli aiemmalta nimeltään Citrix Desktop Receiver. (Citrix Online Plug-in 2009; XenDesktop Components 2010.)

XenServer on Citrixin palvelinvirtualisointialusta, joka perustuu Xen-hypervisorin. XenServer tukee niin Windows kuin Linux käyttöjärjestelmiä. XenServeristä on olemassa ilmainen Free versio, joka sisältää yksinkertaisimmat ominaisuudet, jättäen ulkopuolelle maksullisten versioiden hallinnoinnin ja edistyneimmät ominaisuudet. Kaupalliset versiot ovat Advanced, Enterprise ja Platinum. Maksullisten versioiden ominaisuuksiin kuuluvat muun muassa virtuaaliko-

neiden provisiointi, muistin optimointi ja korkeaan saatavuuteen (High availability) liittyvät ratkaisut. (XenDesktop Components 2010; XenServer editions 2010.)

ICA-protokolla kehitettiin 1980-luvun lopulla ja on yksi Citrixin vanhimmista teknologioista. Protokollaa suunniteltaessa otettiin huomioon myös hitaat verkkoyhteydet, näin yhteyden nopeudella ei ole niin merkitystä minkälaisen yhteyden ICA-client ja palvelin luovat. ICA ei ole kokoajan suoraan toistava protokolla kuten RDP, vaan ICA välittää liikennettä verkossa vain silloin kun käyttäjä tekee jotain, esimerkiksi liikuttaa hiirtä tai kirjoittaa näppäimistöllä. Näin ICA:n vaatima kaista voi olla minimissään 10-20 kpbs käyttäjää kohden. Käyttäjän koneen ollessa passiivisessa tilassa verkon käyttö pienenee ja käyttöaste pysyy automaattisesti optimaalisella tasolla. ICA protokolla tukee yli 200 laitetta sallien joustavuutta päätelaitteen valinnassa. (Casselman ym 2009, 42; Tooley 2009, 150.)

HDX (High Definition User Experience) on Citrixin uusin teknologia, joka tuo työpöytävirtualisointiin joukon ominaisuuksia, (mm. Plug-n-Play, MediaStream ja verkon tasaus) joiden avulla Citrix mahdollistaa käyttäjälle hyvän käyttökokemuksen verkosta tai päätelaitteesta riippumatta. Tämän HDX tekee tasapainottelemalla automaattisesti suorituskyvyn sekä verkon nopeuden kanssa. HDX hyödyntää useissa ominaisuuksissaan SmartRendering -ominaisuutta joka tarkastaa kannattaako grafiikka ja multimedia renderöidä palvelimella vai päätelaitteella. Tämä ominaisuus parantaa virtuaalisen työpöydän käyttökohteita. (HDX overview 2010; Optimizing HDX Technologies 2010, 6,8.)



Kuva 21: Citrix XenDesktop 4 toimintamalli (xendesktop-technology 2008)

2.6 Esityskerroksen virtualisointi

Esityskerroksen virtualisointi eroaa työpöytävirtualisoinnista siten, että käyttäjä jakaa työpöytäympäristön muiden käyttäjien kanssa samalta palvelimelta. Työpöytävirtualisoinnissa jokainen käyttäjä taas saa oman työpöydän. Suurimmat tähän teknologiaan perustuvat ratkaisut ovat Microsoftin Remote Desktop Services ja Citrixin XenApp (aiemmin Citrix Presentation Server). (Ruest & Ruest 2009, 39,272.)

Päätepalvelut mahdollistavat yhden työpöydän ja ohjelmien jakamisen, jopa sadoille käyttäjille. Käyttäjät kirjautuvat palvelimelle samanaikaisesti ja ne jaetaan istuntoihin. Eri käyttäjien istunnot on eristetty toisistaan. Samanaikaisten käyttäjien määrän sanelee suurimmaksi osaksi palvelimen prosessorin tehokkuus, tallennusjärjestelmä ja keskusmuistin määrä. Verkkoysteys asiakastietokoneen ja päätepalvelimen välillä ei vaadi kovinkaan paljon kaistaa, vain muutama kilobitti sekunnissa. Jokainen käyttäjän istunto vie vähintään 20 megatavua keskusmuistia tilaa. Normaalien toimisto-ohjelmien kanssa muistia tulee olla jo 50 megatavua käyttäjän istuntoa kohti. (Kivimäki 2009, 1025.)

Päätepalveluiden käyttäminen helpottaa ylläpidon työtä, kun hallittavana on vain yksi instanssi käyttöjärjestelmästä. Ohjelmistojen asennukset ja päivitykset täytyy tehdä vain yhteen koneeseen. Päätepalvelimelle asennettavien ohjelmien tulee kuitenkin toimia istunto-pohjaisessa järjestelmässä. Ohjelmistojen yhteensopivuuden testaamiseen löytyy omia työkaluja ja scriptejä. (Kivimäki 2009, 1025.)

Windows Server 2008R2 julkistamisen myötä on tapahtunut monia muutoksia päätepalveluihin, jotka parantavat etäohjelmien (RemoteApp) ja työpöytien (Remote Desktop) toimintaa sekä integrointia Windows 7 käyttöjärjestelmään. RemoteApp avulla käyttäjät voivat käynnistää Remote Desktop Session Host -palvelimelle (RDSH) asennettuja ohjelmia erillisinä prosesseina, suoraan käynnistä-valikosta tai työpöydän pikakuvakkeista kirjautumatta erikseen palvelimelle. Etäohjelmat toimivat käyttäjän kannalta aivan kuten muutkin tietokoneeseen paikallisesti asennetut ohjelmat. Käyttäjän halutessa hyödyntää useampaa ohjelmaa RDS-palvelimelta ne jakavat saman istunnon. Etäohjelmat voidaan toimittaa asiakaskoneille perinteisesti Remote Desktop Protocol (.rdp) -tiedoston avulla tai Windows Installer (.msi) -pakettilla. Ohjelmia pystytään tarjoamaan myös RD Web Access palvelimen selainkäyttöliittymän kautta. Asiakaskoneissa tulee olla vähintään Remote Desktop Connection (RDC) -asiakasohjelman 6.x versio, jotta ohjelmat toimivat. Käyttöjärjestelmävaatimuksena on Windows 7, mikäli halutaan hyödyntää RemoteApp and Desktop Connection Feed -ominaisuutta (kuva 22). (Kivimäki 2009, 1045.)



Kuva 22: Windows 7, RAD-feedinä näkyvät linkit Käynnistä-valikossa (Introducing RemoteApp and Desktop Connections.)

3 Testiympäristöt

Valitsimme testattaviksi VMwaren ja Microsoftin VDI-toteutukset. Ympäristöjen tarkoituksena oli simuloida virtualisoituja työpöytiä luokkaympäristössä. Testauksen tavoitteena oli tutkia

näiden ratkaisuiden toimivuutta sekä kerätä tietoa siitä, miten ne soveltuisivat erilaisiin käyttötarkoituksiin opetuksessa. Valitut toteutukset eroavat toisistaan osakomponenttien ja teknologioiden osalta. Päädyimme rakentamaan samankaltaiset ympäristöt, jotta ratkaisujen soveltuvuutta käyttötarkoitukseen voitaisiin arvioida. Molempien ratkaisuiden taustalla on pool-tyyppinen Virtual Desktop Infrastructure (VDI). Ratkaisut perustuvat palvelimella sijaitseviin virtuaalisten työpöytien varantoihin, joista käyttäjälle annetaan oma kone kun hän kirjautuu ympäristöön. Samoilla ratkaisuilla toteutettuja ympäristöjä voitaisiin hyödyntää isommassa mittakaavassa luokkakohtaisten poolien rakentamiseen. Molemmissa testiympäristöissä hyödynsimme samaa domain controller -palvelinta.

Testiympäristöjen domain controller -palvelinta varten asensimme Windows Server 2008 R2. Määritimme sen rooliksi Active Directory Domain Service (AD DS), hallinnoimaan tietokantaa laitteista ja käyttäjistä. Active Directory (AD) nimi muuttui AD DS:ksi Windows Server 2008:n myötä. Osana AD DS:n asennusta emme ottaneet käyttöön DHCP-palvelua, vaan määritimme toimialueemme koneille staattiset IP-osoitteet. DHCP-palvelua ei käytetty käytössä olleen verkon rakenteen vuoksi. Tarvitsimme välillä pääsyn internetiin aktivointeja sekä päivityksiä varten. Yhteys kulki Laurean verkon kautta ja emmekä näin ollen voineet ottaa sitä käyttöön vaarantamatta muuta liikennettä. Myöskään palomuuureja tai liikenteen rajoittamista ei käytetty, mikä mahdollisti ketterän testaamisen ja työn pysymisen rajauksessaan. (Domain Controller Roles 2010.)

Microsoftin ratkaisussa asennettujen palvelimien lisäksi tuotantoympäristössä tarvitaan lisenssipalvelin (Remote Desktop Licensing) järjestelmien RDS-käyttöoikeuksien (CAL) hallintaa varten. Testiympäristössä hyödynsimme 120 päivän koeaikaa. Lisenssipalvelimen lisäksi voidaan ottaa käyttöön Remote Desktop Gateway -palvelin, mikäli halutaan tarjota pääsy virtuaalisille työpöydille yrityksen ulkopuolelta käsin. VMware View -ratkaisusta kannattaa ottaa käyttöön View Composer, jolla voidaan automatisoida työpöytien toimittaminen ja kloonaminen yhdestä golden imagesta (Linked Clone).

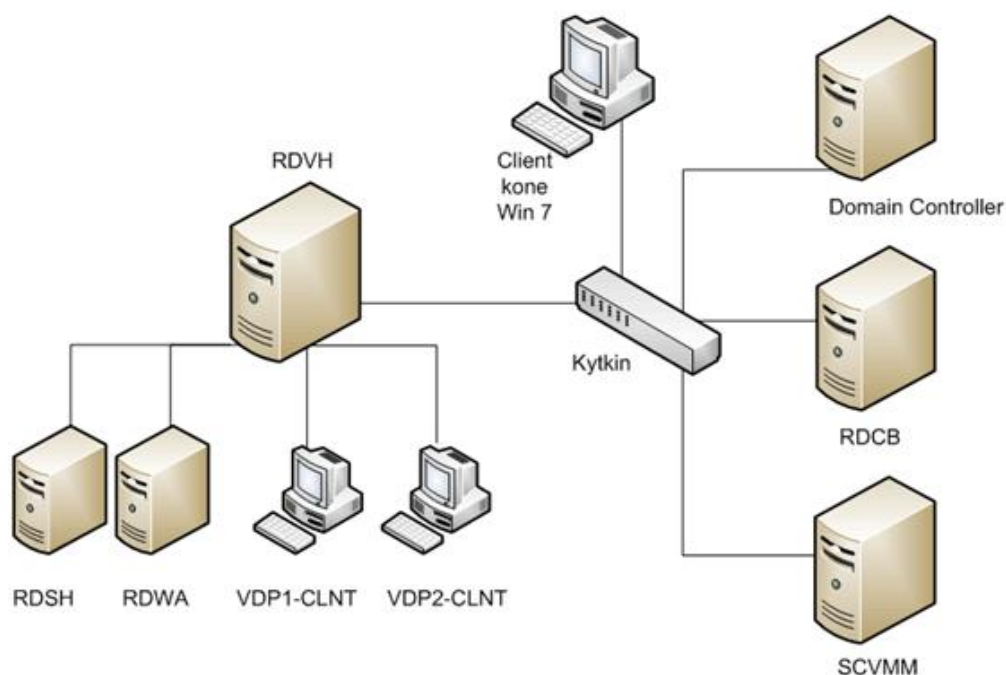
3.1 Testiympäristö 1, Microsoft VDI

Ensimmäiseksi testiympäristöksi rakensimme Microsoftin VDI toteutuksen, joka on kuvattu kuvassa 23. Ympäristö koostuu Windows 7 työasemasta ja Server 2008R2 palvelimista, sekä niille asennetuista rooleista. Hallintapalvelimeksi asensimme System Center Virtual Machine Manager 2008 R2:n. Testiympäristön asennusohje löytyvät liitteistä 1 ja 2.

Microsoftin ratkaisussa käyttäjät ottavat yhteyden virtuaalisten työpöytien varantoon RD Web Accessin kautta tai hyödyntäen Win7-koneelle määriteltyä RemoteApp and Desktop Connectionia. Pyyntö lähetetään RD Session Host -palvelimelle, mikä toimii uudelleenohjauksessa. RD Session Host -palvelin ohjaa pyynnön RD Connection -Broker palvelimelle. RD Connection

Broker -palvelin tarkistaa onko käyttäjätunnuksella jo olemassa olevia istuntoja meneillään, mikäli sessio löytyy se palauttaa virtuaalikoneen nimen RD Session Host -palvelimelle. Mikäli käyttäjän istuntoa ei löydy palvelimelta, niin RD Connection Broker lähettää pyynnön RD Virtualization Host -palvelimelle virtuaalikoneen paikantamista ja käynnistämistä varten. RD Session Host uudelleenohjaa pyynnön päätelaitteelle, joka käynnisti yhteyden. Viimeisessä vaiheessa Win7-kone yhdistää käyttäjän virtualikoneeseen. (Deploying Virtual Desktop Pools 2010, 7.)

Ympäristölle on muutamia laite- ja ohjelmistovaatimuksia sekä huomioitavia asioita. Suurimmat laitevaatimukset tulevat RDVH-palvelimelle, johon asennetaan Microsoftin Hyper-V. Hyper-V:n asennus edellyttää rautapohjaista virtualisoinnin tukea prosessorilta (AMD-V ja INTEL-VT), sekä laitteistopohjaiselle suorituksen estolle (DEP, data execution protection) asetukset kytketään päälle BIOS:n kautta. Lisäksi palvelimen prosessori ja muistin määrä sanelee sillä ajettavien virtuaalikoneiden määrän. Käytetyllä tallennusjärjestelmällä on merkitystä, koska sen I/O-nopeus vaikuttaa järjestelmän suorituskykyyn ja ajettavaan kuormaan. Domain controllerin toiminnallisuuden tason tulee olla vähintään Windows Server 2008 tasolla. Edellä mainittujen vaatimuksien lisäksi tulee ottaa huomioon käyttöjärjestelmäkohtaiset minimivaatimukset, jotka pätevät myös virtuaalikoneissa. (Kivimäki 2009, 427.)

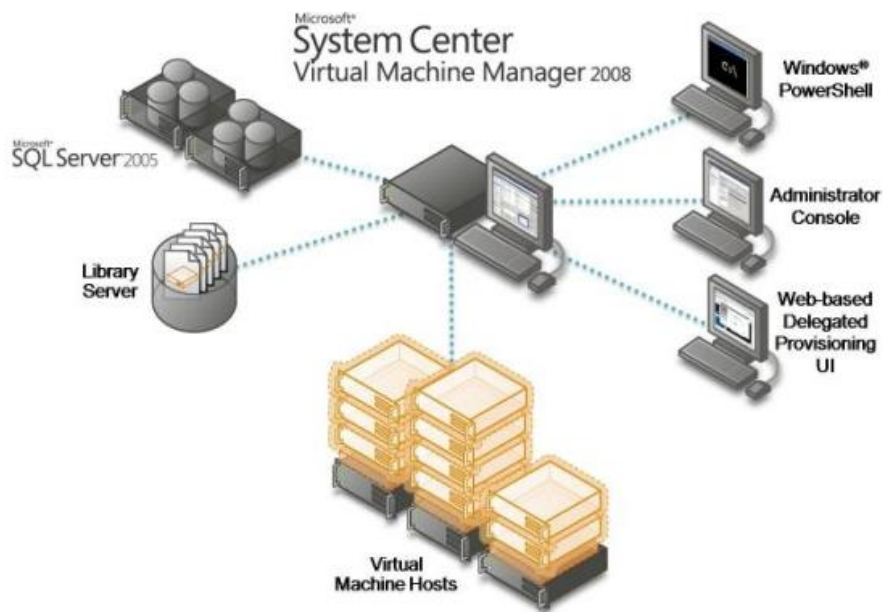


Rooli/laite	Kuvaus	Muistia	Proessori	Käyttöjärjestelmä
RDVH	IBM System X 3650 - palvelin, levyjärjestelmä: RAID 10	12Gt	Intel Xeon 2GHz Quad core	Windows Server 2008 R2 Enterprise
RDVH:n virtuaalikoneet:				
RDWA	virtuaalinen palvelin	2Gt		Windows Server 2008 R2 Enterprise
RDSH	virtuaalinen palvelin	2Gt		Windows Server 2008 R2 Enterprise
VDP 1 ja 2	virtuaaliset työpöydät	2Gt		Windows 7 Professional
RDCB	Osborne PRO945GC	2Gt	Intel E4500 2.2GHz	Windows Server 2008 R2 Enterprise
Domain Controller	HP Compaq 7900	2Gt	Intel E7300 3.16GHz	Windows Server 2008 R2 Enterprise
SCVMM hallintapalvelin	HP Compaq 7800	2Gt	Intel E6550 2.33 GHZ	Windows Server 2008 R2 Enterprise
Client työasema	Osborne PRO945GC	2Gt	Intel E4500 2.2GHz	Windows 7 Professional
Kytin	D-link DGS-1008D 8-porttinen 10/100/1000Mb/s			

Kuva 23: Testiympäristön kuvaus Microsoft VDI

Virtuaalikoneiden valvontaa ja hallintaa varten asensimme erillisen SCVMM-palvelimen (System Center Virtual Machine Manager), jotta ympäristöt olisivat ominaisuuksiltaan lähempänä toisiaan. Server 2008 R2 mukana tuleva Hyper-V Manager tarjoaa yksinkertaiset työkalut palvelinten hallintaan, mutta esimerkiksi koneiden nopea kloonaminen, tehokas valvonta ja tehtävien automatisointi ei mukana tulevilla työkaluilla onnistu. SCVMM 2008 R2 on kokonaisvaltainen hallintatyökalu virtualisoidulle infrastruktuurille (kuva24). SCVMM avulla voidaan hallita Hyper-V, Virtual Server ja VMware ESX -palvelinohjelmistoja keskitetysti. Tärkeimpinä ominaisuuksia ovat P2V ja V2V muunnokset, palvelinten siirto lennossa toiselle Hyper-V alustalle (Live Migration), Performance Resource Optimization (PRO) System Center Operations Manager 2007 integrointia ja valvontaa varten, sekä VHD:n lisääminen lennossa käynnissä olevaan koneeseen (Hot Add). (Virtual Machine Manager 2010.)

Asensimme SCVMM:n kaikki komponentit samalle palvelimelle, jolloin laitevaatimuksina on minimissään 2 Ghz Pentium 4 -tasoinen (x64) suoritin, 2GB muistia, 10GB levytilaa ja Windows Server 2003 R2 SP2 käyttöjärjestelmä. Tuotantoympäristön suositukseksi on, että jokainen komponentti asennettaisiin omalle palvelimelleen. Minimivaatimuksen mukaisella kokoonpanolla pystytään hallinnoimaan 5-10 isäntää, mikä riitti testaukseen enemmän kuin hyvin. Asennuksessa mukana tuleva SQL Server 2005 Express Editionin tietokannan koko on rajoitettu neljään gigatavuun, mikä tulee huomioida isompien ympäristöjen toteutuksessa. (VMM System Requirements 2008 R2 2010.)



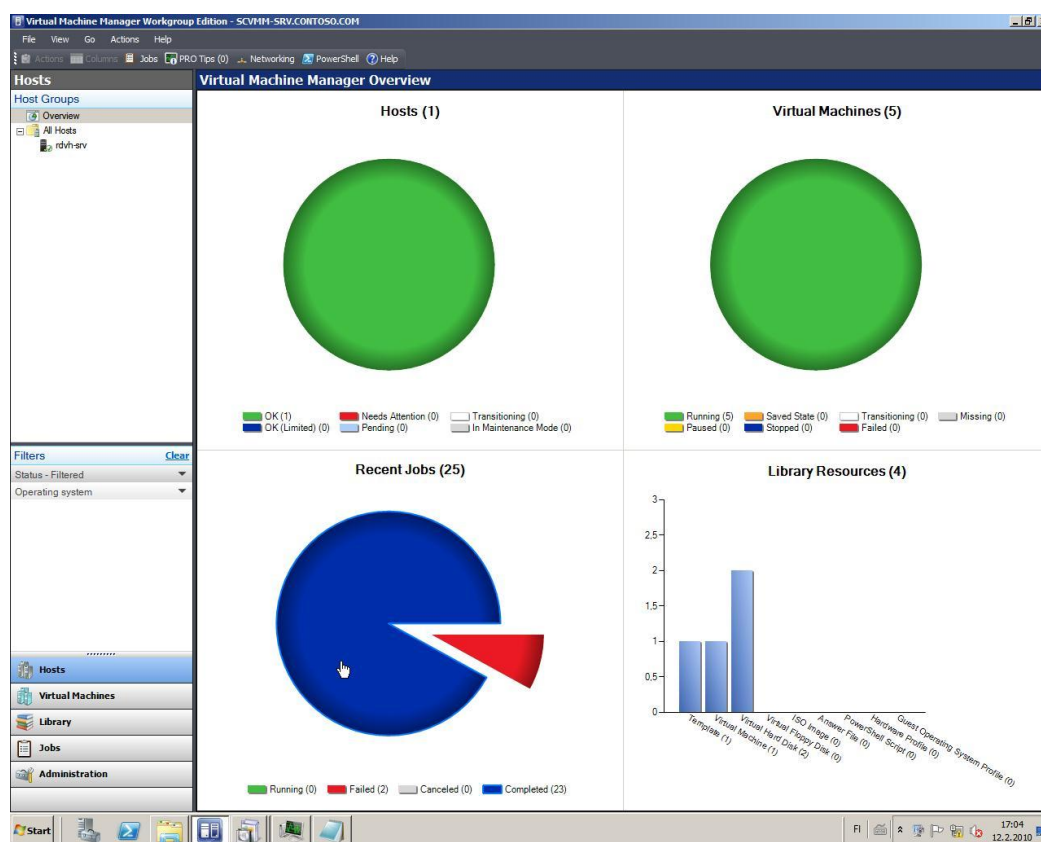
Kuva 24: SCVMM kuvio (VMM Overview 2008)

SCVMM:n ydinkomponentti on Virtual Machine Manager Server. Kaikki muut komponentit ovat vuorovaikutuksessa ja kommunikoivat VMM Serverin kautta. Virtual Machine Management -palvelu pyörii VMM Serverillä, mikä mahdollistaa komentojen suorittamisen ja tiedostojen siirron koko VMM ympäristön läpi. VMM Server kontrolloi kaikkea liikennettä muiden komponenttien ja isäntäpalvelimien välillä ja on yhteydessä SQL-palvelimeen, jota käytetään VMM konfiguraatietojen säilömiseen. VMM Serveriä hallinnoidaan VMM Administrator konsolin kautta. (Tulloch 2009, 91.)

VMM Library -palvelin ylläpitää katalogia resursseista, joita voidaan käyttää virtuaalikoneiden määrittämiseen ja luomiseen. VMM kirjasto pitää sisällään .iso-imaget, scriptit, virtuaaliset kovalevyt, virtuaaliset levyasemat, virtuaalikoneiden mallitiedostot, vieraskoneiden järjestelmä- ja rautaprofiilit. Kirjasto voi pitää myös sisällään valmiita virtuaalikoneita, jotka eivät ole käytössä sillä hetkellä. (Tulloch 2009, 91.)

VMM Agent hallinnoi virtuaalikoneita isäntäpalvelimilla ja mahdollistaa kommunikoinnin Library-palvelimen kanssa. Agentti asentuu automaattisesti kohdekoneeseen kun se on lisätty isäntäpalvelimeksi administrator konsolilla. VMM Agent pitää asentaa käsin niihin koneisiin, jotka ovat toimialueen ulkopuolisia tai verkon ulkopuolella. (Tulloch 2009, 91.)

VMM Administrator -konsoli on MMC-konsoli, jota käytetään asetusten konfigurointiin, isäntien ja Library palvelimien hallintaan, virtuaalikoneiden luomiseen ja jakeluun. Kuvassa 25 on esimerkkinä testiympäristömme yleisnäkymä. (Tulloch 2009, 92.)



Kuva 25: Administrator konsolin yleisnäkymä ympäristöstä

VMM Self-Service portal on valinnainen Web-pohjainen komponentti, minkä avulla loppukäyttäjät pystyvät luomaan ja hallinnoimaan omia virtuaalikoneita, mikäli heille on annettu oikeus siihen. Oikeuksien jakaminen tapahtuu portaalin self service -määritysten kautta. Määrittelyillä säännellään mitä mallikoneita (template) käyttäjä voi luoda, kuinka monta, millä isännällä se suoritetaan ja minkälaiset oikeudet käyttäjällä on luotuun koneeseen. (Tulloch 2009, 92.)

3.2 Testiympäristö 2, VMware View 4

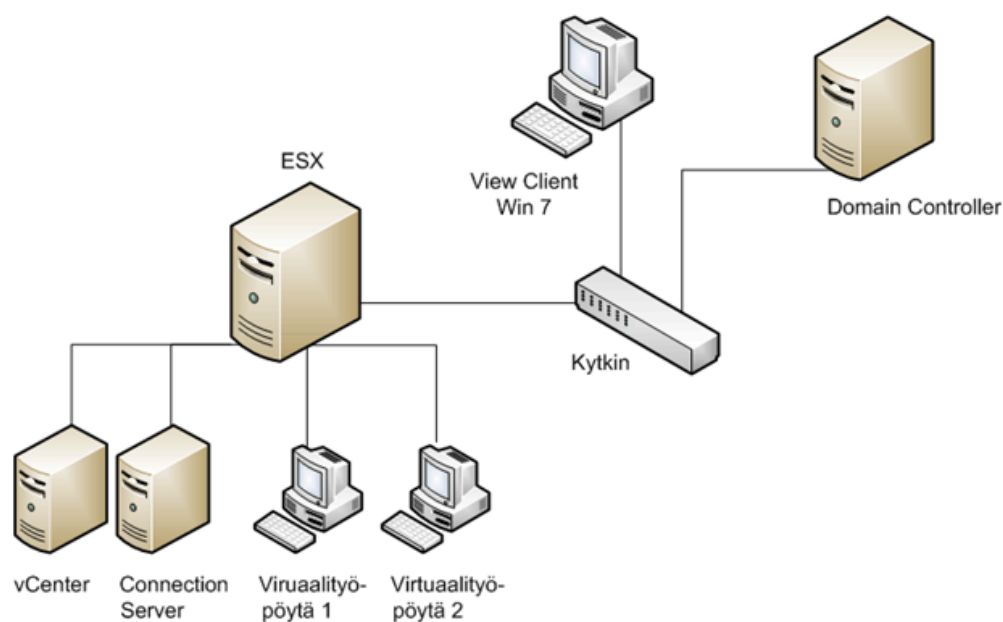
Toisena testiympäristönä teimme kuvan 26 mukaisen VMware View 4 ratkaisun. Testiympäristön asennus on dokumentoitu liitteessä 3. Hyödynsimme Microsoftin ympäristöä varten asennettua Active Directory -toimialuetta, joten sen asennusta ei ole dokumentoitu uudelleen.

VMwaren ratkaisussa käyttäjät ottavat yhteyden virtuaalisiin työpöytiinsä käynnistämällä View Client päätelaitteelta tai kirjautumalla View Portalin kautta Connection Serverille. Connection Server integroituu AD:n kanssa ja tarjoaa pääsyn virtuaalisille työpöydille, jotka sijaitsevat VMware ESX -palvelimella.

VMwaren ESX -palvelimelle on tarkkaan määritelty lista yhteensopivista komponenteista. Lista löytyy kokonaisuudessaan valmistajan kotisivuilta osoitteesta

www.vmware.com/resources/compatibility. Tärkeimpinä vaatimuksina ovat 64-bittinen x86 suoritin (32-bittiset järjestelmät eivät ole enää tuettuna), vähintään 2Gt muistia, yhteensopiva verkkokortti (esim. Intel Pro 1000, Broadcom NetXtreme 570x). Tallennusta varten palvelimesta tulee löytyä yhteensopiva SCSI-ohjain, sisäinen RAID-ohjain tai Fibre Channel adapteri. Serial ATA levyt tulee olla kytketty tuettujen SAS-ohjainten kautta tai emolevyyn integroitujen SATA-ohjainten tulee löytyä yhteensopivien laitteiden listalta. vCenterin osalta laitteistovaatimukset riippuvat pitkälti sillä ajettavien isäntien ja virtuaalikoneiden määrästä. Asennuksen mukana tuleva SQL Server 2005 Express mahdollistaa maksimissaan viiden isännän ja 50 virtuaalisen koneen käytön. Ajettavien isäntien määrän kasvaessa yli 200, isäntäkäyttöjärjestelmän on oltava 64-bittinen versio Windowsista. (ESX Hardware Requirements 2010.)

Laitteiston vähimmäisvaatimuksena (alle 50 virtuaalisen työpöydän ympäristössä) Connection Serverille on Pentium IV 2.0Ghz prosessori, 2Gt muistia sekä verkkokortti. Palvelin voi olla joko fyysinen tai virtuaalinen ja käyttöjärjestelmä voi olla 64- tai 32-bittinen Windows Server. 32-Bittisistä käyttöjärjestelmistä yhteensopivia ovat vain Windows Server 2003/R2 Standard sekä Windows Server 2003/R2 Enterprise ja niiden tulee olla Service Pack 2 tasolla. Windows palvelimessa johon Connection Server asennetaan, ei saa olla Windows Terminal Server roolia asennettuna. (Knowledge Base 2010.)



Rooli/laite	Kuvaus	Muistia	Proessori	Käyttöjärjestelmä
ESX	IBM System X 3650 - palvelin, levyjärjestelmä: RAID 10	12Gt	Intel Xeon 2GHz Quad core	ESX 4.0
ESX:n virtuaalikoneet:				
vCenter	virtuaalinen palvelin	2Gt		Windows Server 2003 sp2
Connection Server	virtuaalinen palvelin	2Gt		Windows Server 2003 sp2
Virtuaalityöpöydät 1 ja 2	virtuaaliset työpöydät	2Gt		Windows 7 Professional
Domain Controller	HP Compaq 7900	2Gt	Intel E7300 3.16GHz	Windows Server 2008 R2 Enterprise
Client työasema	Osborne PRO945GC	2Gt	Intel E4500 2.2GHz	Windows 7 Professional
Kytkin	D-link DGS-1008D 8-porttinen 10/100/1000Mb/s			

Kuva 26: VMware View testiympäristö

4 Testaus

Testauksen arvioitavat kohteet on valittu ISO 9126 - standardin jaottelun mukaisesti. Keski-tyimme arvioinnissa tuotteiden ylläpidettävyyteen, käytettävyyteen ja ratkaisuiden toimivuuteen IT-palveluiden tarpeita silmälläpitäen (kuva 27). Arviointitaulukon on tarkoitus tuoda lisäinformaatiota Laurea IT-palveluille tulevien suunnitelmien avuksi. VMwaren lisenssiehdot kieltävät tuotteiden suorituskyvyn mittauksen ja niiden esittämisen ilman erillistä lupaa. Tuotteiden suoranaisten vertailu ja testaus olisikin erittäin vaikeaa niiden eroavaisuuksien vuoksi. Tämän vuoksi testauksen tulokset ovat työn tekijöiden subjektiivisia arvioita ja huomioita.

Tuotteiden liitettävyyden puolesta molemmat ratkaisut olivat melko tasaväkisiä. Ne pystyttiin liittämään osaksi nykyistä ympäristöä, mikä vaatisi ainoastaan AD:n toiminnallisuuden tason nostamisen Windows Server 2008 tasolle. Asennettavien komponenttien määrässä Microsoft vie selkeän voiton, mikä näkyy laajempaan määrään erilaisia hallintatyökaluja, sekä vaatii enemmän suunnittelutyötä. VMwaren asentamiseen käytetty aika oli noin kolmasosa,

siitä mitä Microsoftiin kului. Microsoftin ratkaisun positiivisia puolia olivat helposti omaksuttavat käyttöliittymät, tuotteiden yhteensopivuus olemassa olevien järjestelmien kanssa ja laajennettavuus System Center ratkaisuilla.

VMwaren järjestelmää puolsi yhtiön pitkä kokemus virtualisoinnista, mikä näkyi ratkaisun ominaisuuksien määrässä ja käytettävyydessä. VMware View 4 jätti positiivisen vaikutelman, vaikka emme hyödyntäneet testauksessa sen kaikkia ominaisuuksia (Composer, Offline Desktops). Yksi hyvistä VMwaren ominaisuuksista on muistin ylivaraus minkä ansiosta, ESX-palvelimella pystytään ajamaan useampia virtuaalikoneita pienemmällä keskusmuistin kuluksella. Microsoftin VDI-toteutus pelkällä Hyper-V managerilla ei pärjää VMwaren vCenterin hallintaominaisuuksille. Microsoftin toteutuksesta jää kaipaamaan VMwaren Linked Clones - ominaisuutta, mikä mahdollistaa nopean virtuaalikoneiden provisioinnin golden-imagesta ja tehokkaan levytilan käytön. SCVMM:n avulla voidaan kyllä kloonata koneita kohtuullisen nopeasti mallitiedostoista. Nopeaa provisiointia vaativia tilanteita tulisi varmasti eteen esimerkiksi laboratorioympäristöissä ja luokkatilojen koneiden päivityksissä. golden-imagin avulla käyttöjärjestelmän päivitykset voitaisiin tehdä vain yhteen levykuvaan, mikä helpottaisi merkittävästi ylläpidon työtä.

Palvelimella sijaitsevien virtuaalikoneiden hiiren, näppäimistön- ja näytön liikkeet täytyy välittää käyttäjälle. Valittu etäyhteysprotokolla määrittelee sen kuinka sovellusten liikuttelu, ruudun päivitys ja multimediiasisällöt toistuvat loppukäyttäjälle. VDI-ympäristöjen haasteena on ollut perinteisesti täydellisen käyttökokemuksen tarjoaminen. Verkon viiveellä on suorainen vaikutus niihin protokolliin, jotka toimivat TCP/IP:n päällä. Testauksessa kävi hyvin ilmi, miten eri protokollat sopivat eri käyttötarkoituksiin. Microsoftin kehittämän RDP 7.0:n etuna oli asiakaspäässä tapahtuva multimedian renderöinti (multimedia redirection), mikä oli vakuuttavaa esimerkiksi HD-videoita toistettaessa Windows Media Playerin avulla. Osa multimedian ja grafiikan renderöinnistä voidaan siirtää vieraskoneen näytönohjaimelle. VMwaren protokollan ehdottomana vahvuutena oli PCoIP:n tarjoama ruudunpäivitys normaalissa käytössä, minkä ansiosta välillä oli todella vaikeaa erottaa virtuaalikone paikallisesta työasemasta. Tarkkuuden huomasi etenkin nopeissa liikkeissä ja kuvankäsittelyohjelman kanssa. VMwaren ratkaisussa voidaan antaa käyttäjälle oikeus valita kumpaa protokollaa hän käyttää istunnonaan (RDP tai PCoIP), mikä parantaa käyttökokemusta. Molemmilla protokollilla oli omat vahvuutensa. Raskaassa multimediakäytössä on hyvä, että osa renderöinnistä voidaan siirtää työaseman näytönohjaimen harteille. Molemmat ratkaisut tukevat laajaa kirjoa paikalliseen koneeseen kytkettyjä lisälaitteita, kuten tulostimia, muistitikkuja, ulkoisia kovalevyjä, web-kameroita, sekä kuulokkeita. Etäohjelman asetuksista tulee valita mitä laitteita otetaan käyttöön ja näytetään vieraskoneessa. Parhaimmillaan laitteet toimivat heti kytkemisen jälkeen ja näkyivät täysin oikein vieraskoneella.

Käyttökokemuksen arviointiin hyödynsimme ohjelmia (esim. Microsoft Office 2007, Adobe Photoshop CS4, Adobe Reader ja flash-vidoot), joita käytetään yleisesti opetuksessa Laurea-ammattikorkeakoulussa. Valitsimme edellä mainitut sovellukset, jotta pystyimme simuloimaan todellisia käyttötarkoituksia käytännössä. Esimerkiksi kuvankäsittelyohjelmalla pystyimme testaamaan tiedonsiirtoprotokollien tarkkuuksien eroavaisuuksia. Toimistotyökaluilla taas pystyimme testaamaan yleisimpien sovelluksien (Microsoft Word ja Excel) toimivuutta virtualisoidussa ympäristössä, koska ne eivät eroa toiminnaltaan yleisimmistä ohjelmista.

Testauksen arviointitaulukko		
asteikolla 1 (heikko) - 5 (erinomainen)		
	Microsoft	VMware
toiminnallinen laatu		
vastaavuus käyttäjän tarpeiden kanssa	3	5
liitettävyyys käyttöympäristöön	4	4
Luotettavuus		
tuotteenkypsyys	3	4
vikasietoisuus	2	4
toipumisvalmius	4	4
Käytettävyys		
ymmärrettävyyttä	3 ¹	4
käytön rationaalisuus	3	4
käyttäliittymä ja sen opittavuus	3	4
USB-muistitikku	2 ²	4
microfoni (äänen nauhoitus)	- ³	- ³
videon toisto (WMV)	5 ⁴	3
videon toisto (avi)	5	3
videon toisto (Flash)	4	4
Kuulokkeet, MP3 (äänenohjaus)	5	5
Ylläpidettävyys		
rakenteellinen selkeys	2	4
johdonmukaisuus	2	4
virheilmoitusten taso	2	5
Siirrettävyys		
alusta- ja ympäristöriippumattomuus		
asennusrutiinit	3	5
päivitettävyys ⁵	4	5
ka.	3,3	4,2

Kuva 27: Testauksen arviointi

1. Riippuu kirjautumistavasta (linkki työpöydältä vai web access)
2. Avaa kehotuksen isäntäkoneessa. Muistitikku näkyy samanlaisena kuin paikalliset asemat, ei tuttua (esim. Kingston) merkintää.
3. Järjestelmän tuettu ominaisuus, mutta ei voitu testata puuttuvien ajureiden vuoksi.
4. Windows Media Player multimedia redirection on päällä.
5. Virtuaalisten työpöytien päivittäminen.

4.1 Johtopäätökset

Molempien valmistajien ratkaisuja voitaisiin hyödyntää opetuskäytössä. Peruskäytössä käyttökokemus vastasi paikallisesti asennettua työasemaa. Raskailla sovelluksilla eron saattoi kuitenkin huomata selvemmin epätarkkuutena, viiveenä ja esimerkiksi videokuvan pikselöitymisinä. Microsoftin ratkaisu käytännössä vaatii SCVMM-palvelimen käyttöönoton isommissa to-teutuksissa, muuten hallinta saattaa muodostua pullonkaulaksi. Kaikkea ei kannata virtuali-soida yhdellä ratkaisulla, eikä se ole järkevää. Suunnitteluvaiheessa tulee huomioida erilais-ten käyttäjäryhmien tarpeet. VDI-ympäristöissä eniten haasteita tuottavat raskaat graafiset sovellukset, multimedia, sekä paljon tiedonsiirtokapasiteettia vaativat ohjelmat. Monissa palvelimissa on integroitu näytönohjain, mikä on rajoitteena ohjelmissa, jotka vaativat tehoa grafiikkapiiriltä palvelimen päässä. Laurean tapauksessa olisi järkevintä suunnitella ympäristö erilaisten käyttäjäryhmien perusteella. Yhdellä RDSH-palvelimella voidaan palvella, jopa sato-ja käyttäjiä ja tarjota perussovellukset Remote App:n kautta tai App-V:n avulla. Laboratorioi-hin taas soveltuvat paremmin työpöytäpoolit. Eri teknologioita yhdistelemällä voidaan voittaa useimmat työpöytävirtualisointiin liittyvät haasteet.

Nykyisellään ympäristöjen käytettävyydessä, rakenteessa ja hallittavuudessa on vielä huomattavia etuja VMwaren suuntaan, mutta tuotteet kehittyvät jatkuvasti. Kuilua tulee kuromaan kiinni Microsoftin tuleva Service Pack 1 -päivitys, joka tulee Windows 7:lle ja Server 2008 R2:lle vuoden 2011 ensimmäisellä neljänneksellä. Päivitys tuo mukanaan tuen dynaamiselle muistinkäytölle, jonka avulla Hyper-V osaa VMwaren tapaan jaella keskusmuistia eri virtuaali-koneiden kesken. Dynamic Memory ominaisuuden lisäksi päivityksessä tulee RemoteFX-laajennus, mikä parantaa 3D-grafiikan toimivuutta, sekä videoiden- ja korkealaatuisen äänen siirtoa etätyöpöytäyhteydessä. (Kotilainen 2010; Paljon uutta tulossa 2010.)

4.2 Kehitysehdotukset

Työpöytien virtualisointi olisi hyvä aloittaa laboratorioista, missä tietojenkäsittelyn opiskelijat tekevät harjoitustöitä ja demoympäristöjä. Näin opiskelijoille voitaisiin tarjota useita valmiita ympäristöjä järjestelmänvalvojan oikeuksilla, ilman huolta peruuttamattomista vahingoista. Projektin tai päivän päätteeksi koneet voitaisiin aina palauttaa aikaisempaan tilaan, jonka

jälkeen seuraavat opiskelijat saavat käyttöönsä puhtaan työpöydän. Nykyisessä tilanteessa hyödynnetään vaihtolevykelkallisia työasemia, joiden ylläpito kuormittaa IT-palveluita. Samaa ratkaisua voitaisiin hyödyntää myös infopäätteissä, joista opiskelijat pystyvät tarkistamaan opiskeluun liittyviä tietoja. Nämä koneet voitaisiin palauttaa aina uloskirjautumisen jälkeen palautuspisteeseen, jolloin näiden koneiden ylläpitoon vaadittu panos on minimaalinen ja ne pysyvät tehokkaina. Alkuvaiheessa voitaisiin jatkaa nykyisten laitteiden elinkaarta käyttämällä niitä päätelaitteina. Myöhemmässä vaiheessa voitaisiin siirtyä asteittain kevytpäätteiden käyttöön.

Toteutusympäristöön olisi järkevää määrittää koulutusalaakohtaiset virtuaalisten työpöytien varannot, joista opiskelijoille tulisi aina tuore ja puhdas työpöytä. Käyttäjien tiedostot tallensivat eri sijaintiin, näin opiskelija voisi kirjautua miltä tahansa päätteeltä ja saisi omat tiedostonsa käyttöön. Työaseman sovellukset voisivat olla vain kaikille samat perusohjelmat ja Office tuotteet. Muut sovellukset tarjottaisiin käyttäjälle sovellusvirtualisoinnin ja terminaalipalveluiden kautta koulutusalaakohtaisesti. Näin esimerkiksi turva-alan opiskelijat saisivat sovellukset, joita he tarvitsevat ja liiketalouden opiskelijat omansa.

5 Huomioitavia asioita virtualisointiprojektissa

Yksi työn tavoitteista oli selvittää, mitä virtualisoinnissa tulee ottaa huomioon. Olemme keränneet tähän osioon asioita ja mietteitä, jotka ovat tulleet esille työtä tehdessä. Toteutusympäristöä suunnitellessa tulisi olla tietoinen ainakin seuraavien asioiden vaikutuksista lopputulokseen: tallennus, tietoturva, tiedonsiirto, lisensoinnin vaikutuksista kustannuksiin sekä ympäristön käytettävyys ja lisälaitteiden toimivuus.

5.1 Tallennus

Työasemien virtualisoinnissa tallennusjärjestelmät ovat olennaisessa osassa, koska tieto pitää saada varmistettua turvallisesti. Tallennusten siirtyessä perinteiseltä työasemilta palvelimille täytyy tietojen olla kahdennettu, jotta mahdollisista vikatilanteista toipuminen onnistuu menettämättä suurta määrää dataa. Tallennuksen tehokkuus ja sekä levyjen I/O-nopeus ovat käytettävyyden takia huomioitava tarkoin, sillä palvelimien tallentaessa tietoa usealta käyttäjältä samanaikaisesti levyjen hidas I/O voi muodostua käytettävyyden pullonkaulaksi. Käyttöjärjestelmien toiminnan kannalta olennaista on levyjärjestelmän luku- ja kirjoitusoperaatioiden suorituskyky. Monet isot toimijat tarjoavat työpöytävirtualisointiin nopeita ssd-levyjärjestelmiä niiden alhaisen hakuajan vuoksi, näin tallennusjärjestelmä kykenee palvelemaan järjestelmiä hyvin nopeasti pienellä viiveellä. Ssd-järjestelmillä on myös monia muita etuja verrattuna perinteisiin levyihin esim. virrankulutus, luku- ja tallennusnopeus. Uuden

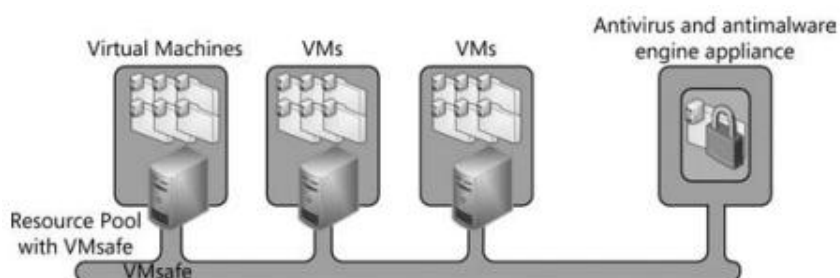
levytekniikan negatiivisena puolena voidaan pitää verrattain korkeaa kustannustasoa perinteisiin levyjärjestelmiin suhteutettuna.

(Understanding how storage 2010.)

5.2 Tietoturva

Virtualisoitu ympäristö ei yksinään ole sen tietoturvasempi kuin fyysinen. Verkkoympäristössä laitteet näkyvät samalla lailla ja samat tietoturvaohjelmat ovat vaaroina. Tietoturvasta tulee pitää huolta, virtuaalisia laitteita tulee käsitellä ja ajatella aivan kuin ne olisivat fyysisiä laitteita. Virtuaalikoneen saadessa virustartunnan se voidaan palauttaa esim. aikaisemmassa palautuspisteessä olevaan tilaan. Tätä kannattaa kuitenkin tehdä harkitusti, sillä se saattaa hävittää jotain dataa mitä ei ole välttämättä vielä tallennettuna uusimpaan palautuspisteeseen. (Ruest & Ruest 2009, 32.)

Jos käytössä on VMware ESX Server, tulisi käyttää VMsafe:a. VMsafe pyörii suoraan ESX hypervisorilla säätäen yleisimmät antimalware ja antivirus työkalut suoraan sen päällä (kuva 28). Tämän takia ei ole tarvetta lisätä virusturvatyökaluja virtuaalikoneille, jotka ovat hypervisorin päällä. Jokainen virtuaalikone joka on asennettu VMsafen avulla hypervisorille, on automaattisesti suojattu. VMsafe tarkistaa tärkeimmät VM komponentit kuten muistit, prosessorin, verkon ja levyt. VMsafe on uusi tapa suojata virtuaaliset koneet ja tulee olemaan käytettävissä tulevaisuudessa uusissa vSphere versioissa. Tämä suojaus tapa on osoittautunut niin toimivaksi, että Linux ja Xen-pohjaiset, komponentit. ovat kehittämässä samanlaista toiminnallisuutta. Tämänkaltaisten toiminnallisuuksien odotetaan yleistävän tulevaisuudessa hypervisorien päälle. Mikäli käytössä on Microsoftin Hyper-V tai Citrixin XenServer tulisi asentaa normaali virustorjuntaohjelma ajettaviin virtuaalikoneisiin. (Ruest & Ruest 2009, 335.)



Kuva 28: VMwaren VMsafe toimii hypervisorin päällä ja turvaten virtuaaliset koneet (Ruest & Ruest 2009, 335)

5.3 Tiedonsiirto

Verkon kaistanleveys, kuormitus ja mahdolliset ongelmakohdat on syytä kartoittaa huolella ennen toteutusympäristöön siirtymistä. Selvitetyin verkkokapasiteetin perusteella saadaan arvio siitä, mitä palveluita pystytään tuottamaan esim. virtuaalikoneiden siirto lennossa paikasta toiseen tai iSCSI liikenne tallennusjärjestelmään. Selvityksessä tulee myös kartoittaa verkkoympäristön komponenttien (reitittimien ja kytkimien) tila, ovatko ne kuinka uusia ja kestävätkö kuinka suurta verkon rasitusta. (Ruest & Ruest 2009, 70,73.)

5.4 Lisensointi ja kustannukset

Ohjelmistojen lisensointi on kuvaus siitä kuinka käyttäjä voi käyttää tuotetta. Lisensoinnissa määritetään mihin ohjelmistoa voidaan käyttää, milloin sitä voidaan käyttää ja kuinka pitkään sitä voidaan käyttää. Työpöytien virtualisoinnissa lisensointi ei ole kaikkein yksiselitteisin tehtävä johtuen jatkuvasti muuttuvista lisenssiehdoista. Tarkat kustannuslaskelmat ovat tämän työn rajauksen ulkopuolella, mutta käsittelemme muutamaa lisenssiä, jotka tulee ottaa huomioon käytettäessä Microsoftin tuotteita VDI-ympäristöissä riippumatta valitusta ratkaisusta. (Sempf 2009, 1.)

Virtual Enterprise Centralized Desktop (VECD) on lisenssi Windows vieraskäyttöjärjestelmille, joita suoritetaan datakeskuksesta. VECD lisenssi vaaditaan jokaisessa VDI-ympäristössä, jossa Windowsia suoritetaan vieraskäyttöjärjestelmänä (guest). (Russel & Zacker 2010, 62.)

Jokaisella käyttäjällä tai laitteella, jolla on suora tai epäsuora pääsy Windows Serverin palveluihin graafisella käyttöliittymällä täytyy olla Windows Server RDS Client Access License (CAL). RDS toiminnallisuus on mielletty niiksi ominaisuuksiksi ja palveluiksi, jotka tulevat voimaan RDS-roolin asennuksen yhteydessä. Nämä pitävät sisällään esimerkiksi RD Gateway, RemoteApp, RD Web Access ja Connection Broker roolit. RDS CAL lisenssejä on saatavilla per käyttäjä tai per laite kohtaisina. VMwaren View -ratkaisussa ei tarvita RDS-lisenssiä, koska View Agent hoitaa saman toiminnallisuuden Microsoftin RDS:n sijasta. Lopulliset lisensointikustannukset määrittyvät voimassa olevan sopimushinnaston (Campus lisensointi) mukaisesti, sekä valitun ratkaisun perusteella. Lisäksi kustannukset vaihtelevat suuresti riippuen siitä käytetäänkö palveluita Laurean sisäverkosta vai ulkopuolelta. Ohjelmistojen lisenssiehdot vaihtelevat toimittajittain ja ne tulee tarkistaa yksittäistapauksina. (Russel & Zacker 2010, 60.)

Työpöytien virtualisointi ei välttämättä tuo laitteistokustannuksissa itsessään suoraa säästöjä, vaan vaatii alkuvaiheessa lisäinvestointeja uusien palvelimien ja tallennusjärjestelmien muodossa. Selkeitä säästöjä on mahdollista saada aikaiseksi pidemmällä aikavälillä kevytpäätteil-

lä, mitkä kuluttavat vähemmän energiaa ja omaavat pidemmän käyttöiän. Yksi vaihtoehto on pidentää olemassa olevan laitteiston vaihtoväliä ja käyttää niitä pelkkinä päätelaitteina. Hallintakustannusten laskeminen edellyttää lähtötilanteen prosessien mittaamista. Ympäristön hallintaa voidaan virtualisoinnin avulla tehostaa ja sitä myötä saavuttaa kustannussäästöjä henkilöstökuluissa. Työlle pitää olla mitattuna arvo ja tehtävään käytetty aika, jotta sitä voidaan verrata saavutettuun hyötyyn.

5.5 Käyttökokemus ja lisälaitteet

VDI-ympäristössä on olennaista kiinnittää huomiota lisälaitteiden toimivuuteen. Käyttäjäkemuksen kannalta on tärkeää, että USB-laitteet toimivat kuten aikaisemmin ja tulostaminen onnistuu paikalliseen tulostimeen, vaikka itse työpöytä sijaitsee palvelimen päässä. Käyttökokemuksen tulisi olla vähintään yhtä hyvä kuin perinteisellä työasemalla, jotta muutos olisi loppukäyttäjän kannalta mahdollisimman huomaamaton. Virtualisoidussa ympäristössä lisälaitteiden kanssa esiintyy samanlaisia ongelmia kuin tavallisessakin ympäristössä, osa laitteista vaatii erillisen ajurin asentamista koneelle. Lisälaitteiden toimivuus ja käytettävyys vaihtelee eri ratkaisuiden välillä. Asia tulisi ottaa huomioon toteutusympäristöä suunnitellessa ja testata huolellisesti.

Sovellusten toimivuuteen ja yleiseen käyttöjärjestelmän sulavuuteen vaikuttaa paljon valittu ratkaisu ja sen tarjoamat etäyhteysprotokollat. Hyvä esimerkki tästä on VMwaren hyödyntämä PCoIP, joka käyttää UDP:tä tiedonsiirto-protokollana. UDP ei lähetä varmistuspaketteja toisin kuin TCP/IP -pohjaiset protokollat (RDP), mikä johtaa sulavampaan ruudunpäivitykseen ja tarkkuuteen graafisissa ohjelmistoissa. WAN-yhteyksissä protokollien merkitys kasvaa entisestään verkon viiveen takia.

6 Yhteenveto

Työpöytävirtualisoinnin hyödyntäminen vaatii paljon resursseja, suunnittelutyötä ja tietotaitoa. Osaamista pitää löytyä niin tallennuksesta, tietoverkoista, palvelinympäristöstä, työasemista kuin tietoturvallisuudesta ja virtuaaliympäristöjen hallinnasta. Edellytyksenä onnistuneelle projektille on selkeä valmistelu ja suunnitteluvaihe. Pitää olla tieto siitä, mitä halutaan saavuttaa ja millä ratkaisulla. Olemassa olevat resurssit on syytä kartoittaa ja selvittää mahdolliset pullonkaulat, puhumattakaan vallitsevista lisenssiehdoista. Kustannusten laskemiseen ja olemassa olevan infrastruktuurin kartoittamiseen löytyy valmiita työkaluja, esimerkiksi Microsoft Assessment and Planning (MAP) ja VMware TCO/ROI Calculator. (Roi Tco Calc 2010; Realize value 2010.)

Tulevaisuudessa käyttöjärjestelmän rooli tulee muuttumaan enemmän väyläksi pilvipalveluille (Cloud Computing). Testatuilla ratkaisuilla voidaan jo nyt toteuttaa erittäin monipuolisia ympäristöjä sekä muuttaa perinteistä ylläpidon mallia tehokkaammaksi. Asennuksia ja hallintaa ei välttämättä ole järkevää enää tehdä niin kuin on aikaisemmin totuttu tekemään, vaan viimeistään Windows 7 -käyttöjärjestelmään siirryttäessä tulisi miettiä ohjelmien jakelua, asennusta sekä ylläpitoa uudestaan. Opetuksen näkökulmasta tämä tarjoaa entistä joustavampaa tietojenkäsittelyä ajasta ja paikasta riippumatta. Työpöytien virtualisoinnilla saavutettavat hyödyt hallinnassa, tietoturvallisuudessa ja joustavuudessa ovat kiistattomat, mutta vasta perusteellisella suunnittelulla saadaan arvioitua onko se taloudellisesti kannattavaa.

Mikäli halutaan hyödyntää työpöytävirtualisointia tuotantoympäristössä, sitä olisi hyvä käyttää ensin pienemmässä mittakaavassa, jossa loppukäyttäjät toimivat testaaajina. Näin saadaan todellisia arvioita järjestelmän toimivuudesta ja pystytään laskemaan aidoista käyttötilanteista aiheutuva kuormitus. Laskelmien perusteella pystytään mitoittamaan oikeassa suhteessa laajempien ympäristöjen vaatima kapasiteetti. Näiltä osin testauksemme tulokset jäivät toteutumatta.

Opinnäytetyö oli aiheeltaan erittäin ajankohtainen ja avasi aivan uuden näkökulman tietojenkäsittelyn tulevaisuuteen. Esille nousi vahva kysymys siitä, mikä on perinteisen käyttöjärjestelmän rooli tulevaisuudessa. Tarvitaanko enää nykyisessä muodossa olevaa massiivista alustaa vai riittääkö suurelle osalle käyttäjistä pelkkien ohjelmien ja palveluiden tarjonta palvelinsalista suoraan alustariippumattomaan päätelaitteeseen?

Työn aikana opimme todella paljon uutta ja saimme luotua paljon uusia kontakteja alan ihmisiin. Pystymme hyödyntämään työssä opittuja asioita omalla uralla. Aineiston kasaamisen ja kirjoittamisen lomassa opimme näkemään aikataulutuksen merkityksen projektien onnistumisen kannalta entistä selkeämmin.

Lähteet

Application Virtualization. 2008. Application Virtualization Solutions Overview and Feature Compare Matrix. Viitattu 10.4.2010.

<http://communities.vmware.com/servlet/JiveServlet/download/1151141-18142/ApplicationVirtualizationSolutionsOverviewandFeatureMatrix.pdf>

Application Virtualization Whitepapers 2010. Microsoft. Viitattu 22.03.2010.

<http://technet.microsoft.com/en-us/appvirtualization/cc843994.aspx>

Boyles, T. 2010. CCNA Security Study Guide: Exam 640-553. Yhdysvallat: Wiley Publishing, Inc.

Casselman, B., Kaplan, S.& Reeser, T. 2009. Citrix XenApp Platinum Edition for Windows: The Official Guide. Yhdysvallat: The McGraw-Hill Companies.

Centralized Management. 2010. Microsoft. Viitattu 26.10.2010.

<http://www.microsoft.com/systemcenter/appv/infrastructure.msp>

Citrix Desktop Virtualization. 2010. The Citrix guide to desktop virtualisation. Viitattu 12.6.2010.

http://www.citrix.com/%2Fsite%2Fresources%2Fdynamic%2Fsalesdocs%2FCitrix_Guide_to_desktop_virtualisation.pdf

Citrix Online Plug-in. 2009. Citrix. Viitattu 15.10.2010.

<http://support.citrix.com/proddocs/index.jsp?topic=/xenapp5fp2-w2k3/ps-gs-overview-plugin-online-fp2.html>

Citrix XenApp. 2010. Conguide. Viitattu 13.11.2010.

http://www.conguide.com/media/6804/citrix_xenapp_500x309.jpg

Debloying Virtual Desktop Pools. 2010. Microsoft. Viitattu 21.9.2010

<http://www.microsoft.com/downloads/en/confirmation.aspx?FamilyID=e33b0953-e89a-4b97-a6fe-60da44add5c7>

Desktop Virtualization 2010. Microsoft. Viitattu 22.03.2010.

<http://www.microsoft.com/virtualization/en/us/products-desktop.aspx>

Dittner, R. & Rule, D. 2007. The best damn virtualization book period. Yhdysvallat: Syngress Publishing.

Domain Controller Roles. 2010. Microsoft. Viitattu 27.10.2010.

<http://technet.microsoft.com/en-us/library/cc786438%28WS.10%29.aspx>

ESX Hardware Requirements. 2010. VMware. Viitattu 30.10.2010.

http://pubs.vmware.com/vsp40/wwhelp/wwhimpl/js/html/wwhelp.htm#href=install/c_esx_hw.html

Facts About Microsoft. 2010. Microsoft. Viitattu 10.11.2010.

http://www.microsoft.com/presspass/inside_ms.msp

Golden, B. 2009. Virtualization For Dummies®, 2nd Sun and AMD Special Edition. Yhdysvallat: Wiley Publishing, Inc.

HDX overview. 2010.Citrix. Viitattu 20.04.2010. <http://hdx.citrix.com/hdx-overview>

Introducing Citrix XenApp 2010.Citrix. Viitattu 04.11.2010.

<http://www.citrix.com/English/ps2/products/product.asp?contentID=1297817>

Introducing RemoteApp and Desktop Connections. Viitattu 17.4.2010.

<http://blogs.msdn.com/b/rds/archive/2009/06/08/introducing-remoteapp-and-desktop-connections.aspx>

Kivimäki J. 2009 Windows Server 2008R2 Tehokas hallinta. Kariston Kirjapaino Oy, Hämeenlinna.

Knowledge Base. 2010. VMware. Viitattu 30.10.2010.

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015858

Kotilainen, S. 2010. Kotilainen S. Windows 7 Service Pack 1 RC tuli jakeluun. Viitattu 27.10.2010. http://www.tietokone.fi/uutiset/windows_7_service_pack_1_rc_tuli_jakeluun

Laurea numeroin 2009. Laurea. Viitattu 15.4.2010.

http://www.laurea.fi/internet/fi/03_tietoa_laureasta/01/01_Esittely/04_Laurea_numeroin/index.jsp

Long, J. 2006. Storage networking protocol fundamentals. Yhdysvallat: Cisco Press

LUN, 2009. Viitattu 1.11.2010.

http://4.bp.blogspot.com/_TtKS8btMDV0/R49aKW_Vn4I/AAAAAAAAADg/3-seOVv3Qml/s1600-h/Screenshot_3.jpg

Microsoft VDI Overview. 2009. Msdn. Viitattu 12.02.2010.

<http://blogs.msdn.com/rds/archive/2009/08/19/microsoft-vdi-overview.aspx>

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. WSOYpro Oy. Helsinki.

Optimizing HDX Technologies.2010. Citrix. Viitattu 13.9.2010.

<http://support.citrix.com/servlet/KbServlet/download/23686-102-646022/Best%20Practices%20for%20Optimizing%20HDX%20Technologies%20for%20XenDesktop%204.pdf>

Paljon uutta tulossa. 2010. Microsoft. Viitattu 20.10.2010.

http://www.microsoft.com/finland/subscribe/example/Technet_uutiskirje_huhtikuu.htm

Products & Solutions. 2010. Citrix. Viitattu 12.10.2010.

<http://www.citrix.com/English/ps2/products/product.asp?contentID=1857200>

Realize value. 2010. Microsoft. 20.11.2010. www.microsoft.com/virtualization/ROItool/default.aspx

Remote Desktop Connection 7. 2009. Msdn. Viitattu 17.05.2009.

<http://blogs.msdn.com/b/rds/archive/2009/08/21/remote-desktop-connection-7-for-windows-7-windows-xp-windows-vista.aspx>

RD Session Host. 2010. Microsoft. Viitattu 12.02.2010.

<http://technet.microsoft.com/en-us/library/cc742822.aspx>

RD Virtualization Host, 2010. Microsoft. Viitattu 1.11.2010. <http://technet.microsoft.com/en-us/library/dd759170.aspx>

RD Web Access. 2010. Microsoft. Viitattu 12.02.2010.

<http://technet.microsoft.com/en-us/library/cc731923.aspx>

Roi Tco Calc. 2010. VMware. Viitattu 20.11.2010.

www.vmware.com/products/vi/calculator.html

- Ruest, D. & Ruest, N. 2009. Virtualization: A Beginner's Guide. Yhdysvallat: The McGraw-Hill Companies.
- Russel, C. & Zacker, C. 2010 Introducing Windows Server 2008 R2. Yhdysvallat: Microsoft Press
- Sempf, B. 2009. Licensing Windows Server 2008 For Dummies Microsoft Special Edition. Yhdysvallat: Wiley Publishing, Inc.
- Storage layer 2008. Clennetwork. Viitattu 22.5.2010.
<http://www.cleannetwork.com/news/i/storagelayer.gif>
- Technical Overview of Windows Server 2009. Microsoft. Viitattu 14.05.2010.
http://download.microsoft.com/download/5/B/D/5BD5C253-4259-428B-A3E4-1F9C3D803074/RDS_TDM_Whitepaper.docx
- Tooley, S. 2009. The Real Citrix CCA Exam Preparation Kit: Prepare for XenApp 5.0. Yhdysvallat: Syngess Publishing, Inc.
- Tulloch, M. 2009. Understanding Microsoft Virtualizations From the Desktop to the Datacenter. Yhdysvallat: Microsoft Press
- Understanding Clones. 2010. VMware. Viitattu 14.10.2010.
http://www.vmware.com/support/ws55/doc/ws_clone_overview.html
- Understanding how storage. 2010. Brian Madden Viitattu 17.11.2010.
<http://www.brianmadden.com/blogs/rubenspruijt/archive/2010/05/02/vdi-and-storage-deep-impact.aspx>
- Virtual Machine Manager. 2010. Microsoft. Viitattu 27.10.2010.
<http://www.microsoft.com/systemcenter/en/us/virtual-machine-manager.aspx>
- Virtualisointi suomalaisissa organisaatioissa 2009. Mext. Viitattu 29.04.2010.
<http://mext.fi/tutkimukset/virtualisointi-suomalaisissa-organisaatioissa-2009>
- VMM Overview 2008. Susanaguedes. Viitattu 11.11.2010.
http://susanaguedes.spaces.live.com/?_c11_BlogPart_pagedir=Last&_c11_BlogPart_BlogPart=blogview&_c=BlogPart
- VMM System Requirements 2008 R2. 2010. Microsoft. Viitattu 19.10.2010.
<http://www.microsoft.com/systemcenter/en/us/virtual-machine-manager/vmm-system-requirements-r2.aspx#comp>
- VMware Manager 4.2009. VMware View Manager 4 Easily Manage, Provision and Deploy Virtual Desktops Across the Enterprise. Viitattu 20.9.2010.
<http://www.vmware.com/files/pdf/VMware-View-Manager-4-DS-EN.pdf>
- VMware Overview 2010. VMware Company Overview. Viitattu 11.11.2010.
<http://www.vmware.com/files/pdf/VMware-Company-Overview-DS-EN.pdf>
- VMware ThinApp. 2010. VMware ThinApp Application Virtualization Made Simple Viitattu 4.11.2010.
<http://www.vmware.com/files/pdf/VMware-ThinApp-DS-EN.pdf>
- VMware ThinApp intro. 2008 VMware® ThinApp Agentless Application Virtualization Overview. Viitattu 7.10.2010.
http://www.vmware.com/files/pdf/thinapp_intro_whitepaper.pdf
- VMware ThinApp made simple. 2010. VMware. Viitattu 28.8.2010.

<http://www.vmware.com/products/thinapp/>

VMware Työasema virtualisointi. 2009. Ulmanen. Viitattu 18.02.2010.

<http://finland.emc.com/collateral/campaign/global/forums/vmware-tyoasemavirtualisointi-taysi.pdf>

VMware vCenter. 2009. VMware vCenter Server 4 Unify and Simplify Virtualization Management. Viitattu 12.10.2010. <http://www.vmware.com/files/pdf/VMware-vCenter-Server-4-DS-EN.pdf>

VMware View. 2010. VMware View Architecture Planning Guide. Viitattu 11.11.2010. http://www.vmware.com/pdf/view40_architecture_planning.pdf

VMware View 4 PCoIP. 2009. VMware View™ 4 with PCoIP information guide. Viitattu 18.9.2010. <http://www.vmware.com/files/pdf/VMware-View4-PCoIP-IG-EN.pdf>

VMware View 4.5 new features.2010.VMware. Viitattu 22.09.2010.

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027460

VMware View features. 2010. VMware. Viitattu 22.10.2010.

<http://www.vmware.com/products/view/features.html>

VMware vSphere 2009.Introduction to VMware vSphere. Viitattu 7.10.2010.

http://www.vmware.com/pdf/vsphere4/r40/vsp_40_intro_vs.pdf

What is Xen. 2010. Xen. Viitattu 13.10.2010. <http://www.xen.org>

Xen.org History. 2010. Citrix. Viitattu 1.11.2010.

<http://www.xen.org/community/xenhistory.html>

XenApp editions.2009. Citrix. Viitattu 16.02.2010.

<http://www.citrix.com/English/ps2/products/feature.asp?contentID=1686588>

XenApp how it helps.2010.Citrix. Viitattu 16.02.2010.

<http://www.citrix.com/English/ps2/products/feature.asp?contentID=1862682>

Xendesktop-technology. 2008. Vmetc. Viitattu 21.9.2010. <http://vmetc.com/wp-content/uploads/2008/07>

XenDesktop Components. 2010. Citrix. Viitattu 19.10.2010.

<http://support.citrix.com/proddocs/index.jsp?topic=/xendesktop-bdx/cds-overview-xd-components-bdx.html>

XenDesktop Features and Editions.2010. Citrix. Viitattu 15.10.2010.

<http://support.citrix.com/proddocs/index.jsp?topic=/xendesktop-bdx/cds-overview-features-wrapper-bdx.html>

XenServer editions. 2010. Citrix. Viitattu 19.10.2010.

<http://www.citrix.com/English/ps2/products/subfeature.asp?contentID=2300456>

Kuvaluettelo

Kuva 1: Virtualisoinnin kohteita (Ruest & Ruest 2009, 26)	11
Kuva 2 Mext virtualisointi Suomessa (Virtualisointi suomalaisissa organisaatioissa 2009)	12
Kuva 3: Käytetyimmän virtualisointi ratkaisut (Virtualisointi suomalaisissa organisaatioissa 2009)	12
Kuva 4: Ohjelmistopohjainen virtualisointi.....	14
Kuva 5: Vieraskoneet suoraan virtualisointikerroksen päällä	15
Kuva 6 Paravirtualisointi kerrokset	16
Kuva 7: Perinteisen ja virtualisoitujen sovellusten riippuvuudet toisistaan.....	17
Kuva 8: Microsoft App-V:n osakomponentit (Centralized Management 2010)	18
Kuva 9: VMware ThinApp sovellusten jakelu käyttäjille (VMware ThinApp made simple 2010)	19
Kuva 10: Kuvaus Citrix XenApp ympäristöstä (Citrix XenApp 2010)	20
Kuva 11: Tallennusvirtualisoinnin kerroksia (Storage layer 2008.)	21
Kuva 12: LUN näkymä tallennus järjestelmässä (LUN, 20009)	22
Kuva 13: Remote Desktop Servicen roolipalvelut (Russel & Zacker 2010, 45-46)	24
Kuva 14: Microsoft VDI komponentteja (RD Virtualization Host, 2010)	24
Kuva 15: Kirjautuminen Web Access:n avulla tarjolla oleviin ohjelmiin ja työpöytiin. .	26
Kuva 16: RDP 7.0 käyttökokemusten vertailu (Remote Desktop Connection 7)	27
Kuva 17: Järjestelmän toiminta View 4 (VMware View features 2010).....	28
Kuva 18: VMware View:n kuvaus (VMware View 2010, 10)	29
Kuva 19: vCenterin toimintamalli (VMware vCenter 2009)	31
Kuva 20: VMware päätelaitteet (VMware View 4 PCoIP 2009)	33
Kuva 21: Citrix XenDesktop 4 toimintamalli (xendesktop-technology 2008)	37
Kuva 22: Windows 7, RAD-feedinä näkyvät linkit Käynnistä-valikossa (Introducing RemoteApp and Desktop Connections.).....	38
Kuva 23: Testiympäristön kuvaus Microsoft VDI	41
Kuva 24: SCVMM kuvio (VMM Overview 2008)	42
Kuva 25: Administrator konsolin yleisnäkymä ympäristöstä	43
Kuva 26: VMware View testiympäristö	45
Kuva 27: Testauksen arviointi.....	47
Kuva 28: VMwaren VMsafe toimii hypervisorin päällä ja turvaten virtuaaliset koneet (Ruest & Ruest 2009, 335)	50

Liitteet

LIITE 1 Microsoft VDI testiympäristön asennusohje

LIITE 2 System Center Virtual Machine Manager 2008 R2 asennus

LIITE 3 VMware View 4 testiympäristön asennusohje

Liite 1 Microsoft VDI-ympäristön asennus

1. Virtuaalikoneen luominen Hyper-V:n avulla
2. infrastruktuurin asennus ja määrittely
3. Ympäristön toimivuuden testaus

Testiympäristön asennuksen tukena käytettiin seuraavia lähteitä, jotka on tulostettu Marras-kuussa 2009.

Installing Remote Desktop Session Host Step-by-Step Guide

(<http://www.microsoft.com/downloads/details.aspx?FamilyID=DA934121-F85D-4827-BB11-E17E9DB5D53A&displaylang=en&displaylang=en>)

Deploying Virtual Desktop Pools by Using Remote Desktop Web Access Step-by-Step Guide

(<http://www.microsoft.com/downloads/details.aspx?FamilyID=E33B0953-E89A-4B97-A6FE-60DA44ADD5C7&displaylang=en&displaylang=en>)

System Center Virtual Machine Manager 2008 R2 Deployment Guide

(<http://technet.microsoft.com/en-us/library/ee441285.aspx>)

Ympäristön Verkkoasetukset:

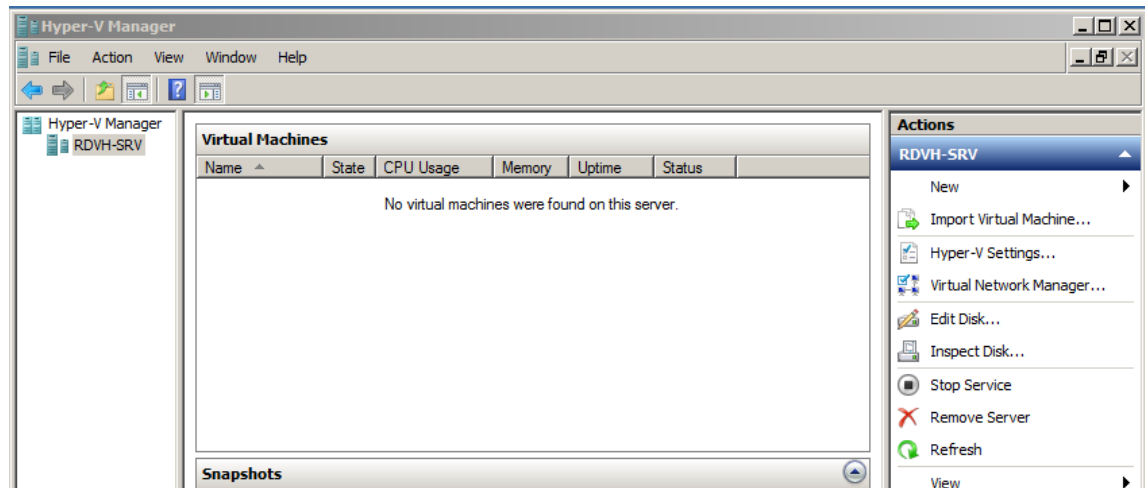
Palvelimet:	IP
RDCB-SRV	10.0.0.5
RDSH-SRV	10.0.0.2
RDVH-SRV	10.0.0.4
RDWA-SRV	10.0.0.6
Test-DC	10.0.0.1
SCVMM-SRV	10.0.0.10

Clientit:

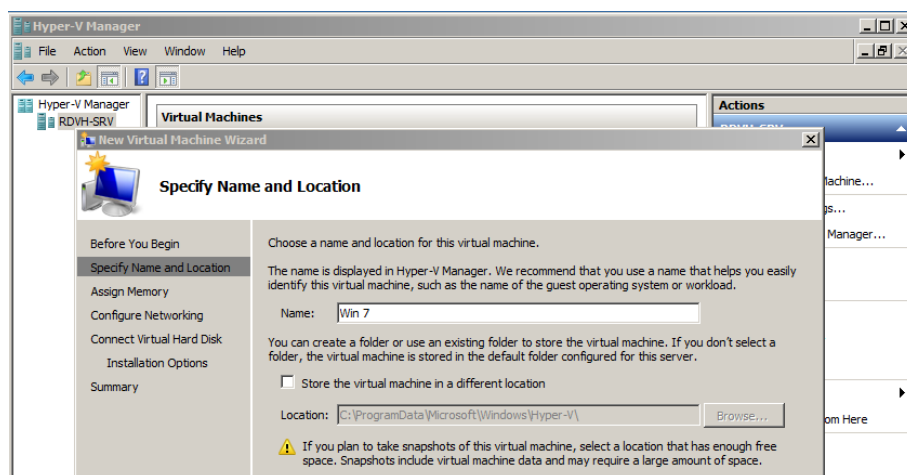
CLNT1 (Win7prof)	10.0.0.3
CLNT2 (WinXP prof)	10.0.0.15
VDP1-CLNT Win7prof	10.0.0.7
VDP2-CLNT Win7prof	10.0.0.8
VDP3-CLNT Win7ent1	10.0.0.9

1. VIRTUAALIKONEEN LUOMINEN HYPER-V:N AVULLA

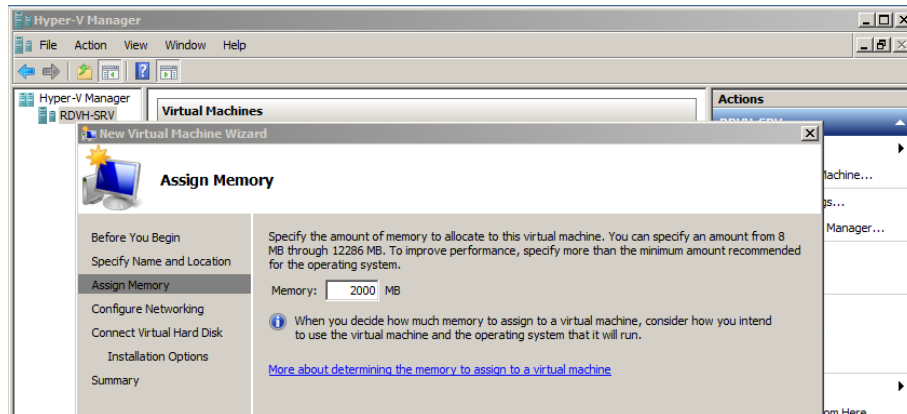
Tämän ohjeen avulla voidaan luoda virtuaaliset työasemat ja palvelimet testiympäristöä varten.



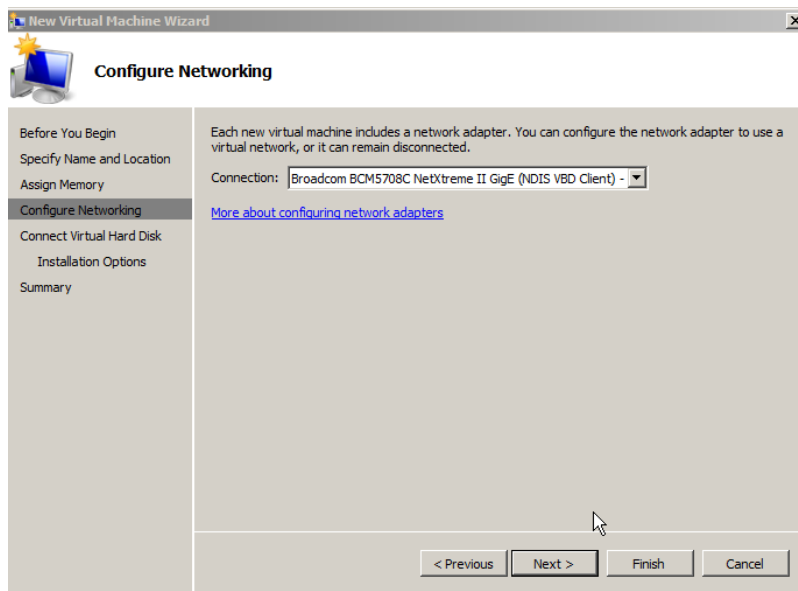
1.1 Avataan palvelimella Hyper-V Manager (RDVH) ja valitaan New -> Virtual Machine



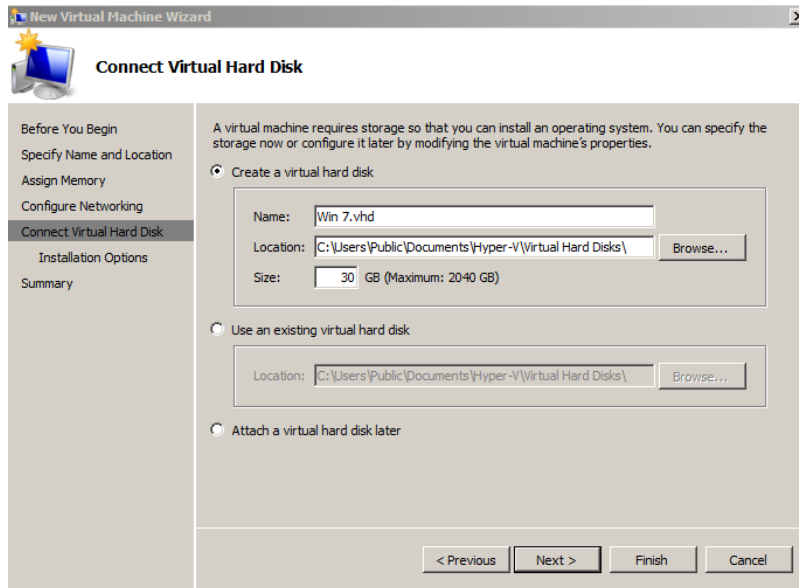
1.2 Annetaan virtuaalikoneelle nimi (esim. Vdp1-clnt) ja määritetään sen sijainti. Oletusasetuksilla kone tallennetaan palvelimen C:\ProgramData\Microsoft\Windows\Hyper-V\ kansioon, merkittävällä kohdan "Store the virtual Machine in a different location" voidaan kansiota vaihtaa. Siirrytään painamalla "next" eteenpäin.



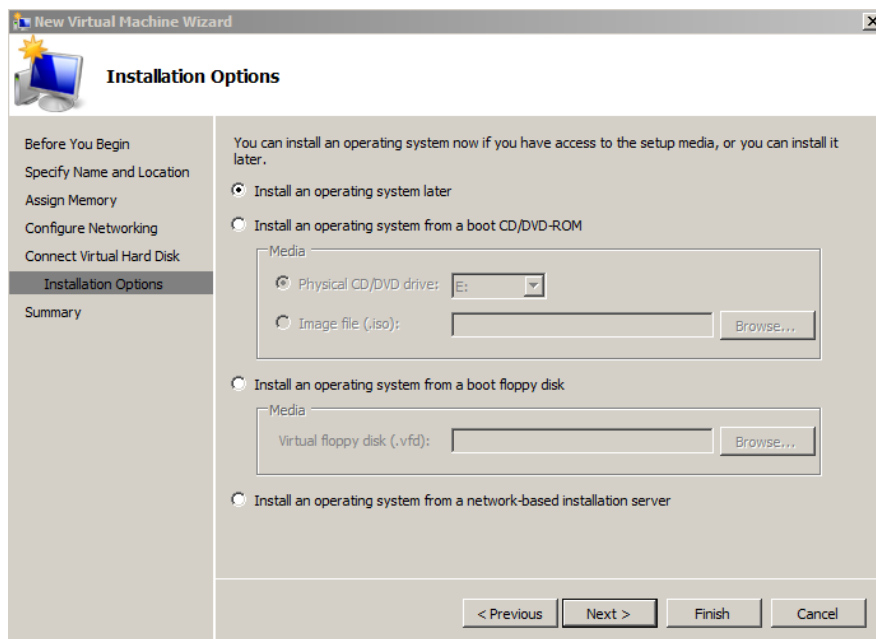
1.3 Annetaan koneelle haluttu määrä keskusmuistia. Muistia kannattaa varata koneen käyttöjärjestelmän vaatimusten ja tarkoituksen mukaisesti. Annoimme kaikille virtuaalikoneille käyttöön 2Gt muista. Siirytään painamalla "next" eteenpäin.



1.4 Valitaan koneelle verkkokortti jota virtuaalikone hyödyntää. Alasvetovalikosta saadaan listaus käytössä olevista vaihtoehdoista. Siirytään painamalla "next" eteenpäin.



1.5 Luodaan koneelle uusi virtuaalinen kovalevy (.vhd) ja valitaan sen sijoituspaikka. Tässä kohtaa voidaan määrittellä kuinka iso levytila koneelle varataan vai käytetäänkö aikaisemmin luotua levyä. Koneelle voidaan myös määrittellä, että vhd liitetään koneeseen myöhemmin. Annoimme koneelle 30Gt:n verran tilaa. Siirrytään painamalla "next" eteenpäin.

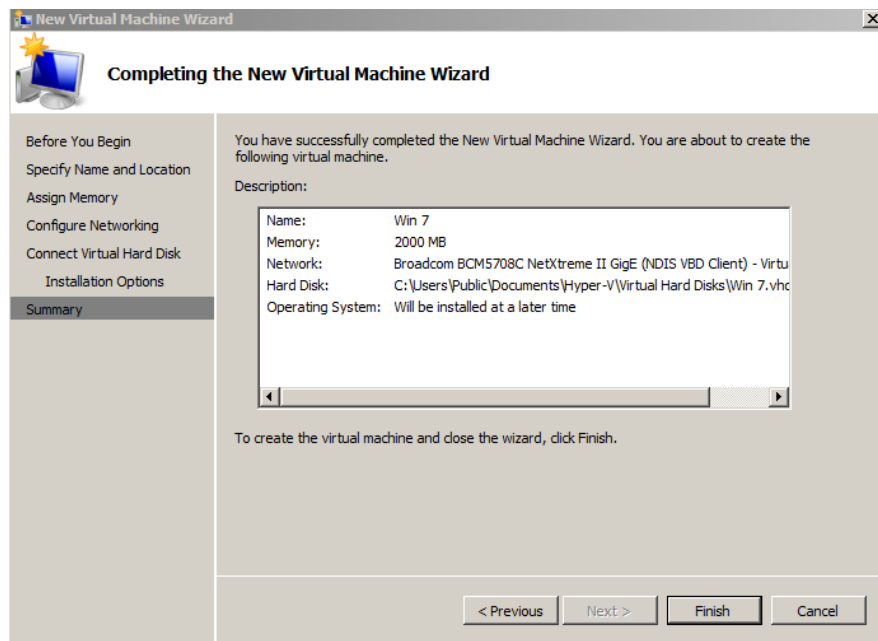


1.6 Määritellään miten käyttöjärjestelmän asennus tapahtuu, asensimme käyttöjärjestelmän myöhemmin.

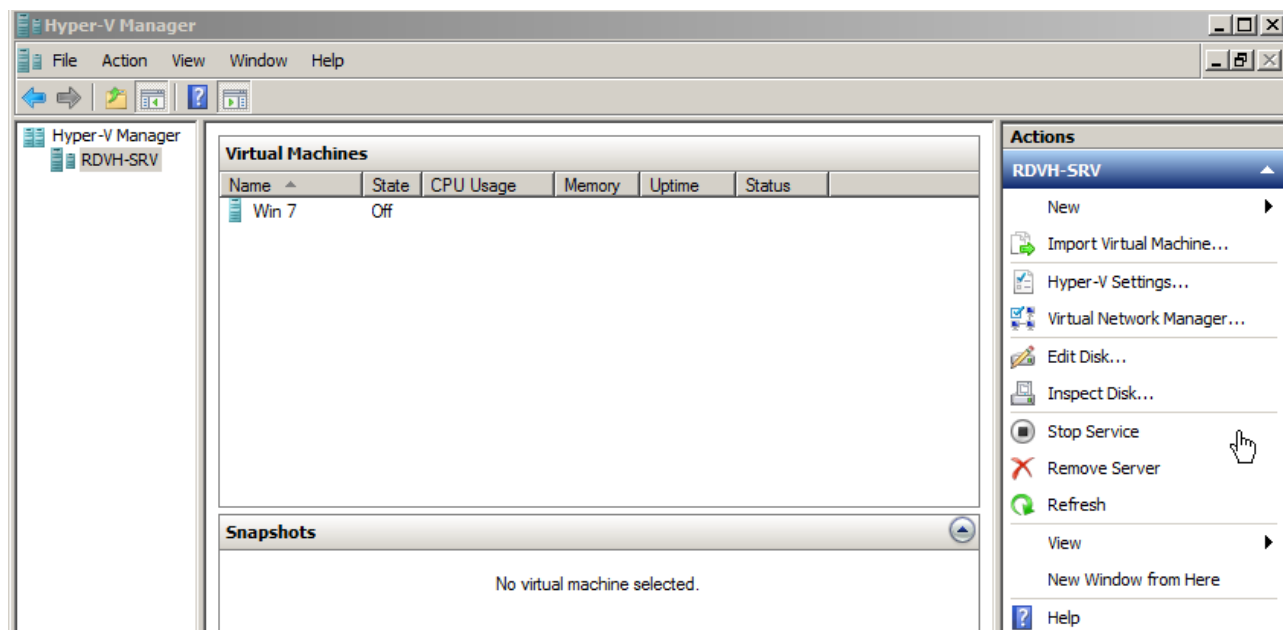
Asennus vaihtoehdot:

- Asenna käyttöjärjestelmä myöhemmin
- Asennusmedialta CD/DVD-rom tai image-tiedostosta (.iso)
- Virtuaalinen floppy disk (.vfd)
- Asennus verkkopalvelimelta

Siirrytään painamalla "next" eteenpäin.



1.7 Lopuksi asennusohjelma näyttää yhteenvedon valinnoista. Viimeistellään asennus painamalla ”finish”.



1.8 Hyper-V Manageriin ilmestyy juuri luotu virtuaalikone.

2. INFRASTRUKTUURIN ASENNUS JA MÄÄRITTELY

2.1. DOMAIN CONTROLLER ASENNUS

Palvelimen asennus:
Server 2008r2 64bit Enterprise

Huomioita asennuksessa:
- käyttäjän salasana on muutettava ennen ensimmäistä kirjautumista

Luodaan uusi domain controller:

1. Koneelle määritetään kiinteä ip 10.0.0.1
2. Aliverkon peite 255.255.255.0
3. Dns viittaamaan palvelimeen itseensä 10.0.0.1
4. Suoritetaan run toiminnolla komento dcpromo.exe
5. Määritetään ja nimetään uusi metsä (forest) "testi.local"
6. Määritetään metsän uusi functional level ja valitaan Server2008r2
7. Luodaan uusi DNS-palvelin
8. Hyväksytään oletusasetukset järjestelmän tietokannalle, lokitiedostoille ja SYSVOL-kansiolle
9. Määritetään Directory services restory mode -salasana "Password1"
10. Hyväksytään yhteenveto määrittämisistä
11. Käynnistetään kone uudestaan koneen määritettyä toimialueen asetukset
12. Lisätään aktiivihakemistoon halutut käyttäjät "Visitor1" ja "Visitor2". Järjestelmän ylläpitoa varten teimme käyttäjän "Admin" domain admin -oikeuksin
13. (kohdat 13-15 ovat valinnaisia)
14. Asennetaan server backup features
15. Ajetaan Backup once ja varmistetaan koko palvelin (Full Server)
16. Valitaan kohde mihin halutaan sijoittaa varmuuskopio, tässä tapauksessa paikalliselle kovalevylle

Uusien koneiden liittäminen aikaisemmin luotuun domainiin.

1. Avataan Computer, properties
2. Change settings
3. Vaihdetaan workgroup domainiksi
4. kirjoitetaan domainin nimi "testi"
5. Vahvistetaan toimenpide "domain admin" -tunnuksilla

2.2. REMOTE DESKTOP VIRTUALIZATION HOST SERVER (RDVH-SERVER) ASENNUS

1. Windows Server 2008 R2 asennus fyysiseksi palvelimeksi
2. Koneen nimeksi RDVH-SRV
3. Verkoasetukset
4. IP 10.0.0.4
5. DNS 10.0.0.1
6. Aliverkon peite 255.255.255.0
7. Yhdyskäytävä 10.0.0.1
8. Koneen liittäminen domainiin
9. RD Virtualization roolin asentaminen (HYPER-V sisältyy tähän automaattisesti)
10. Rooli asennetaan Add Roles -toiminnolla, Server Managerin kautta

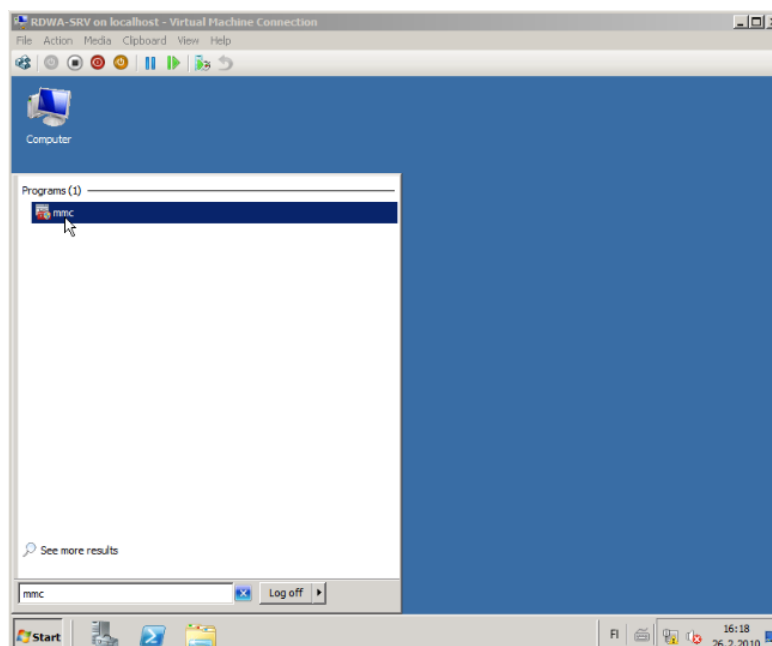
2.3. REMOTE DESKTOP SESSION HOST SERVER (RDSH-SERVER) ASENNUS

1. Windows Server 2008 R2 asennus virtuaalipalvelimeksi RDVH-palvelimelle
2. Koneen nimeksi RDSH-SRV
3. Verkoasetukset
4. IP 10.0.0.2

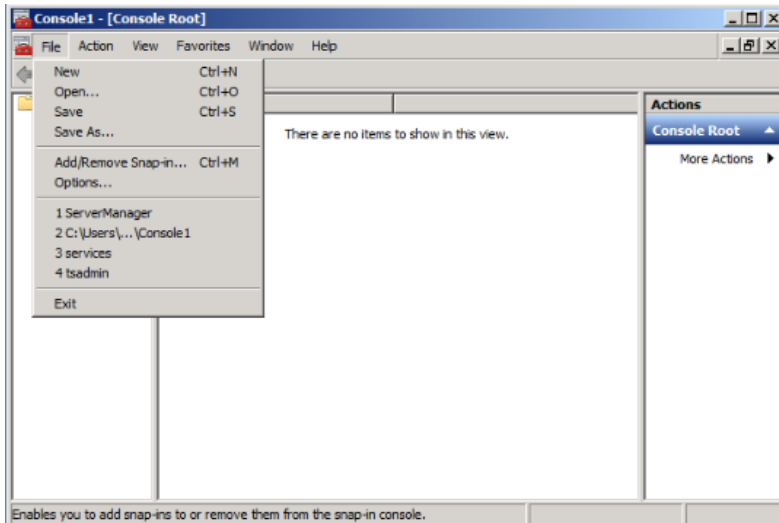
5. DNS 10.0.0.1
6. Aliverkon peite 255.255.255.0
7. Yhdyskäytävä 10.0.0.1
8. Koneen liittäminen domainiin
9. RD Session Host roolin asentaminen
10. Rooli asennetaan Add Roles -toiminnolla, Server Managerin kautta
11. Huom!
12. Käytettäessä Windows XP:tä päätelaitteena, ei tule vaatia verkkotason tunnistusta (NLA)
13. Kohdassa Specify Licensing Mode valitaan kohta Configure later, koska testiympäristössämme emme halua määrittää lisensointipalvelinta (kokeilu-aika 120 päivää). Tuotantoympäristössä lisensointipalvelin tulee ottaa käyttöön.
14. Lisenssipalvelimen määrittämisen jälkeen valitaan halutut käyttäjäryhmät, joille sallitaan pääsy tälle palvelimelle. Testiympäristössä lisäsimme manuaalisesti Visitor1, Visitor2 ja Admin käyttäjätilit palvelimen paikalliseen Remote Desktop User -ryhmään.
15. käyttäjän lisääminen paikalliseen Remote Desktop User -ryhmään
Administrative tools -> Computer Management -> Local User and Groups -> Remote Desktop Users -> Add to group -> Visitor1/Visitor2/Admin -> Add -> OK

2.4.REMOTE DESKTOP REMOTE DESKTOP WEB ACCESS SERVER (RDWA-SERVER) ASENNUS

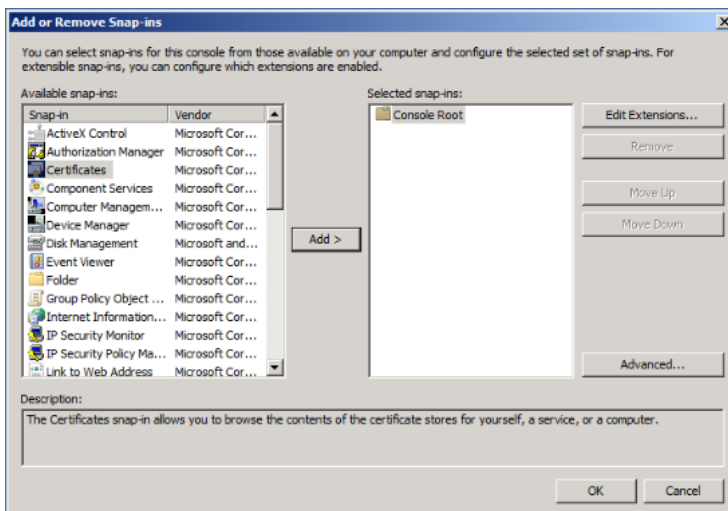
1. Windows Server 2008 R2 asennus virtuaalipalvelimeksi RDWH-palvelimelle
2. Koneen nimeksi RDWA-SRV
3. Verkoasetukset
4. IP 10.0.0.6
5. DNS 10.0.0.1
6. Aliverkon peite 255.255.255.0
7. Yhdyskäytävä 10.0.0.1
8. Koneen liittäminen domainiin
9. RD Web Access roolin asentaminen
10. Rooli asennetaan Add Roles-toiminnolla, Server Managerin kautta, Web Server (IIS) asentuu mukana
11. Itseallekirjoitetun SSL-sertifikaatin luominen



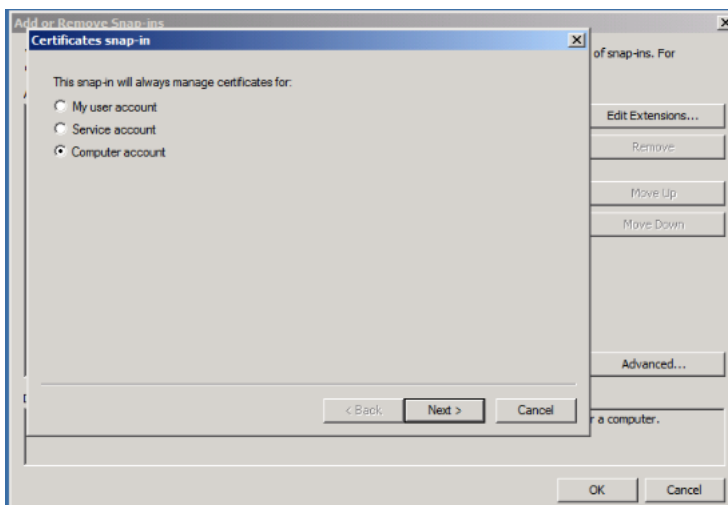
1. Avataan MMC suorita kohdasta



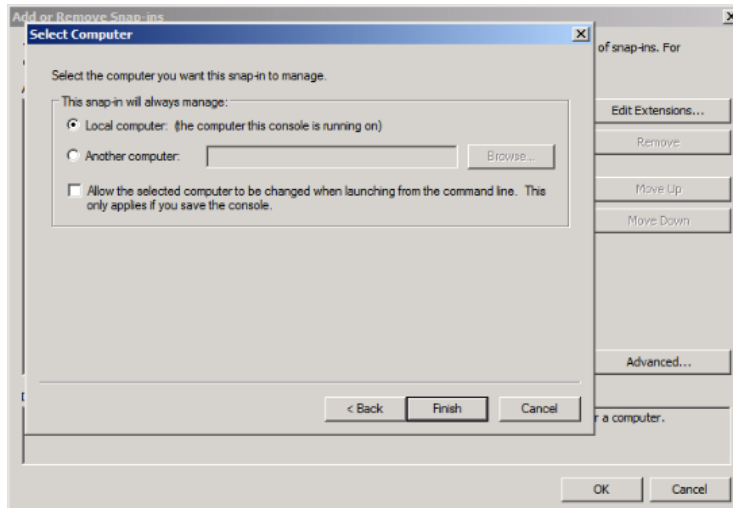
2. Avataan Add/Remove Snap-in



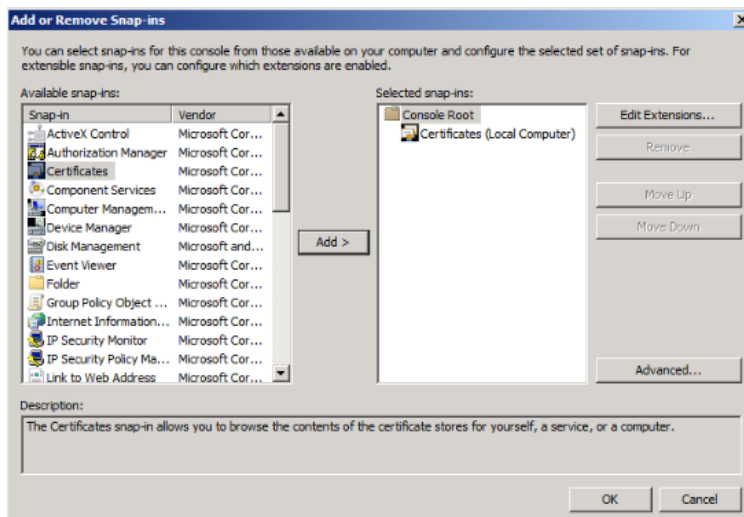
3. Valitaan saatavilla olevista Snap-In:stä "Certificates" ja painetaan "Add"



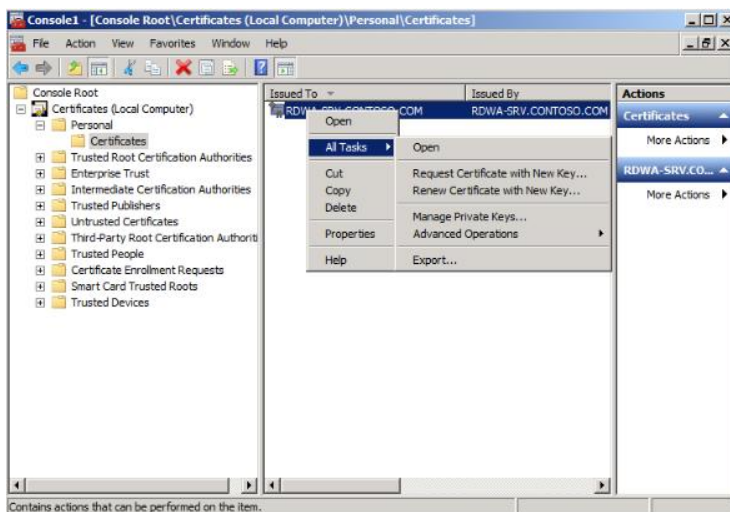
4. Certificates snap-in ikkuna aukeaa, valitaan kohta "Computer account"



5. Valitaan Local computer ja painetaan "Finish"



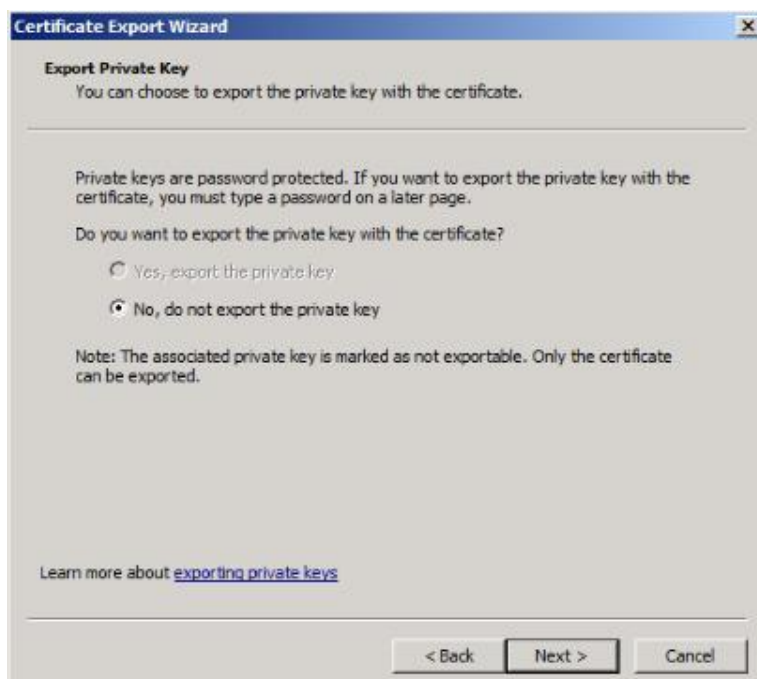
6. Olemme nyt valinneet sertifiikaatin ja voimme painaa "OK"



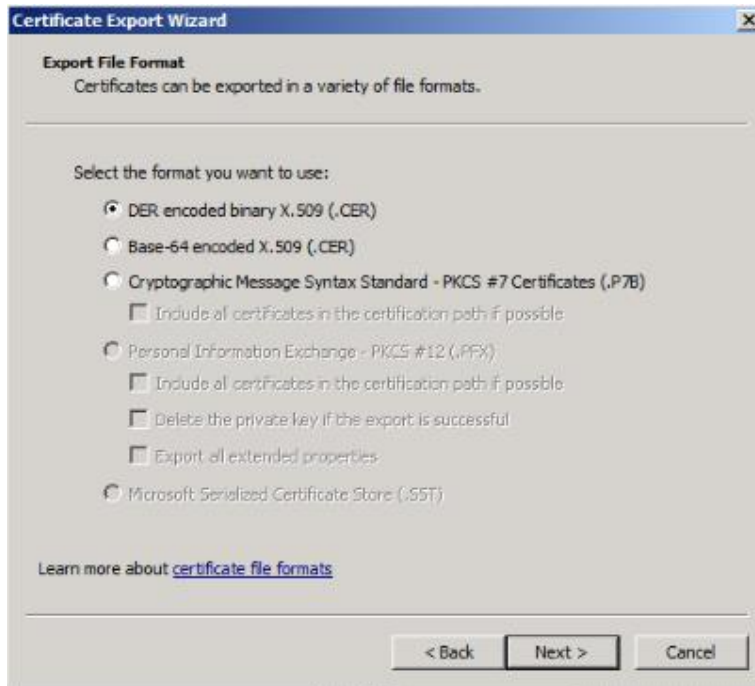
7. Navigoi seuraavasti: Certificate\Personal\Certificates
Valitse hiiren oikealla painikkeella lisäämäsi serifiikaatti ja mene All Tasks -> Export



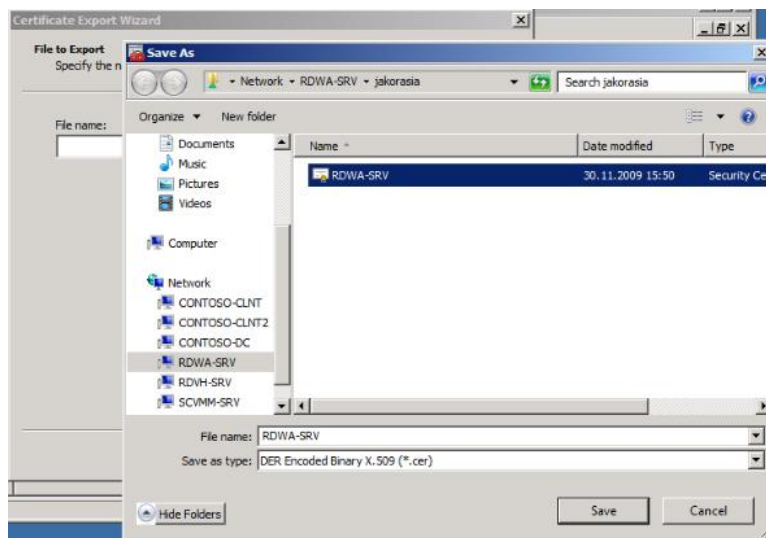
8. Valitse "Next"



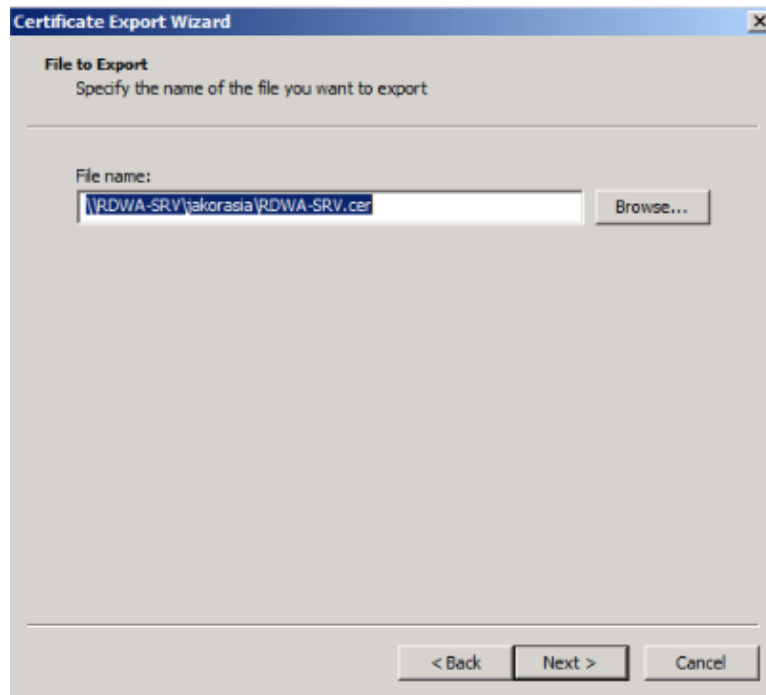
9. Varmista että "No, -" vaihtoehto on valittuna.



10. Varmista että ylin vaihtoehto ”DER encoded binary X.509(.CER)” on valittuna.



11. File to Export sivulta selaa ja tallenna nimellä RDWA-SRV.



12. Valitse nyt "Next"



13. Viimeistelläkseksi Sertifikaatin luonnin valitse "Finish".



14. Lopuksi tulee vahvistus että luonti on onnistunut, valitse "OK"
15. Sulje Certificates Snap-in.

Tämä sertifikaatti tulee kopioida kaikkiin virtuaalisiin ja fyysisiin client-koneisiin.

2.5. REMOTE DESKTOP CONNECTION BROKER SERVER (RDCB-SERVER) ASENNUS

1. Windows Server 2008 R2 asennus fyysiseksi palvelimeksi RDCB-palvelimelle
Koneen nimeksi annettiin RDCB-SRV
2. Verkkoasetukset
IP 10.0.0.5
DNS 10.0.0.1
Aliverkon peite 255.255.255.0
Yhdyskäytävä 10.0.0.1
Koneen liittäminen domainiin
3. RD Connection Broker roolin asentaminen
Rooli asennetaan Add Roles-toiminnolla, Server Managerin kautta
Remote desktop services -> RD Connection Broker

2.6. REMOTE DESKTOP CLIENT (CLNT1) ASENNUS

1. Windows 7 asennus fyysiseksi työasemaksi
Koneen nimeksi annettiin CLNT1
2. Verkkoasetukset
IP 10.0.0.3
DNS 10.0.0.1
Aliverkon peite 255.255.255.0
Yhdyskäytävä 10.0.0.1
3. Koneen liittäminen domainiin

2.7. REMOTE DESKTOP CLIENT (CLNT2)

1. WinXP pro asennus fyysiseksi työasemaksi
Koneen nimeksi annettiin CLNT2
Asennetaan Remote Desktop Connection 7.0 client (vaatii Windows XP Service Pack 3 -päivityspaketin)
2. Verkoasetukset
IP 10.0.0.15
DNS 10.0.0.1
Aliverkon peite 255.255.255.0
Yhdyskäytävä 10.0.0.1
3. Koneen liittäminen domainiin

2.8. VIRTUAALIKONEIDEN LUOMINEN JA MÄÄRITTÄMINEN

1. Asennetaan käyttöjärjestelmä
Määritetään verkoasetukset
Liitetään virtuaalikoneet domainiin
2. Lisätään Remote Desktop Web Access:n SSL -sertifikaatti virtuaalikoneisiin

1. Virtuaalikoneen asennus

1. Kirjautu RDVH-serverille domain admin -tunnuksin
2. Laita Windows 7-dvd dvd-asemaan
3. Avaa Hyper-V Manager
4. Paina hiiren oikealla painikkeella "RDVH-SRV" navigoi New -> Virtual Machine
5. Before You Begin sivulla valitse "Next"
6. Nimeä virtuaalikone (Esim. Vdp1-clnt)
7. Assign Memory sivulla määritetään muistin määrä (esim. 2Gt)
8. Configure networking sivulla, Connection kohdasta valitse virtuaalinen verkko joka sisältää muut domainin koneet
9. Connect Virtual Hard Disk sivulla määrität kovalevyn koon (esim. 30Gt)
10. Installation Options sivulla valitse "Install an operation system from a boot CD/DVD-ROM drive"
11. Valitse "Finish" Completing the New Virtual Machine Wizard sivulta
12. Virtual Machines valitse kohdasta hiiren oikealla painikkeella VDP1-CLNT ja valitse Connect
13. Paina Action ja seuraavaksi Start.
14. Viimeistele käyttöjärjestelmän asennus, määritä verkoasetukset ja liitä domainiin.
15. Toista samat kohdat kohteille VDP2-CLNT ja VDP3-CLNT

VDP1-CLNT Win7prof IP 10.0.0.7 DNS 10.0.0.1 Aliverkon peite 255.255.255.0 Yhdyskäytävä 10.0.0.1	VDP2-CLNT Win7prof IP 10.0.0.8 DNS 10.0.0.1 Aliverkon peite 255.255.255.0 Yhdyskäytävä 10.0.0.1	VDP3-CLNT Win7ent IP 10.0.0.9 DNS 10.0.0.1 Aliverkon peite 255.255.255.0 Yhdyskäytävä 10.0.0.1
--	--	---

2. Tuodaan Remote Desktop Web Access:n SSL sertifikaatti virtuaalikoneisiin

1. Kirjautu VDP1-CLNT domain admin tunnuksin
2. Avataan Microsoft Management Console
3. File-valikosta valitaan Add/Remove Snap-in
4. Lisätään Certificates, Available snap-ins kohdasta lisää toiminnolla
5. Certificates snap-in valintaikkunasta: Computer account

6. Select computer valintaikkunasta: Local computer: (the computer this console is running on)
7. Valitse "OK" Add or Remove snap-in valintaikkunassa
8. Laajenna Certificates (Local Computer) ja valitse Trusted Root Certification Authorities
9. Paina hiiren oikealla painikkeella Trusted Root Certification Authorities kansiota.
10. Navigoi All Tasks -> Import
11. Valitse "Next" welcome to the Certification Authorities sivulla
12. File to Import sivulla valitse "Browse" ja selaa minne kopioit SSL sertifikaatin RDWA-SRV koneelle. Valitse "Open" ja seuraavaksi "Next".
13. Certificate Store sivulla hyväksy oletusvaihtoehto (Place all certificates in the ...)
14. Paina "Finish" Completing the Certificate Import Wizard sivulla.
15. Mikäli sertifikaatin lisäys onnistui, niin tulee ilmoitus asiasta.
16. Kirjautu ulos VDP1-CLNT:lta ja suorita sama myös VDP2-CLNT ja VDP3-CLNT.

2.9. VIRTUAALIKONEIDEN MÄÄRITTÄMINEN REMOTE DESKTOP-TOIMINNOILLE

1. Mahdollistetaan Remote Desktop
2. Lisätään virtuaalikoneiden Remote Desktop User -ryhmään
3. Sallitaan Remote RPC Remote desktop palveluille
4. Mahdollistetaan poikkeukset palomuriin salliakseen Remote Services Management
5. Lisätään suostumus RDP protokollalle.
6. Mahdollistetaan virtuaalikoneiden palauttaminen käyttöä edeltävään tilaan
 1. Mahdollistetaan Remote Desktop
 1. Kirjaututaan virtuaalikoneille koneelle domain admin tunnuksin
 2. Avataan Remote Settings ja valitaan "Allow connections only from computer using Remote Desktop with Network Level Authentication (more secure)".
 3. Toistetaan samat tehtävät myös muille virtuaalikoneille (VDP2 ja VDP3)
 2. Lisätään virtuaalikoneiden käyttäjät Remote Desktop Users ryhmään
 1. Kirjaututaan virtualikoneille paikalli sadmin -tunnuksin
 2. Avataan Local Users and Groups välilehti Computer Managementista ja lisätään Remote Desktop Users -ryhmään halutut käyttäjät/ryhmät (Käytimme käyttäjänimiä Visitor1 ja Visitor2)
 3. Kirjaututaan ulos ja toistetaan samat tehtävät myös muille virtuaalikoneille
 3. Sallitaan Remote RPC Remote desktop palveluille
 1. Kirjaututaan virtualikoneille paikallis admin -tunnuksin
 2. Avataan Rekisterieditori (esimerkiksi komentokehotteeseen komennolla regedit.exe)
 3. Navigoi itsesi seuraavasti:
 4. HKEY_LOCAL_MACHINE\SYSTEMS\CurrentControlset\Control\TerminalServer
 5. Avaa AllowRemoteRPC kohta ja sallimalla tämä, vaihtamalla nollan (0) tilalle ykkönen (1).
 6. Kirjaututaan ulos ja toistetaan samat tehtävät myös muille virtuaalikoneille
 4. Lisätään palomuurille poikkeukset Remote Services palveluille.

Ympäristössämme koneilla ei ollut pääsy ulkoverkkoon, joten kaikista koneista palomuurit olivat pois käytöstä. Toteutusympäristössä palomuurit on syytä pitää käytössä niin; Kirjaututaan virtuaalikoneille paikallis admin -tunnuksin. Muutetaan Windowsin Palomuurin asetuksia, jotta Remote Service Managementin pääsee Windowsin Palomuurin lävitse.

5. Lisätään suostumus RDP protokollalle
 1. Kirjaututaan virtuaalikoneille paikallis admin -tunnuksin
 2. Avataan komentokehote suorittamalla se järjestelmänvalvojana (saa valittua painamalla hiiren oikeaa näppäintä komentokehotteen päällä.)
 3. Kirjoitetaan komentokehoteeseen seuraavat käskyt:
 - wmic /node:localhost RDPERMISSIONS where TerminalName="RDP-Tcp" CALL AddAccount "*domainisi nimi*\rdvh-srv\$",1
 - wmic /node:localhost RDACCOUNT where "(TerminalName='RDP-Tcp' or TerminalName='Console') and AccountName='*domainisi nimi*\rdvh-srv\$'" CALL ModifyPermissions 0,1
 - wmic /node:localhost RDACCOUNT where "(TerminalName='RDP-Tcp' or TerminalName='Console') and AccountName='*domainisi nimi*\rdvh-srv\$'" CALL ModifyPermissions 2,1
 - wmic /node:localhost RDACCOUNT where "(TerminalName='RDP-Tcp' or TerminalName='Console') and AccountName='*domainisi nimi*\rdvh-srv\$'" CALL ModifyPermissions 9,1
 - Net stop termservice
 - Net start termservice
 4. Kirjaututaan ulos ja toistetaan samat tehtävät myös muille virtuaalikoneille
6. Mahdollistetaan virtuaalikoneiden palauttaminen käyttöä edeltävään tilaan.
 1. Kirjaututaan RDVH-palvelimelle domain admin -tunnuksilla
 2. Avataan Hyper-V Manager
 3. Painetaan hiiren oikealla painikkeella VDP1-CLNT ja sitten painetaan Snapshot
 4. Nimetään Snapshot uudelleen: RDP_Rollback
 5. Toistetaan sama myös muille virtuaalikoneille.

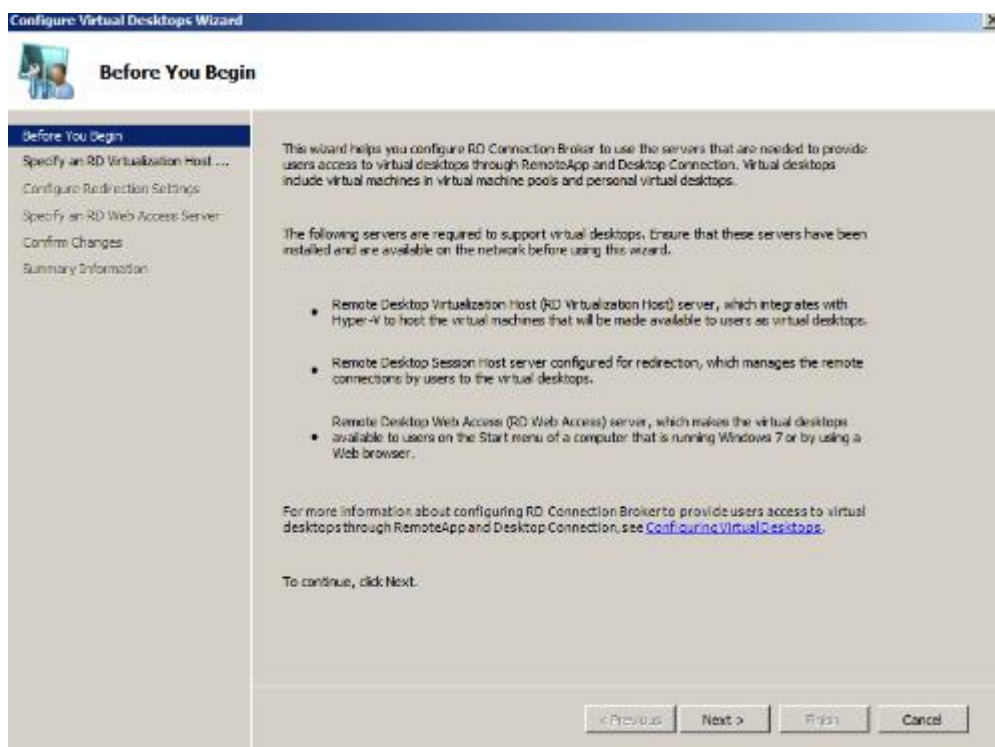
2.10. VIRTUAALISTEN POOLIEN KONFIGUROINTI

1. Lisätään RDWA-palvelin TS Web Access Computers ryhmään RDCB-palvelimelle
 2. Määritellään Remote Desktop Web Accessin lähde
 3. Määritetään virtuaalikoneiden "POOLI" Remote Desktop Connetion Brokerille (RDCB-palvelimelle)
 4. Lisätään virtuaalikoneet Pooliin
-
1. Lisätään RDWA-serveri TS Web Access Computers ryhmään RDCB-palvelimelle
 1. kirjautu RDCB-palvelimelle domain admin -tunnuksin
 2. Avataan Computer Management ja Local Users and Groups ja valitaan Groups. Klikataan hiiren oikealla painikkeella Terminal Web Access Computers ja valitaan kohta "Add to Group" -> Add -> Object Types -> Computers ja lisätään sinne "RDWA-SRV"
 3. Valitse "OK" ja kirjautu ulos.
 2. Määritellään Remote Desktop Web Accessin lähde
 1. Kirjautu RDWA-palvelimelle paikallis admin -tunnuksin
 2. Navigoi seuraavasti:

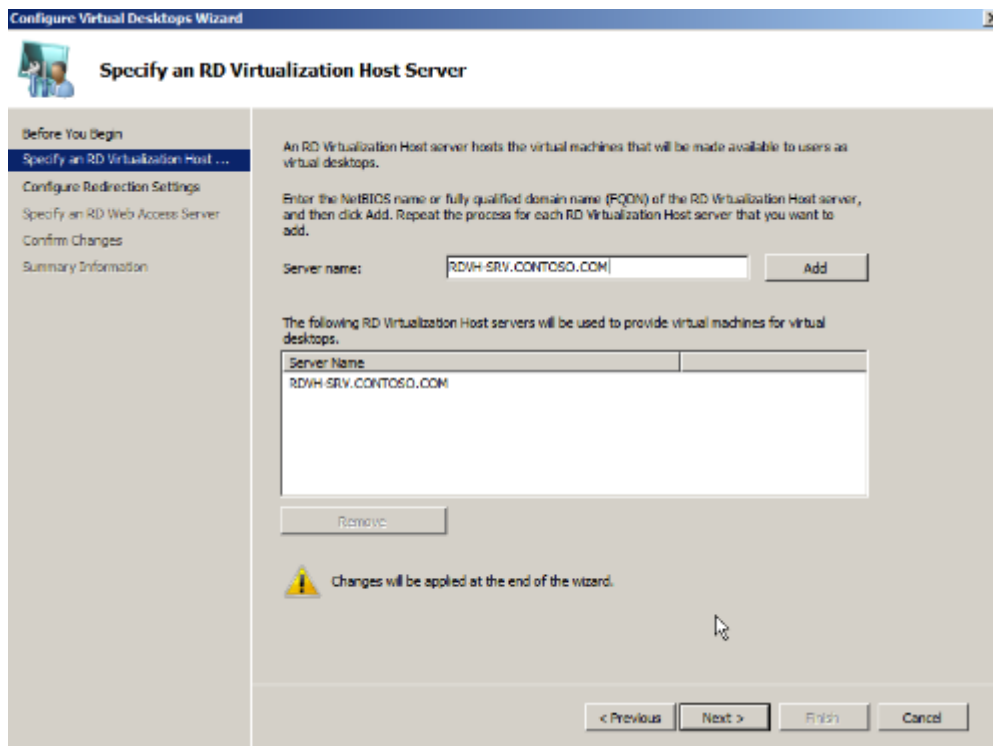
Start->Administrative Tools->Remote Desktop Services->Remote Desktop Web Access Configuration

3. Valitse "Continue to this website (not recommended)"
 4. Kirjoita Domain/user name kohtaan *domain nimesi*\administrator ja määrittele-
mäsi salasana, sille varattuun kohtaan
 5. Configuration sivulla valitse "An RD Connection Broker server".
 6. Source name kohtaan laita "RDCB-SRV" ja valitse "OK".
 7. Kirjauus ulos
3. Määritetään virtuaalikoneiden "POOLI" Remote Desktop Connection Brokerille (RDCB-
palvelimelle)

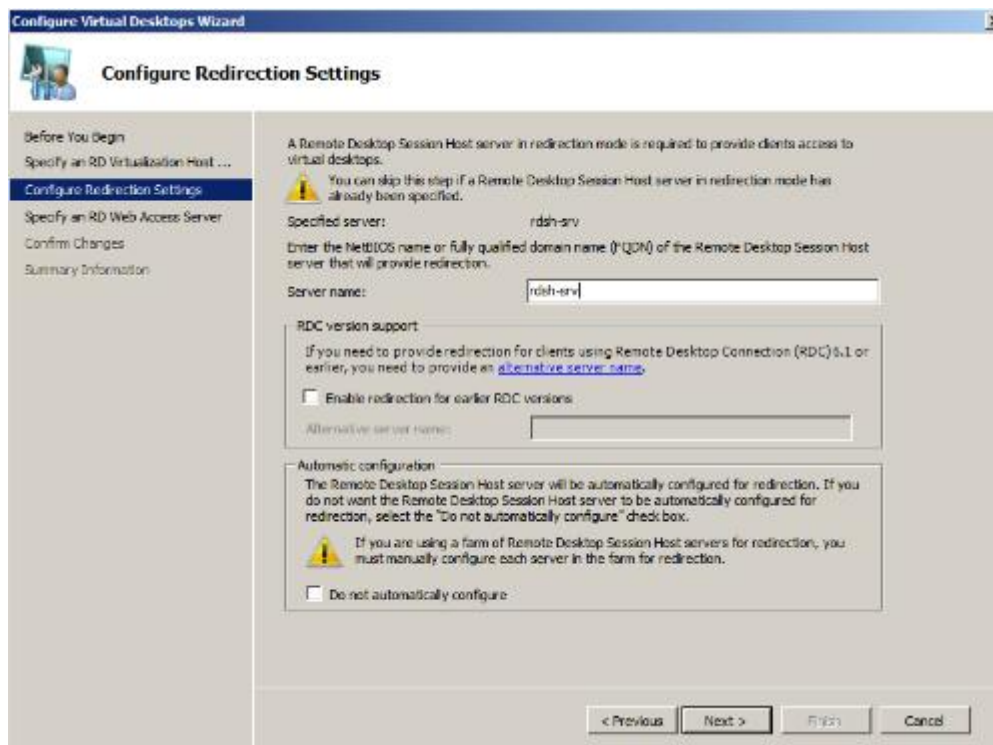
Valitaan Start -> Administrative Tools ->Remote Desktop Services -> Remote
Desktop Connection Manager -> Configure Virtual Desktops



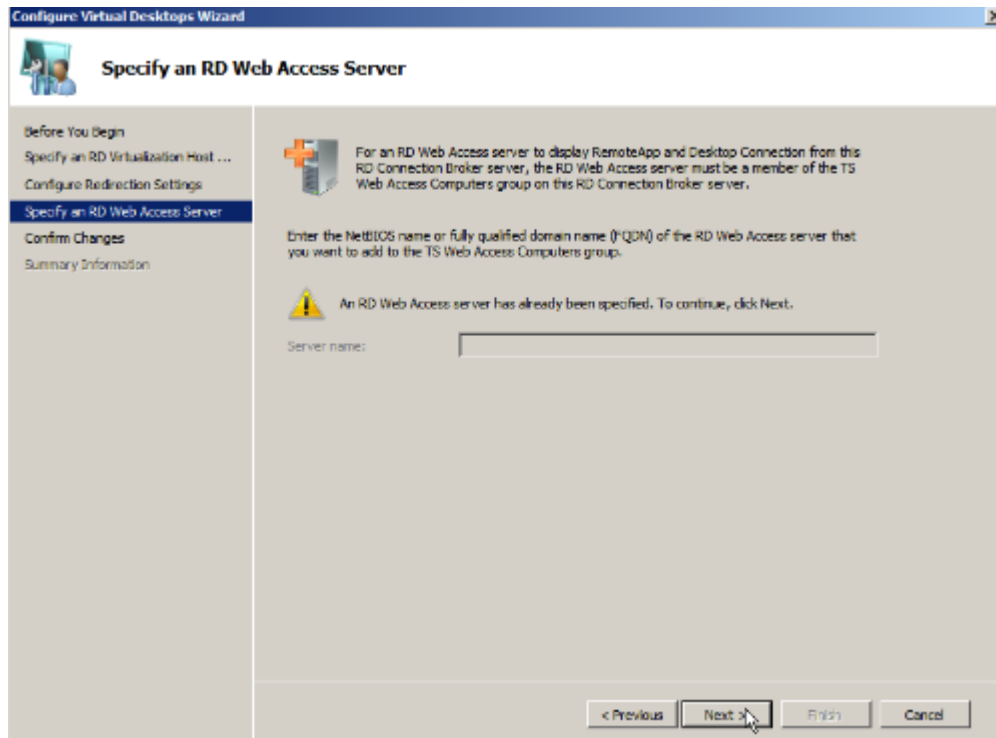
1. Valitse "Next"



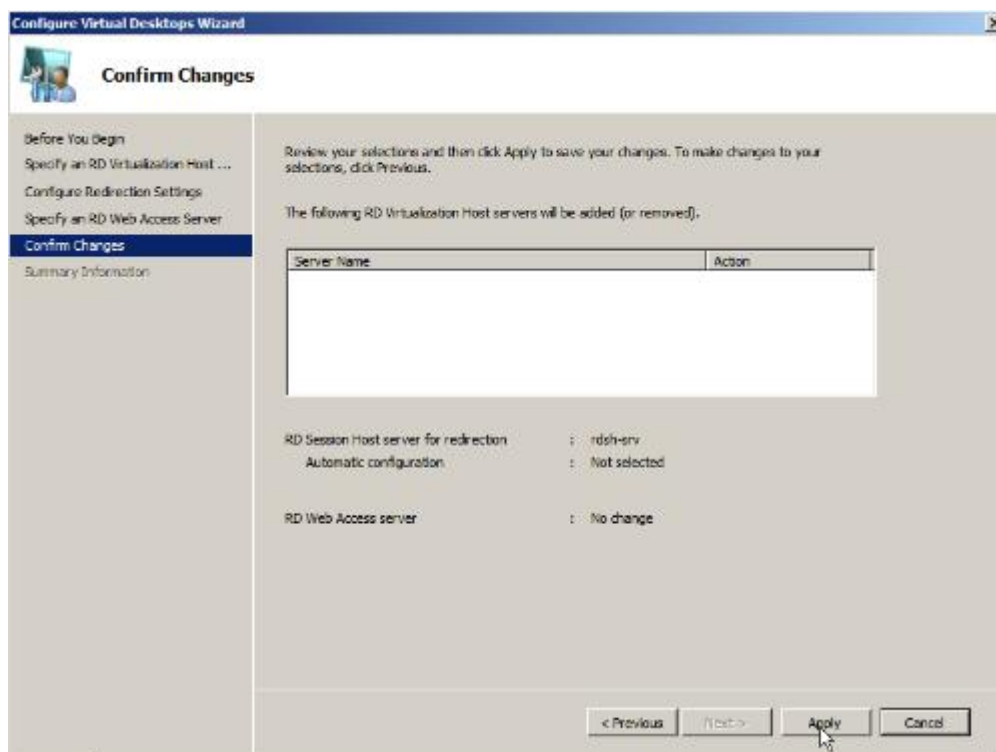
2. Lisää palvelin jolle on asennettua virtuaaliset koneet. Kirjoita palvelimen nimi FQDN muodossa.



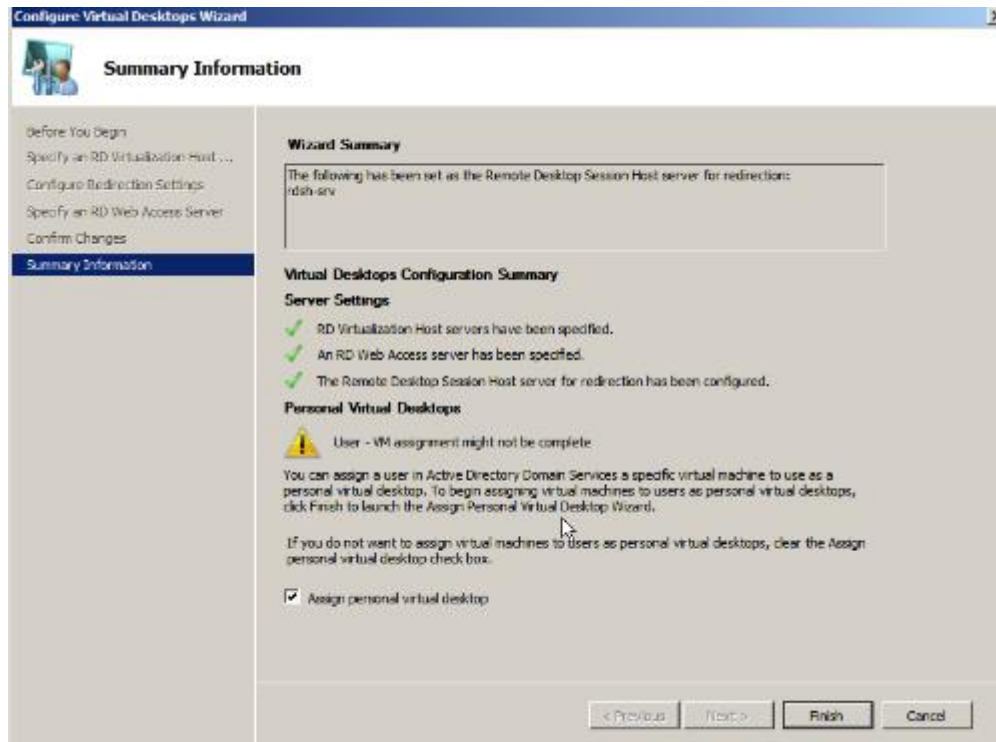
3. Kirjoita Session Host palvelimen nimi FQDN muodossa: RDSH-SRV



4. Valitse "Next"



5. Vahvista muutokset valitsemalla "Apply".



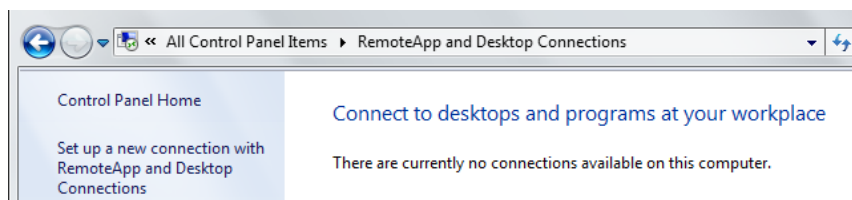
6. Summary Information sivulla, ota täppä pois kohdasta "Assign personal virtual desktop", sillä emme tehneet henkilökohtaisia työpöytiä. Lopuksi valitse "Finish".

4. Virtuaalikoneiden lisäys pooliin
 1. Kirjaututaan koneelle RDCB-SRV:lle domain admin tunnuksin
 2. Navigoi seuraavasti Start -> Administrative Tools ->Remote Desktop Services -> Remote Desktop Connection Manager
 3. Paina Action-painiketta ja valitse "Create Virtual Desktop Pool"
 4. Valitse haluamasi työpöydät Pooliin. Lopuksi anna poolille haluamasi nimi.

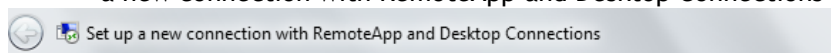
3. YMPÄRISTÖN TOIMIVUUDEN TESTAUS

Kirjaututaan paikalliselle Windows 7 työasemalle Visitor1-tunnuksin. Otetaan käyttöön RemoteApp & Desktop- toiminto, jonka avulla käyttäjät saavat yhteyden virtuaalisiin työpöytiinsä.

1. Avaa Ohjauspaneeli ja valitse RemoteApp and Desktop Connections



2. Uuden RemoteApp and Desktop yhteyden luomista varten, valitse vasemmalta "Set up a new connection with RemoteApp and Desktop Connections".



Connection URL:

3. Syötä kenttään Remote Desktopin Web Access-palvelimen RAD-feed -osoite ja paina next
4. Viimeistele asennus valitsemalla finish ja testaa työpöytään yhdistäminen käynnistävalikon RemoteApp and Desktop Connectionin alta löytyvältä Enterprise Remote Access-kuvakkeella.
5. Yhdistä käynnistävalikon kautta luotuun virtuaalikoneiden pooliin.

Huom. pooliin voidaan myös kirjautua Windows XP sp3 koneelta käyttämällä RD-Web Access liittymää. Kirjautuminen tapahtuu selaimen kautta, syöttämällä palvelimen osoite.

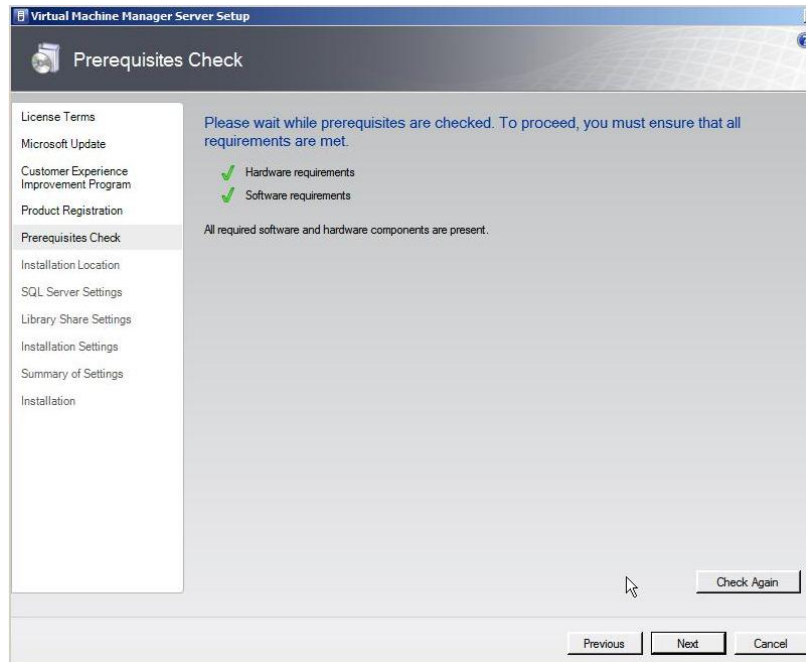
Liite 2 SCVMM 2008 R2

System Center Virtual Machine Manager 2008 R2

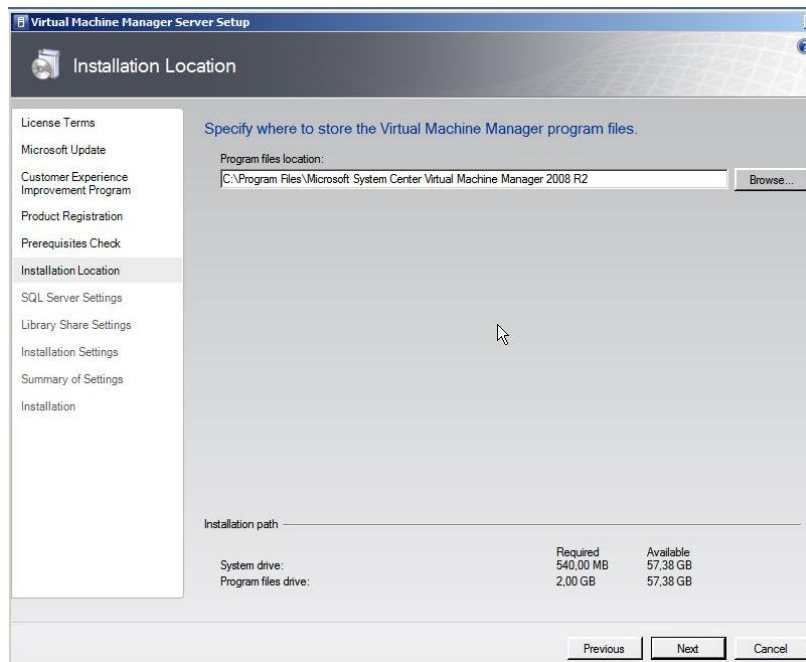
1. Asennetaan SCVMM-palvelin
2. Asennetaan VMM Administrator Console
3. Virtualization host



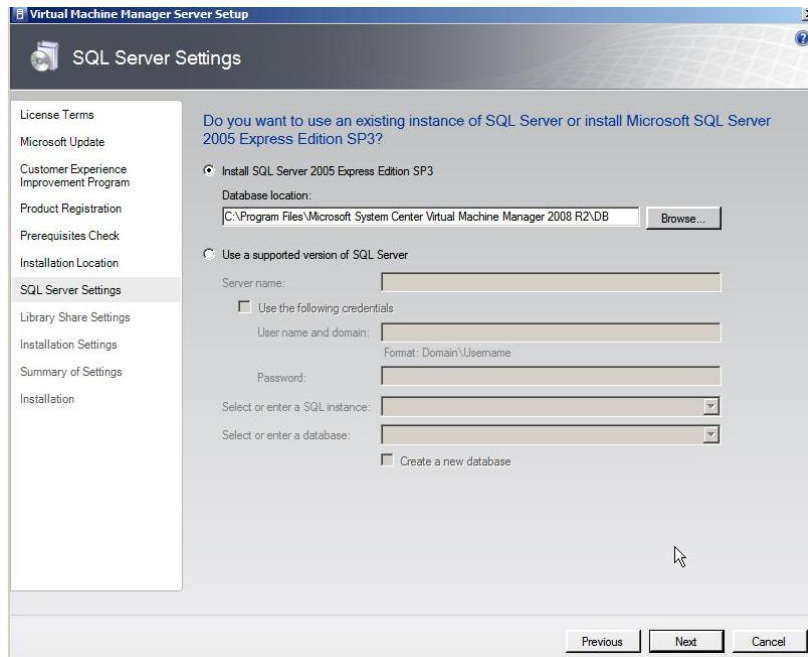
- 1.1 SCVMM asennus käynnistetään klikkaamalla kohtaa VMM Server. Asennuslevyltä löytyvät kattavat asennusohjeet ja järjestelmävaatimukset. Asennusmedialta voidaan suorittaa myös VMM Administrator Consolen, Self Service Portalin, Local Agent asennuksen ja määrittellä Virtual Machine Manager toimimaan Operations Managerin kanssa. Seuraavassa kohdassa pyydetään vahvistamaan ohjelmiston lisenssiehdot ja valitaan käytetäänkö Microsoft Update palvelua päivitysten tarkistamiseen.



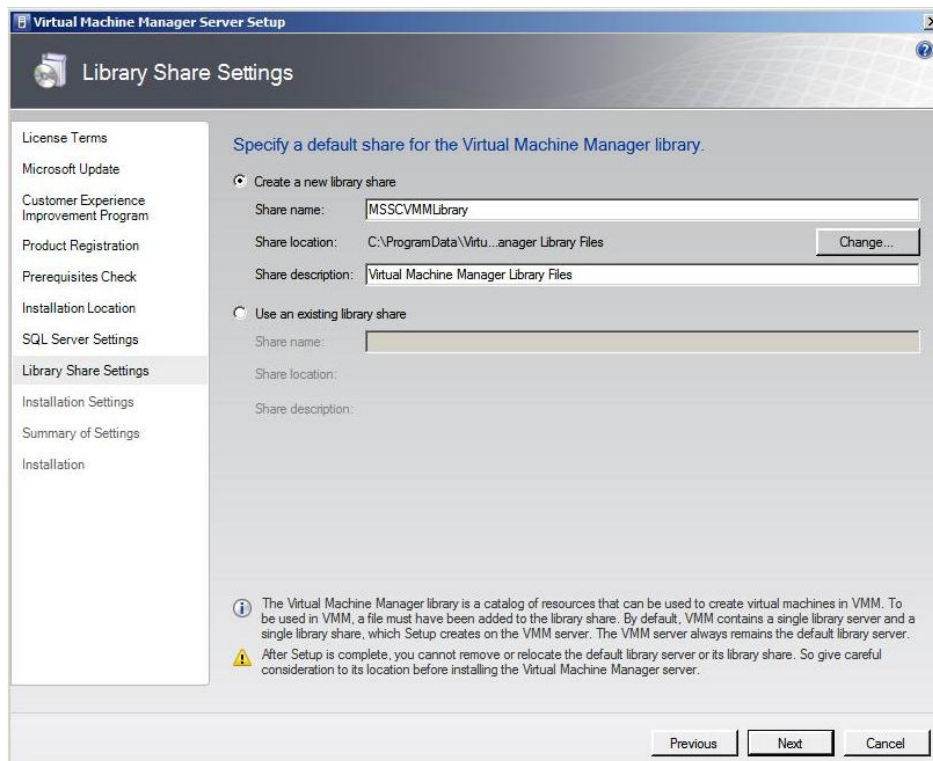
1.2 Asennusohjelma tarkistaa onko järjestelmälle asetetut minivaatimukset kunnossa.



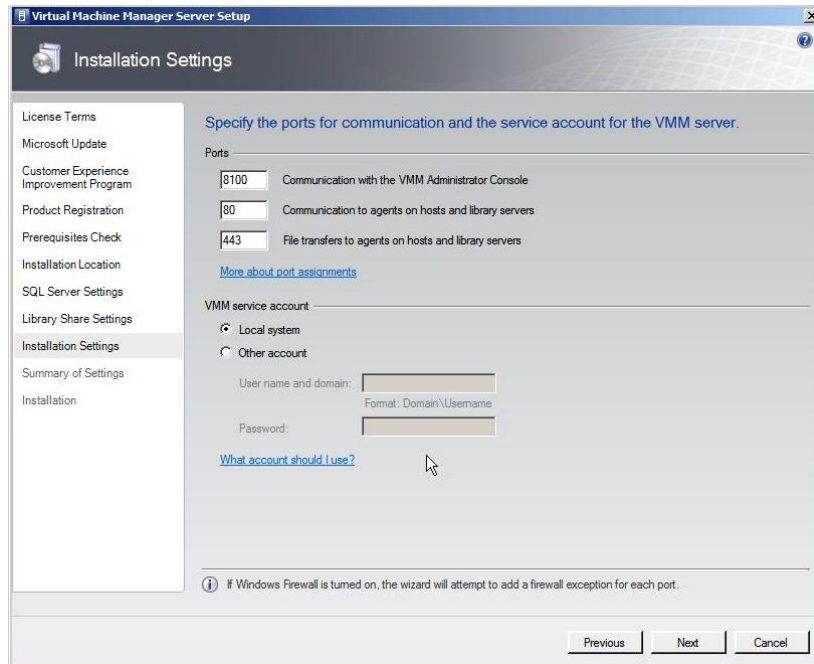
1.3 Installation Location kohdassa valitaan mihin Virtual Machine Managerin tiedostot sijoitetaan. Asennuskohteeksi valitsimme paikallisen koneen kovalevyn.



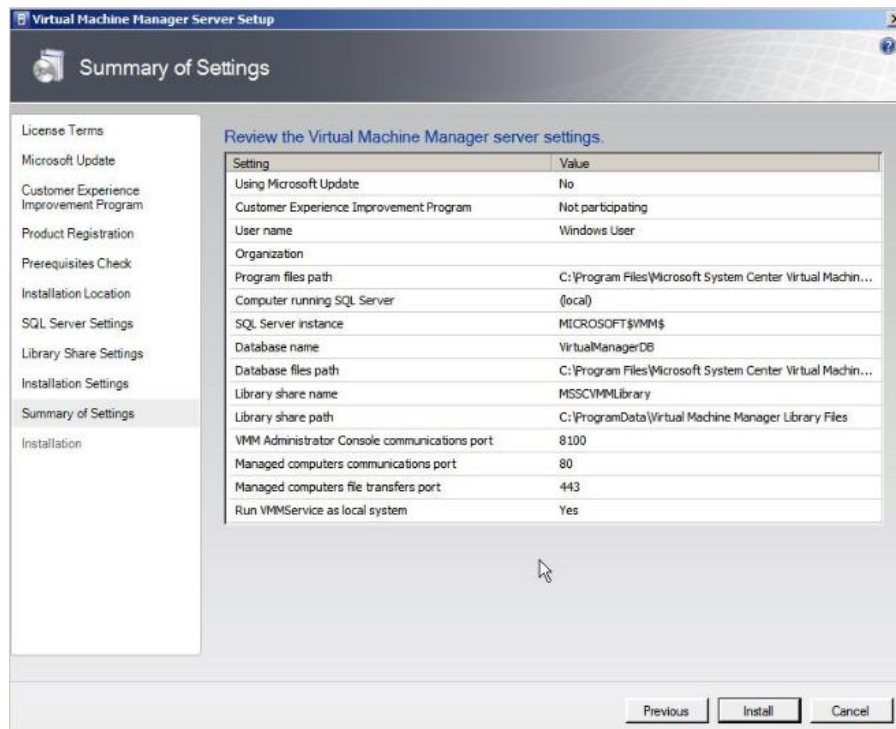
1.4 Valitaan käytetäänkö olemassa olevaa SQL-palvelinta vai asennetaanko Microsoft SQL Server 2005 Express Edition SP3. Käytimme testiympäristön kanssa asennuksen tarjoamaa MS SQL Server Express Editionia.



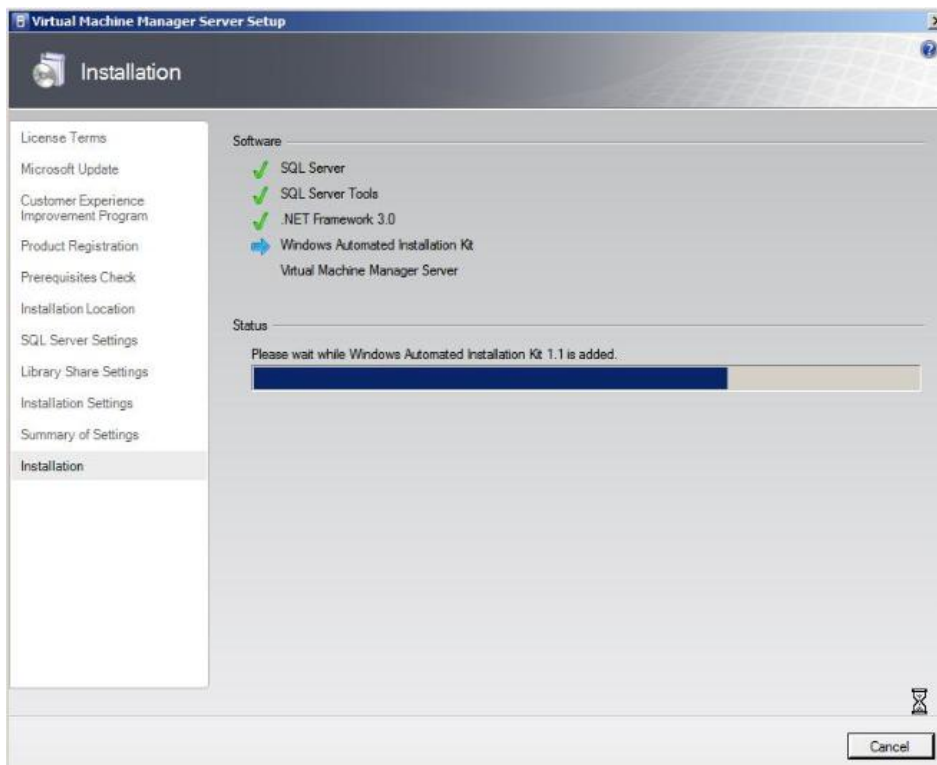
1.5 Library Share Settings kohdassa määritetään missä SCVMM:n käyttämä resurssikirjasto tulee sijaitsemaan. Testiympäristössä valitsimme isäntäkoneen paikallisen kovalevyn tiedostojen sijaintipaikaksi. Tuotantoympäristössä tämän osio kannattaa sijoittaa toiselle palvelimelle tai käyttää levyjärjestelmää (SAN) kirjastona.



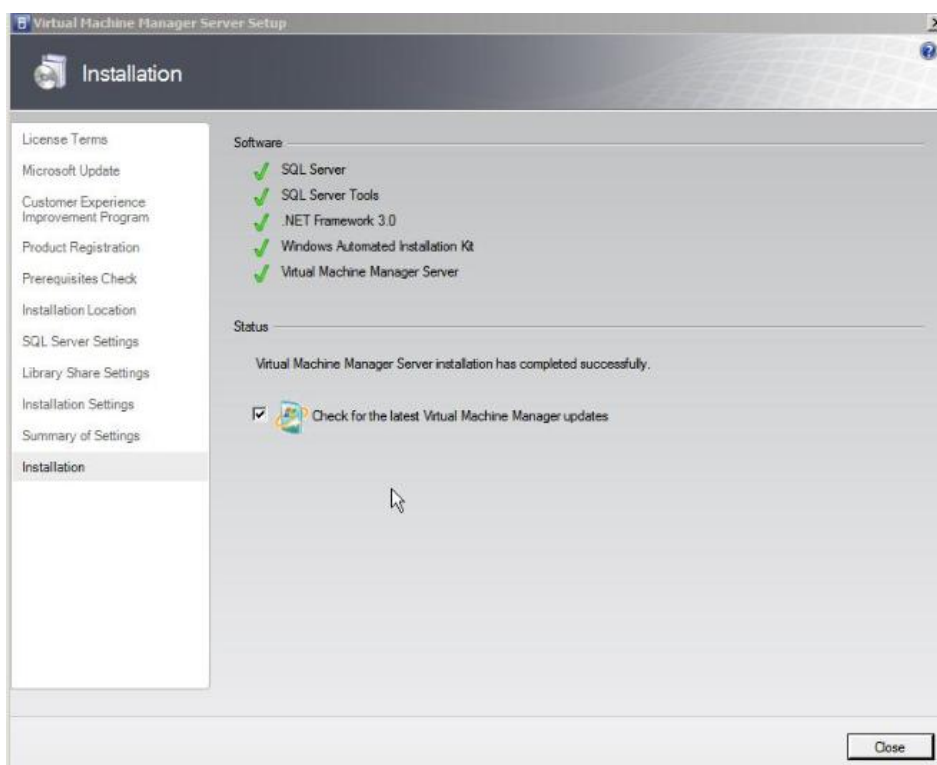
1.6 Installation Settings kohdassa määritellään mitä portteja SCVMM käyttää kommunikointiin kirjastopalvelimen ja agenttien välillä, sekä tiedonsiirtoon. Alemmassa kohdassa voidaan määritellä mitä tilii käytetään SCVMM hallintaan, valitsimme asetukseksi Domain administrator-tilin. Porttien osalta käytimme järjestelmän oletusasetuksia.



1.7 Ennen varsinaista asennusta ohjelma näyttää yhteenvedon määritellyistä asetuksista. Varsinainen asennus käynnistyy painamalla "Install".

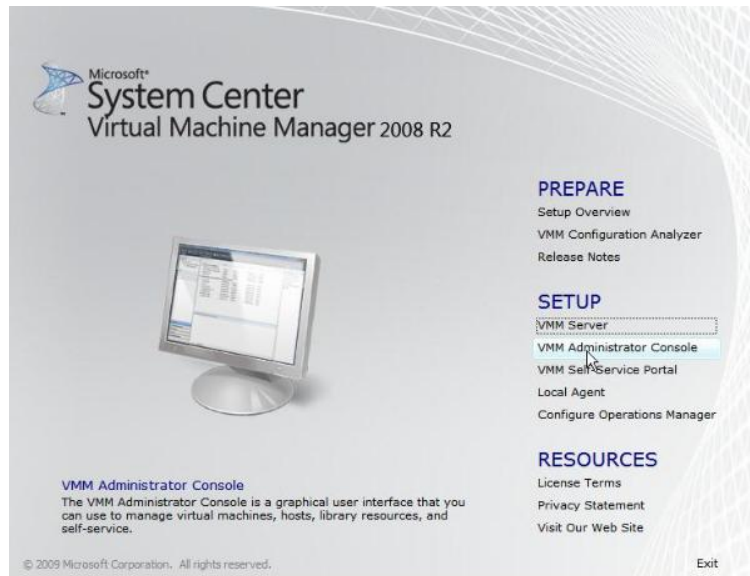


1.8 Asennusohjelma näyttää etenemisvaiheen ja ilmoittaa, mitkä komponentit on asennettu.

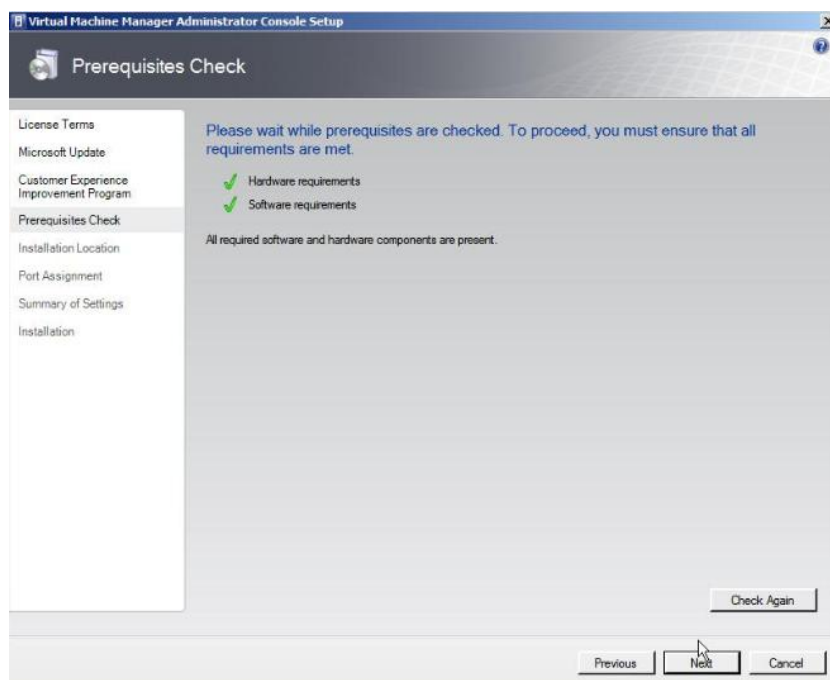


1.9 Asennuksen loppuksi nähdään kaikki asennetut komponentit, sekä voidaan pyytää järjestelmää tarkistamaan viimeisimmät päivitykset.

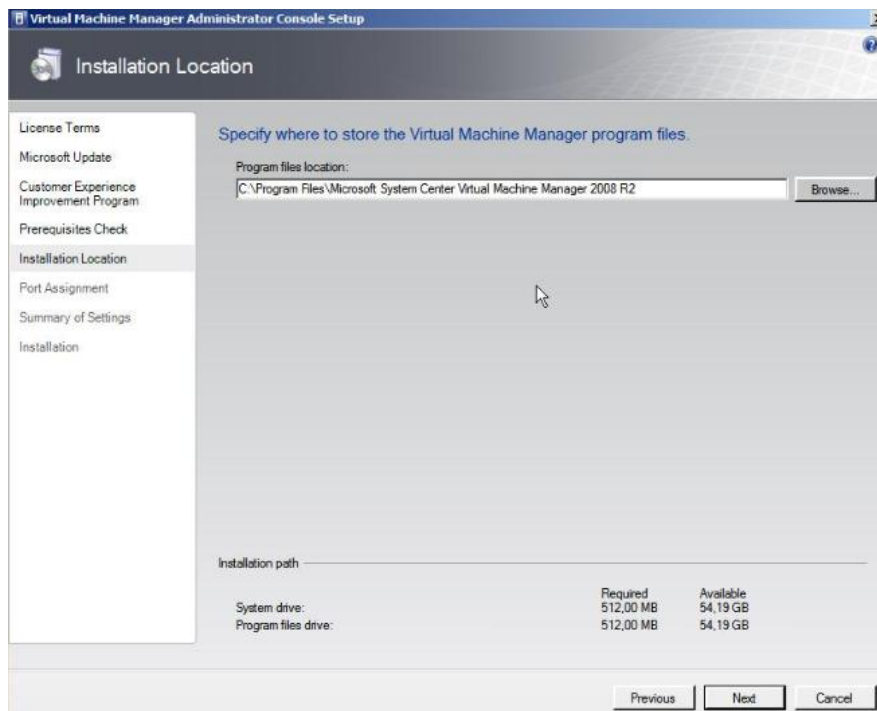
2. ASENNETAAN VMM ADMINISTRATOR CONSOLE



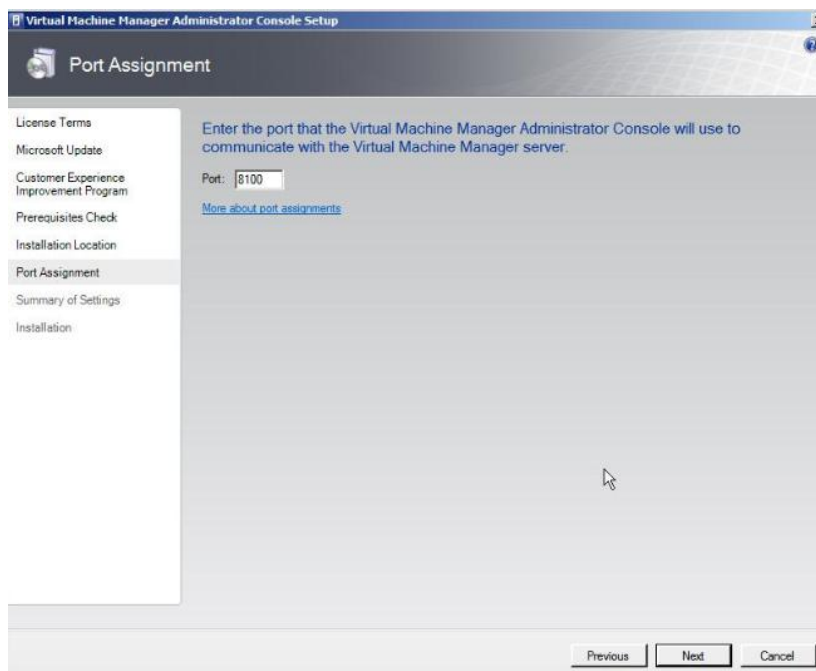
2.1 Asennus tapahtuu SCVMM asennusmedialta valitsemalla kohta VMM Administrator Console. Seuraavassa kohdassa pyydetään vahvistamaan ohjelmiston lisenssiehdot ja valitaan käytetäänkö Microsoft Update palvelua päivitysten tarkistamiseen.



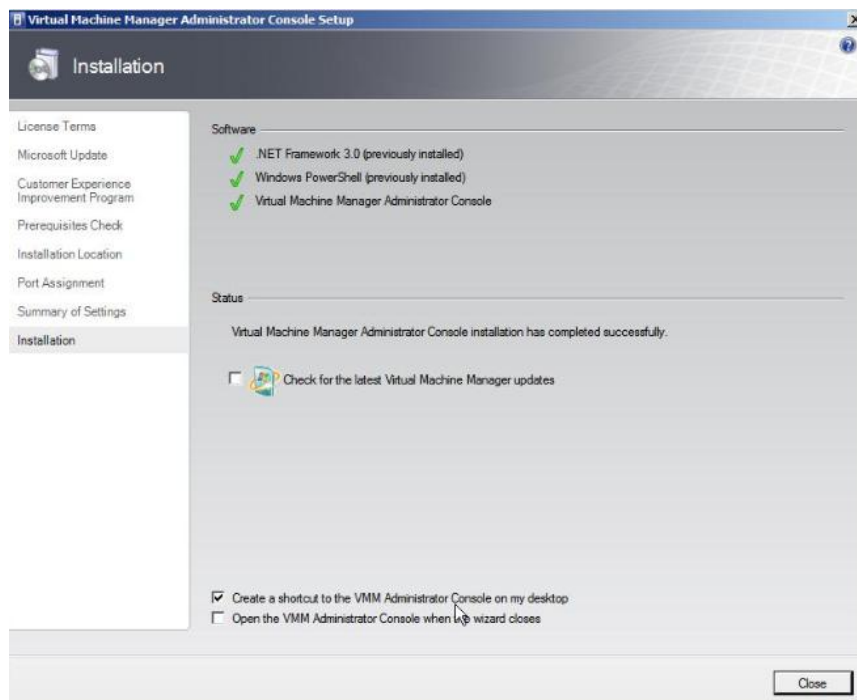
2.2 Asennusohjelma tarkistaa ohjelmisto- ja järjestelmävaatimukset.



2.3 Installation Location kohdassa valitaan mihin Virtual Machine Managerin ohjelmatiedostot sijoitetaan. Valitsimme taas paikallisen koneen kovalevyn kohdeasemaksi.

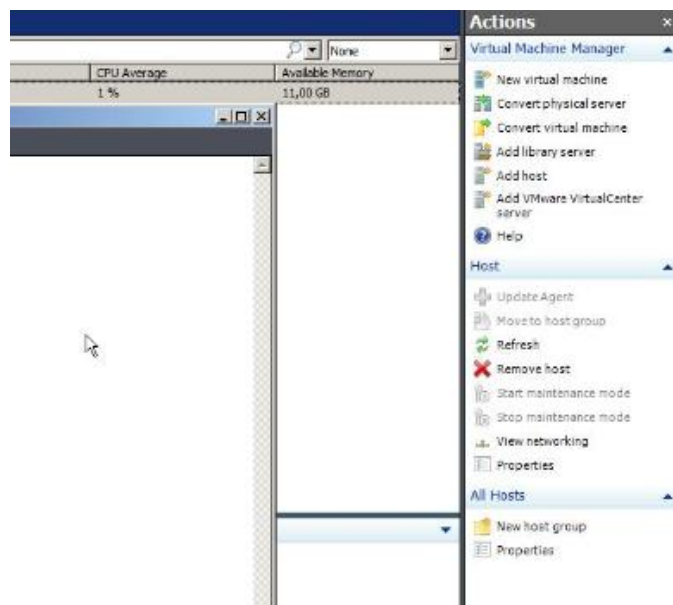


2.4 Port Assignment kohdassa määritetään mitä porttia Administrator Console käyttää kommunikointiin SCVMM-Serverin kanssa. Valitsimme oletusportin 8100, joka on sama kuin SCVMM-Serverin asennuksessa määritettiin. Seuraavassa vaiheessa asennus näyttää yhteenvedon aikaisemmissa vaiheissa määritetyistä asetuksista ja aloittaa varsinaisen asennuksen.

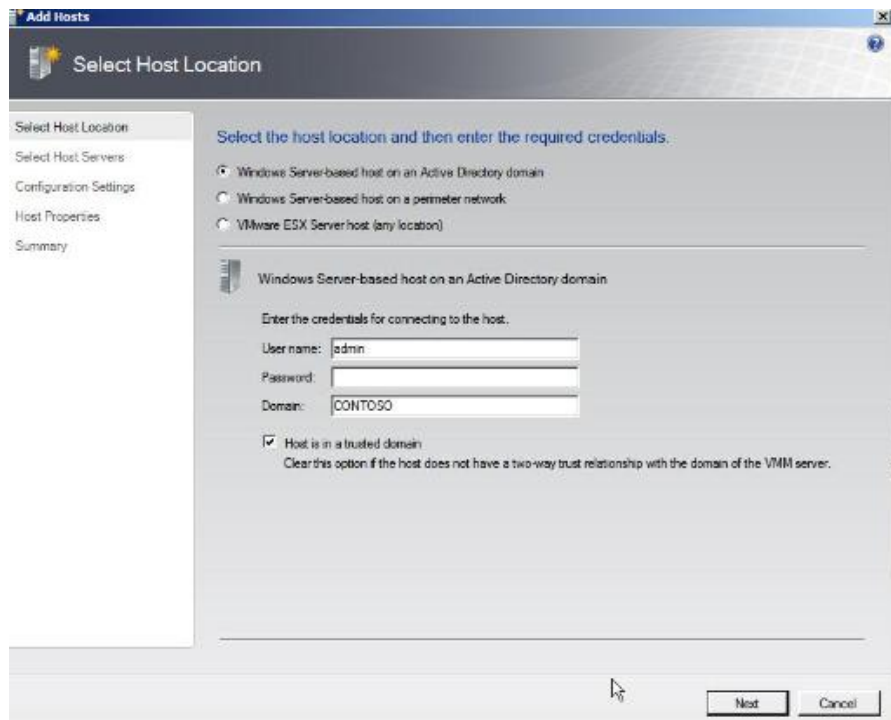


2.5 Asennuksen lopuksi näytetään yhteenveto asennetuista komponenteista ja pyytää järjestelmää tarkistamaan viimeisimmät päivitykset. Samasta ikkunasta voidaan myös käynnistää ohjelma asennuksen päätyttyä ja luoda pikakuvake työpöydälle.

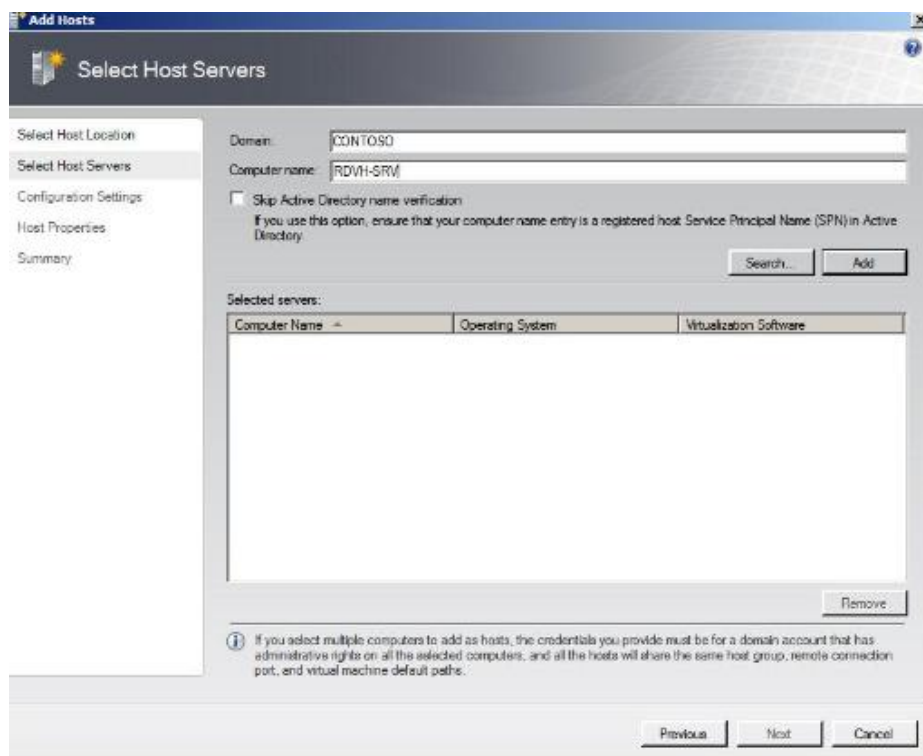
3. VIRTUALIZATION HOST



3.1 Palvelimen toimintakuntoon saattaminen vaatii Virtualization Hostin lisäämisen. Lisääminen tapahtuu klikkaamalla toimintoa Add host.



3.2 Host location kohdassa valitsimme Windows Server pohjaisen vaihtoehdon, mikä lisää Active Directory domainissa olevan isännän. Seuraavaksi asennus pyytää syöttämään tunnuksen, jolla on oikeus lisätä kone osaksi ympäristöä.

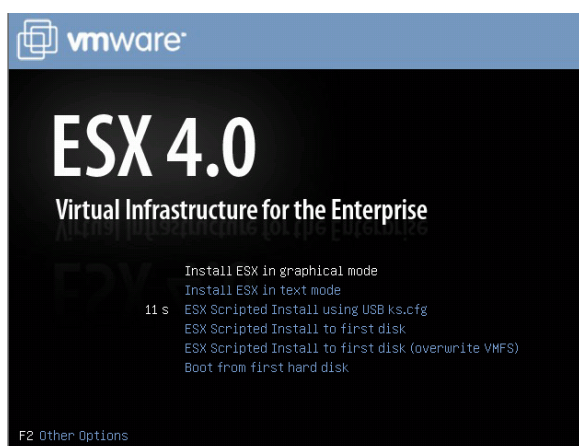


3.3 Viimeistellään asennus valitsemalla ensin Next ja sen jälkeen Finish.

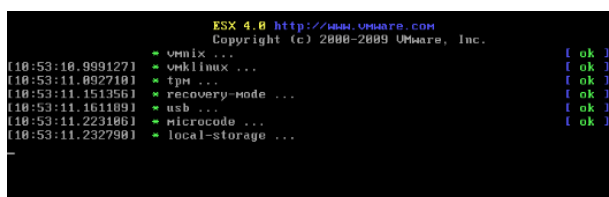
Liite 3 VMware View 4.0 asennus

1. ESX 4.0 Palvelimen asennus
2. ESX 4.0 Hallintakone
3. Active Directory
4. vCenter
5. VMware View Connection Server 4
6. Määrittys
7. Virtuaalisten työpöytien määrittäminen
8. VMware View Client asennus
9. VMware iew Manager konfigurointi
10. Poolin käyttäjäryhmien määrittely
11. Poolin toimivuuden testaus

1. ESX 4.0 PALVELIMEN ASENNUS



1.1 Käynnistetään graafinen asennus valitsemalla “install ESX in graphical mode”. Asennukseen käytettiin levylle poltettua asennusmediaa.



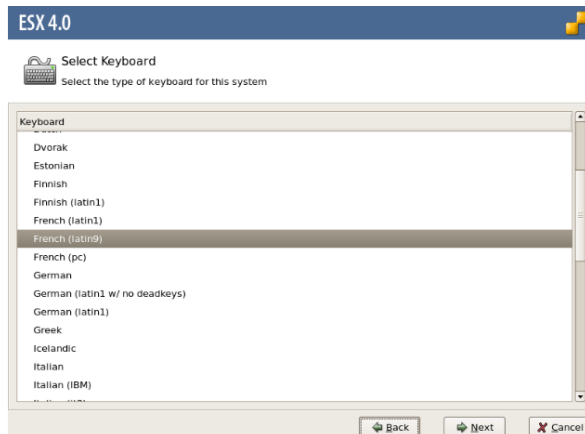
1.2 Asennus käynnistyy ja samalla ruudulle tulee tietoja ladatuista komponenteista.



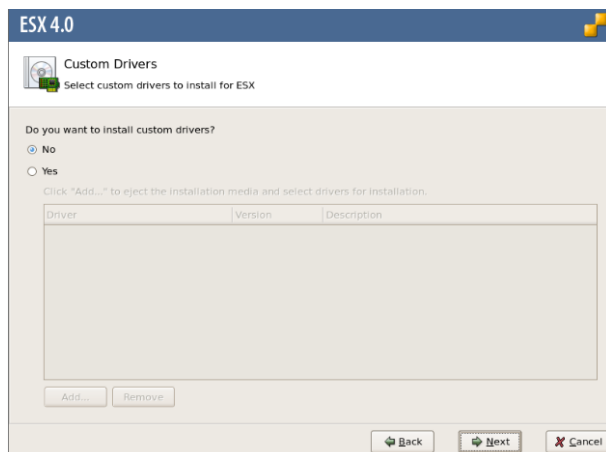
1.3 Tässä vaiheessa asennusohjelma käynnistää graafisen liittymän. Siirrytään seuraavaan vaiheeseen painamalla ”next”.



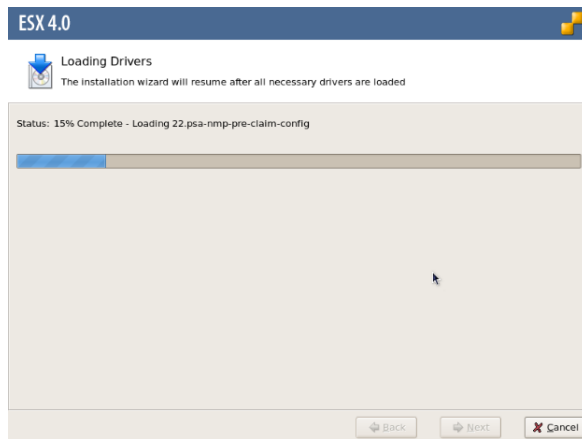
1.4 Asennusohjelma pyytää lukemaan lisenssiehdot. Siirrytään eteenpäin painamalla ”next” ja samalla hyväksytään annetut lisenssiehdot.



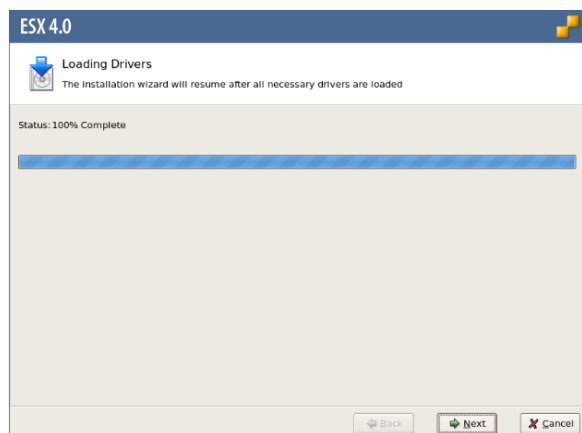
1.5 Valitaan haluttu näppäimistön kieliasettelu, siirrytään eteenpäin valinnalla ”next”.



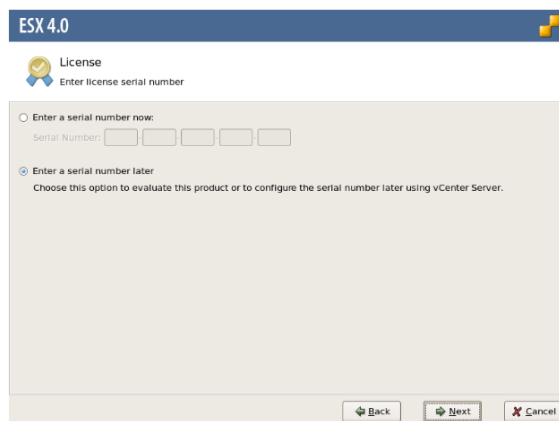
1.6 Tässä vaiheessa on mahdollista asentaa järjestelmän vaatimia laiteajureita. Testiympäristömme ei vaatinut erikoisajureiden käyttöä, joten siirryimme perusasetuksilla eteenpäin.



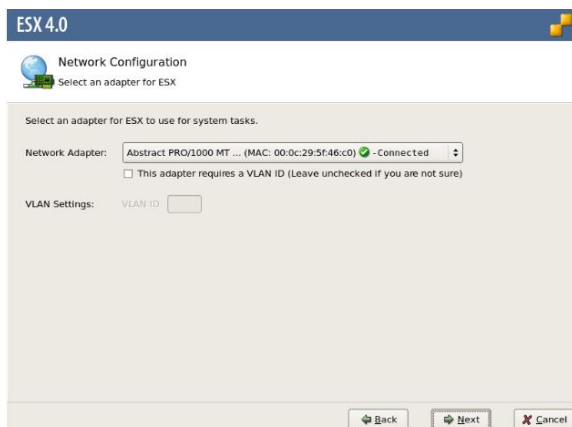
1.7 Asennusohjelma lataa tarvittavat ajurit.



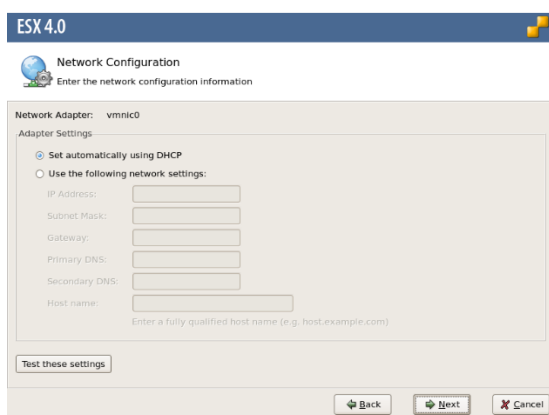
1.8 Ajureiden lataamisen jälkeen voidaan jatkaa varsinaista asentamista eteenpäin.



1.9 Käytimme testaamista varten olevaa lisenssiä (Evaluation 60pv) ja valitsimme kohdan ”Enter a serial number later”.



1.10 Määritetään mitä verkkokorttia ESX käyttää järjestelmätehtäviin.



1.11 Syötetään verkkoasetukset käsin tai valitaan DHCP käyttöön. Tässä ympäristössä määritimme asetukset manuaalisesti ja osoitteet kiinteiksi.

Verkkoasetukset:

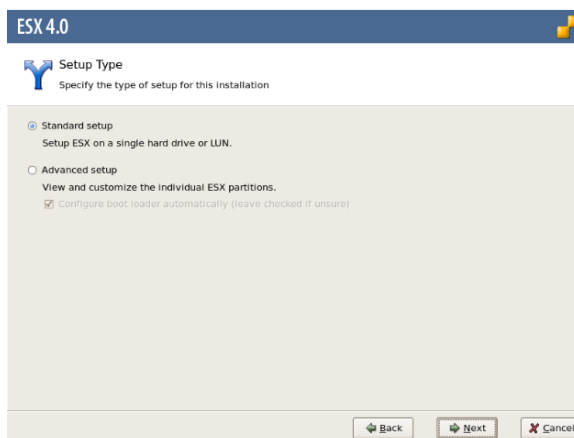
IP : 10.0.0.69

Mask : 255.255.255.0

Gateway:10.0.0.1

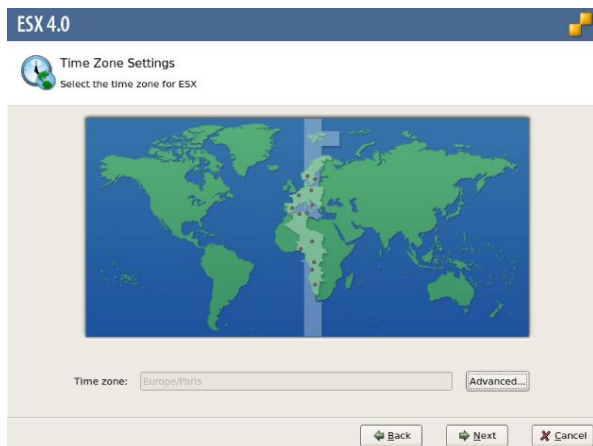
DNS :10.0.0.1

Hostname : esx.test.com

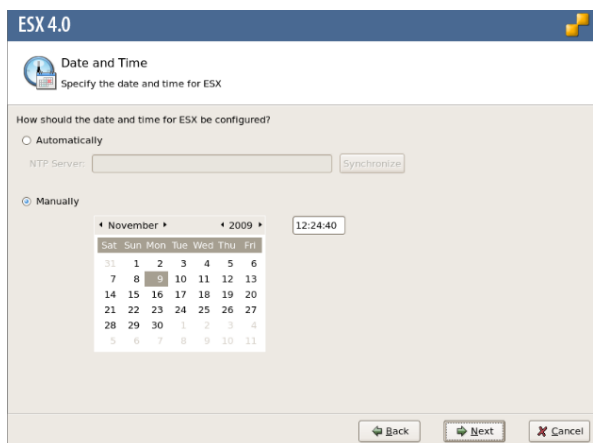


1.12 Tässä vaiheessa voidaan määrittää mihin ESX halutaan asentaa. Valitsimme "Standard setup" vaihtoehdon, koska halusimme asentaa sen yhteen sijaintiin.

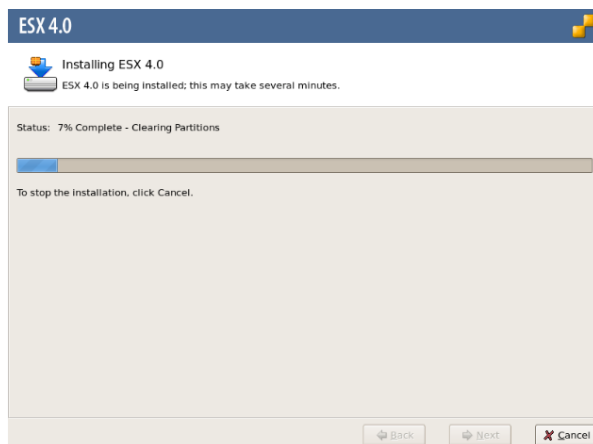
1.13 Asennuskohteeksi määritimme IBM x3650 palvelimen D-aseman. Vapaata tilaa asemalla oli n. 180Gt



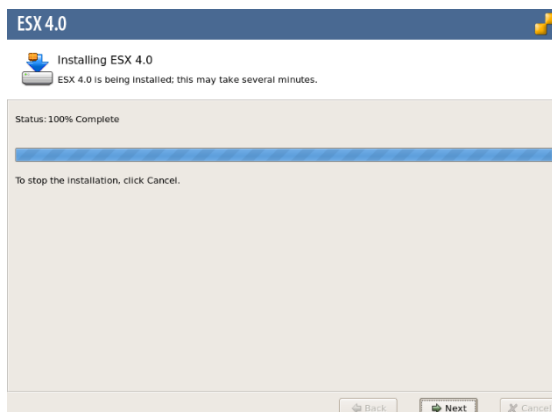
1.14 Valitaan haluttu aikavyöhyke



1.15 Määritetään päivämäärä ja aika-asetukset manuaalisesti tai automaattisesti. Valitsimme manuaalisen vaihtoehdon, koska testiympäristömme ei ollut yhteydessä Internetiin.



1.16 ESX 4.0 Suorittaa asennuksen loppuun.

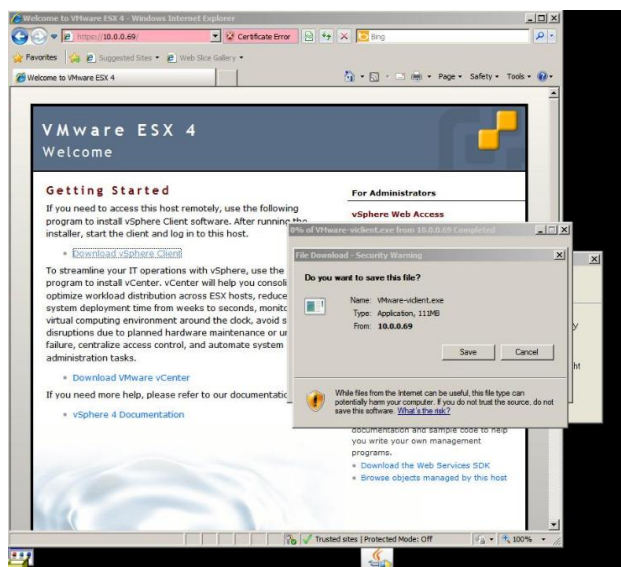


1.17 Ohjelma ilmoittaa onnistuneesta asennuksesta ja pyytää siirtymään eteenpäin.



1.18 Viimeisessä vaiheessa asennusohjelma pyytää käynnistämään palvelimen uudestaan. Yhteenvedosta selviää vielä palvelimen IP-osoite, josta sitä pystytään hallinnoimaan.

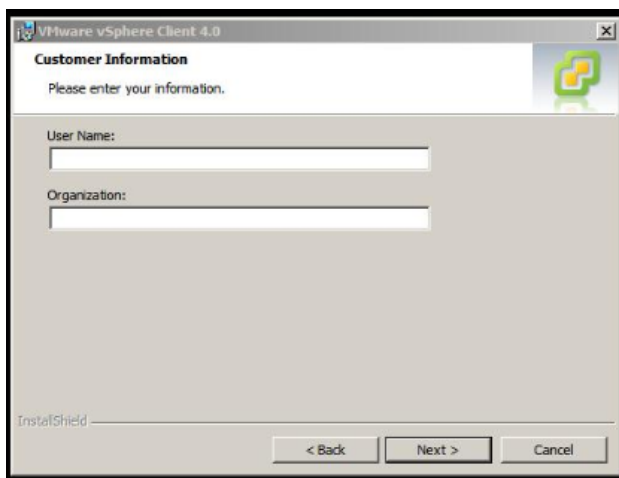
2. ESX 4.0 HALLINTAKONE



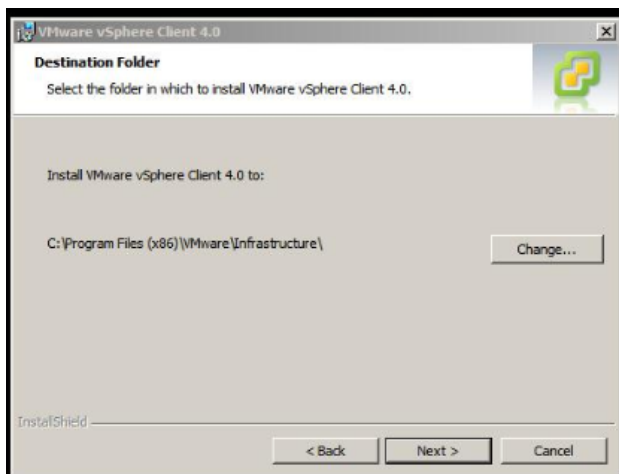
2.1 Palvelimen hallintaa varten asiakaskoneelle pitää ladata VMware vSphere Client. Tämän saa ladattua menemällä samassa verkossa olevalta koneelta palvelimen -osoitteeseen 10.0.0.69. Selaimen ikkunaan aukeaa VMware ESX 4 "Getting Started" sivu.



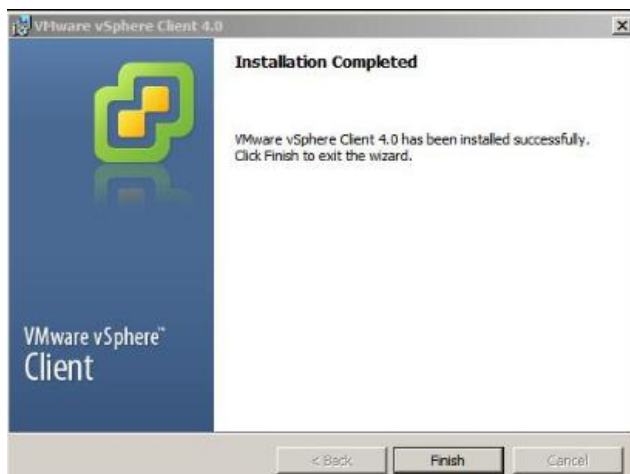
2.3 VMware vSphere Client asennus käynnistyy



2.4 Syötetään käyttäjänimi ja organisaation tiedot



2.5 Valitaan hakemisto mihin asiakasohjelma asennetaan



2.6 Asennusohjelma ilmoittaa onnistuneesta asennuksesta ja pyytää viimeistelemään asennuksen painamalla "finish".

3. ACTIVE DIRECTORY

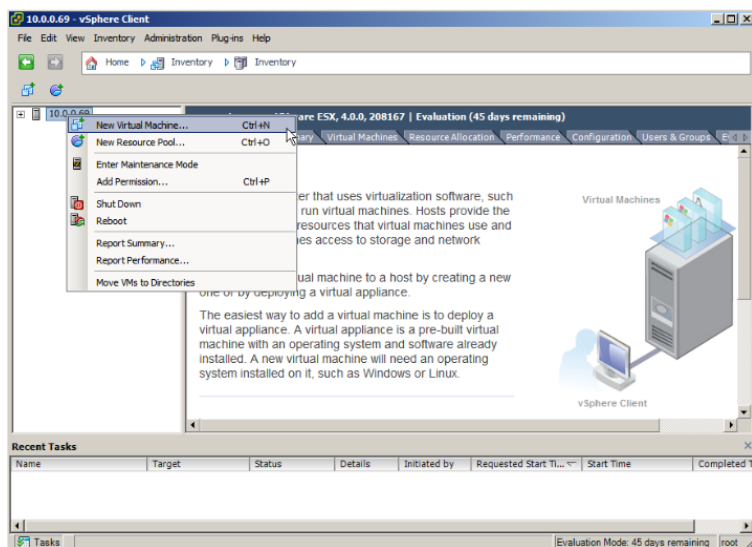
Yhtenä vaatimuksena VMware View 4 ympäristölle on toimiva Active Directory. Hyödynsimme Microsoftin testiympäristössä käyttämäämme Active Directory -palvelinta. Liitimme fyysiset ja virtuaaliset laitteet osaksi esx.test.com toimialuetta.

4. vCenter

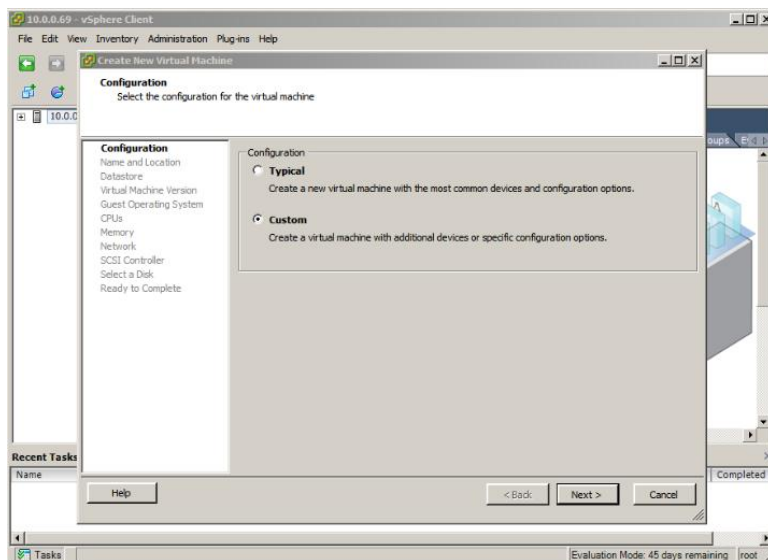
vCenter voidaan asentaa joko fyysiselle palvelimelle tai virtuaalisesti ESX 4.0 palvelimelle, kuten testiympäristössämme.



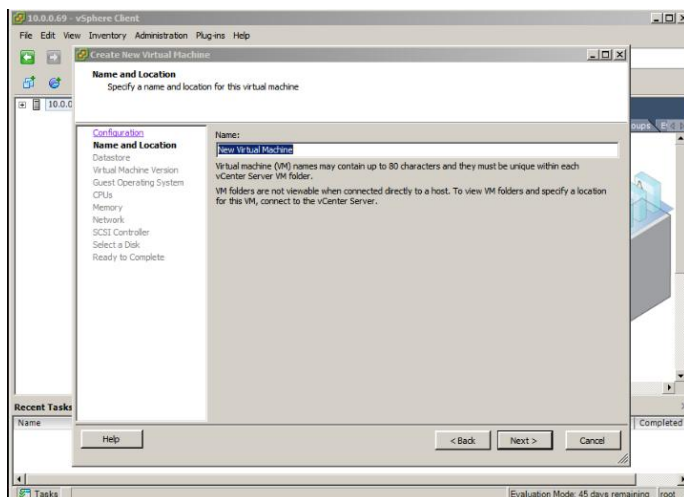
4.1 Ennen varsinaista vCenterin asennusta loimme virtuaalisen Server 2003sp2 vCenter palvelinta varten. Virtuaalipalvelimen asennus tapahtuu ottamalla yhteys ESX-palvelimeen vSphere clientilla tai myöhemmässä vaiheessa vCenterillä.



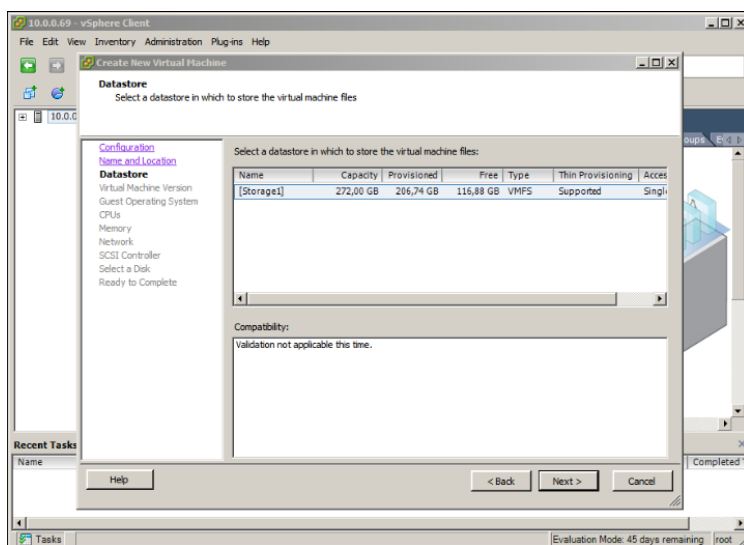
4.2 Virtuaalikoneen luomin käynnistyy komennolla Ctrl+N tai valikosta ”New Virtual Machine”.



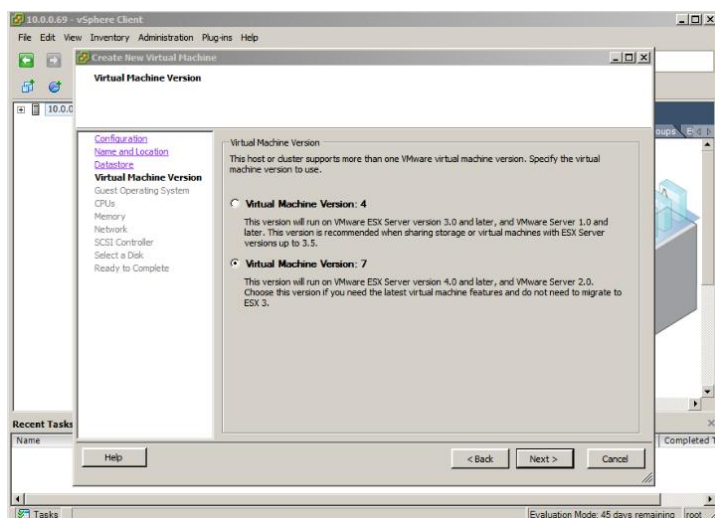
4.3 Ohjattu toiminto käynnistyy ja siitä voidaan valita joko tyypillinen tai mukautettu asennus. Etenimme mukautetulla asennuksella, koska halusimme määrittellä virtuaalikoneen käyttämät resurssi tarkasti.



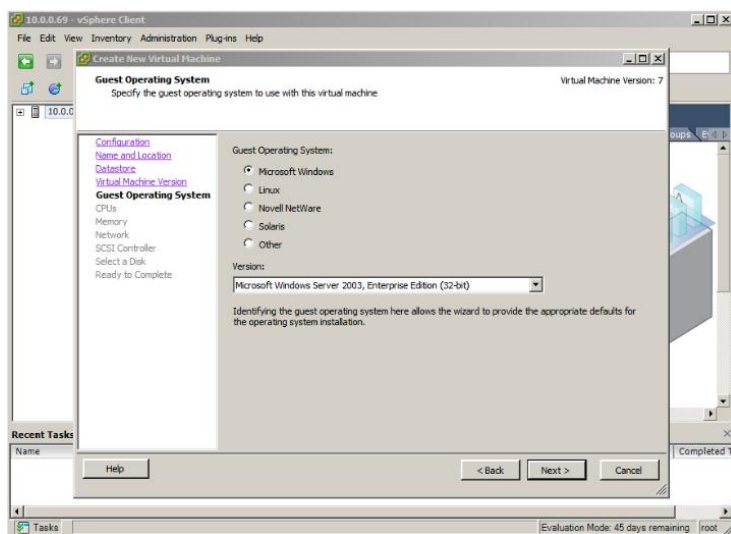
4.4 Tässä kohtaa annetaan virtuaalikoneelle nimi.



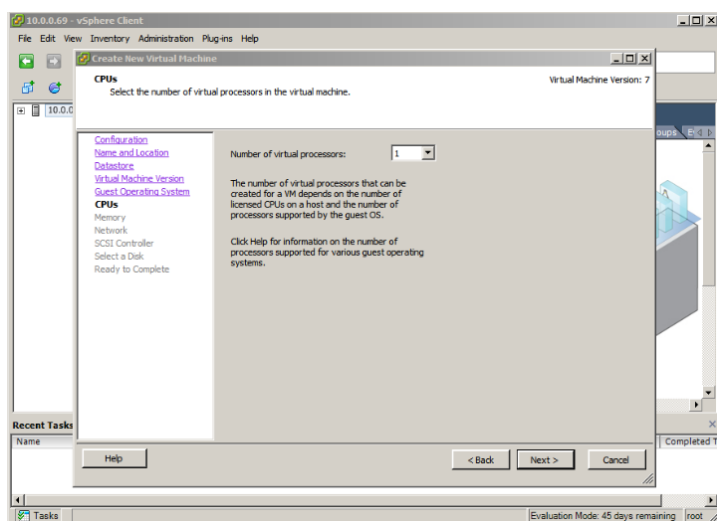
4.5 Valitaan sijainti johon virtuaalikoneen tiedot tallennetaan. Testiympäristössä tallennuspaikkana toimi ESX-palvelimen paikallinen kovalevy.



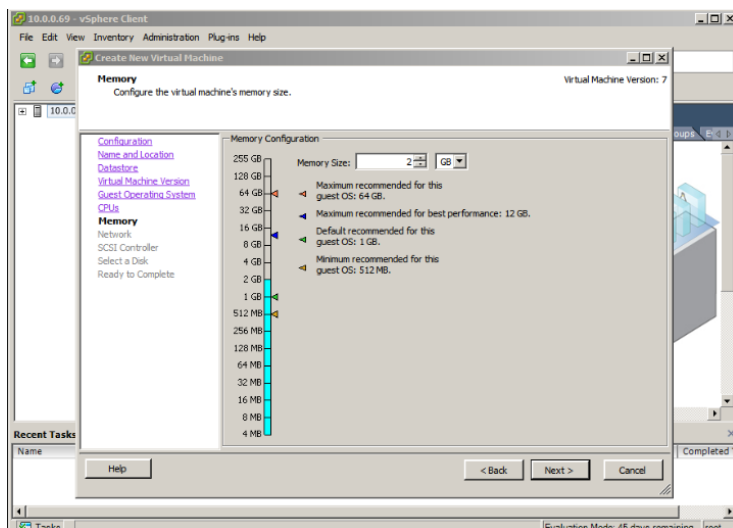
4.6 Asennusvaiheessa voidaan määrittää mitä versiota virtuaalikone tulee käyttämään. Ympäristössä käytimme viimeisintä versiota (version 7), koska taaksepäin yhteensopivuudelle ei ollut tarvetta.



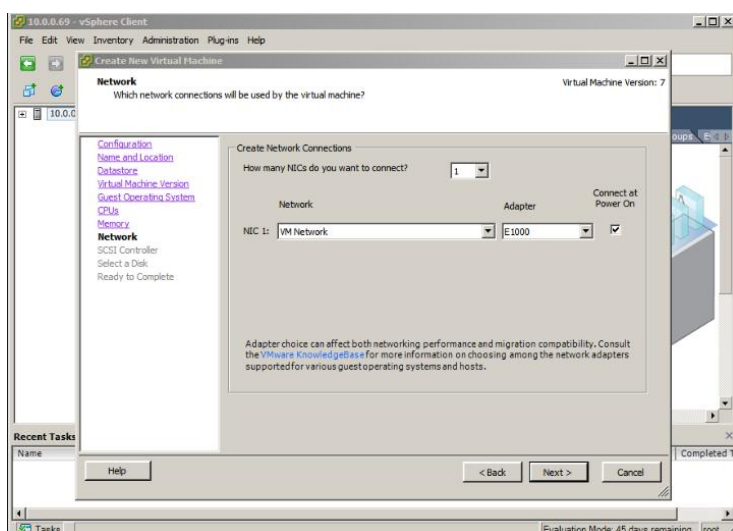
4.7 Määritetään virtuaalikoneen käyttöjärjestelmä, Microsoft Windows Server 2003 Enterprise Edition (32-bit)



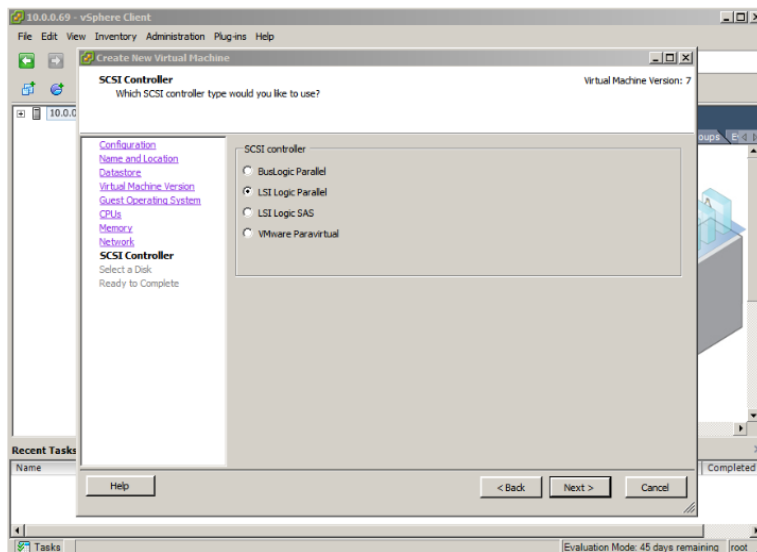
4.8 Annoimme palvelimelle käyttöön yhden virtuaalisen prosessorin.



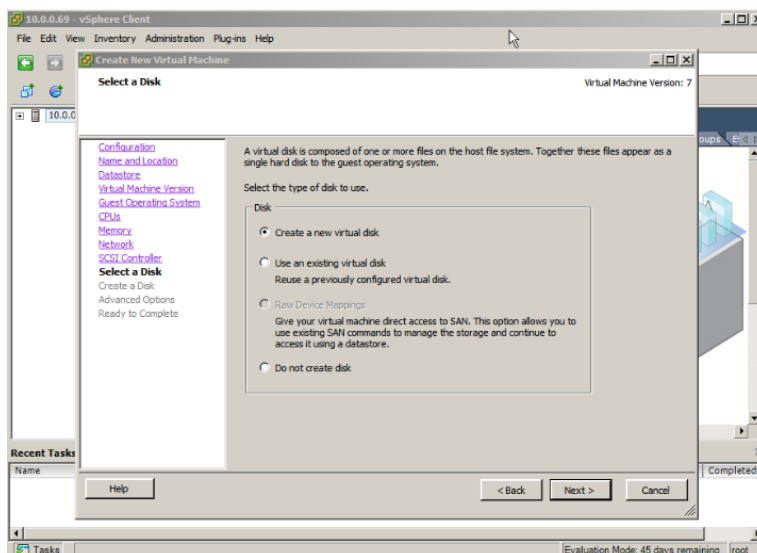
4.9 Varasimme muistia 2Gt koneelle.



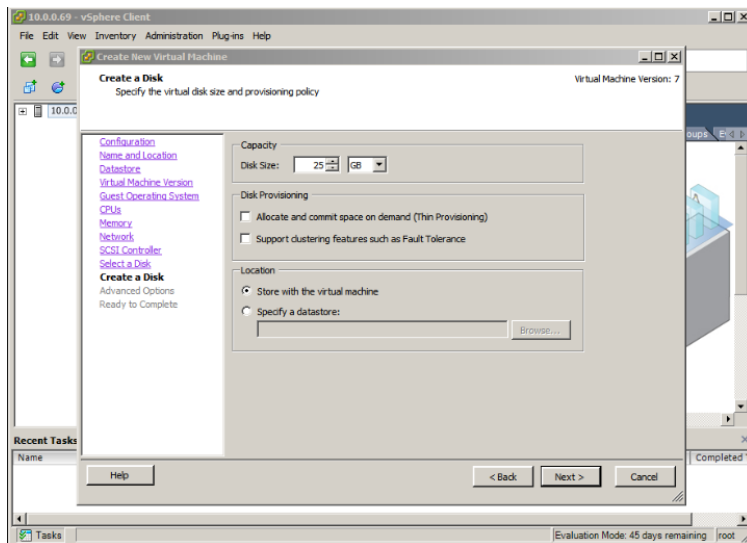
4.10 Tässä kohtaan valitaan mitä verkkokorttia virtuaalikone käyttää ja määritetään sen automaattinen käynnistyminen. Valitsimme isäntäpalvelimen tarjoaman verkkosovittimen ja valitsimme sen kytketymään päälle virtuaalikoneen käynnistyessä.



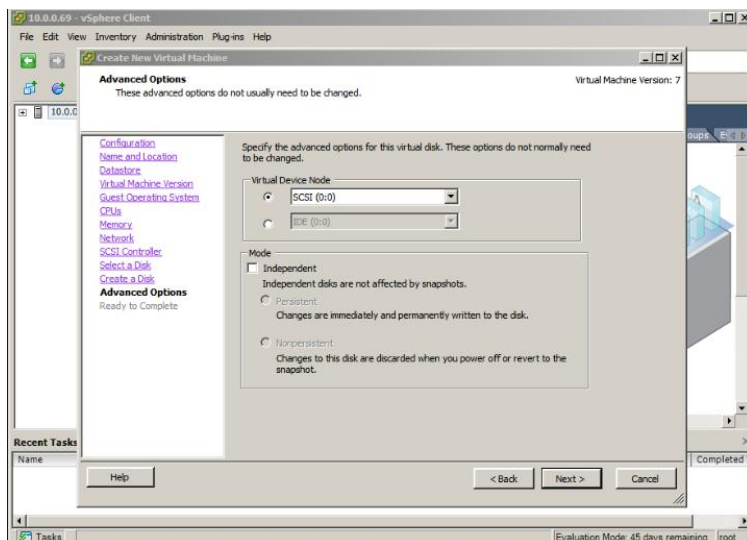
4.11 Hyväksyimme SCSI-levyohjaimeksi LSI Logic Parallelin.



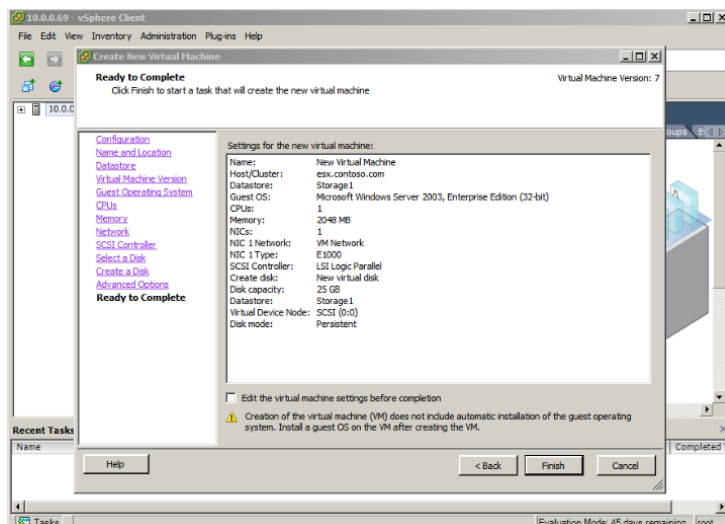
4.12 Luodaan uusi virtuaalinen kovalevy tai voidaan hyödyntää jo olemassa olevaa levyä. Teimme uuden virtuaalisen kovalevyn asennusta varten.



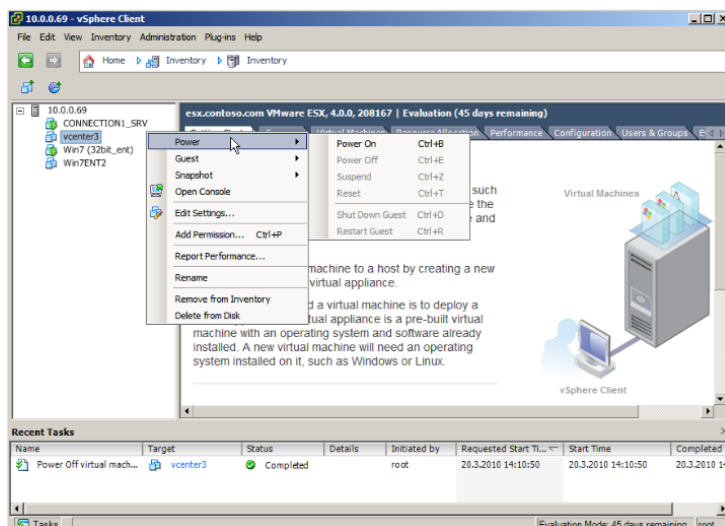
4.13 Varasimme palvelimen käyttöön 25Gt tilaa. Vaihtoehtona olisi ollut varata tila dynaamisesti levyn käytön mukaan. Näillä asetuksilla virtuaalikone ja levy tallennetaan samaan sijaintiin.



4.14 Hyväksymme asennusohjelman suosittelemat vaihtoehdot levyasetuksille.

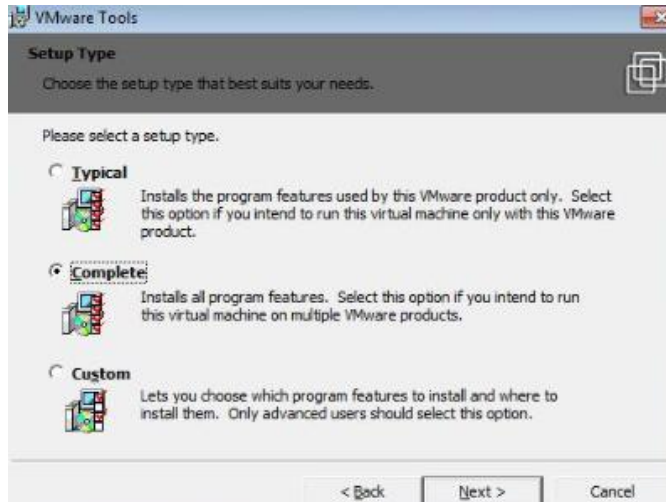


4.15 Asennuksen lopussa ohjelma näyttää yhteenvedon valituista asetuksista. Asennus viimeistellään painamalla ”Finish”.



4.16 Käyttöjärjestelmän asennus virtuaalikoneeseen tapahtuu seuraavalla tavalla:

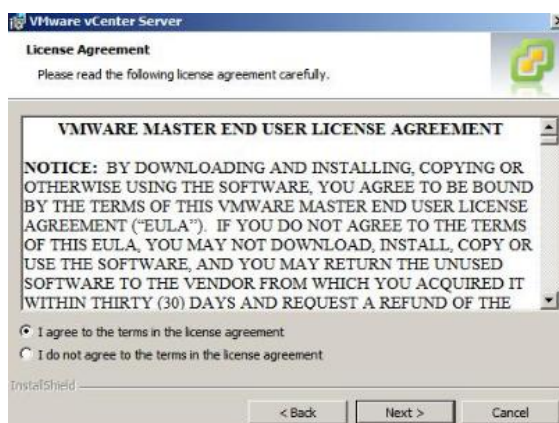
- Kytetään virtuaalikoneeseen virta päälle toiminnolla ”Power on”.
- Yhdistetään koneeseen toiminnolla ”Open Console”, mikä avaa virtuaalikoneen graafisen käyttöliittymän.
- Valitaan virtuaalikoneen asetuksista mitä levyasemaa tai iso-tiedostoa hyödynnetään käyttöjärjestelmän asennuksessa.
- Itse käyttöjärjestelmän asennus sujuu samalla tavalla kuin asennettaisiin käyttöjärjestelmä fyysiseen koneeseen.
- Käyttöjärjestelmän asennuksen jälkeen määritellään koneelle kiinteä IP-osoite ja liitetään osaksi toimialuetta.



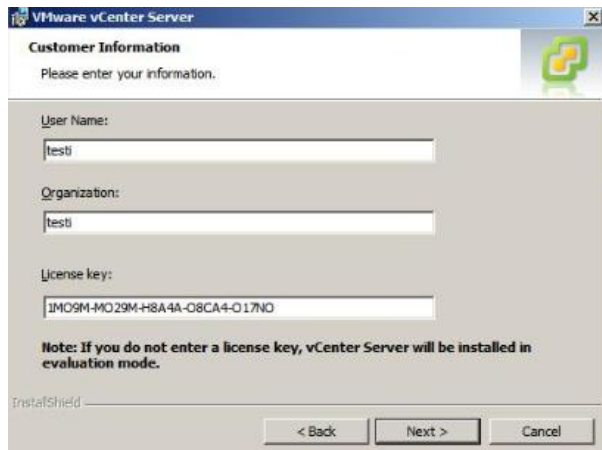
4.17 Kaikkiin virtuaalikoneisiin tulee asentaa VMware Tools. Asentaminen tapahtuu kirjautumalla virtuaalikoneelle järjestelmävalvojan oikeuksilla ja valitsemalla yläpalkista VM->Guest->Install VMware Tools. Tällöin käynnistyy asennusohjelmisto näytölle, josta voidaan määritellä mitä kaikkia työkaluja halutaan asennettavan.



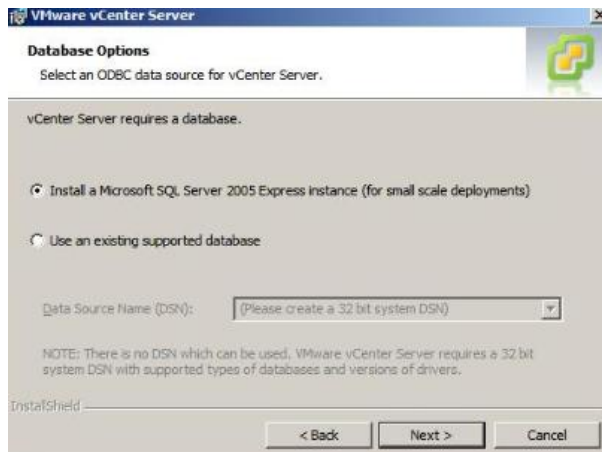
4.18 Käynnistä asennustiedosto VMware vCenter Server 4.0 ja valitse vCenter Server.



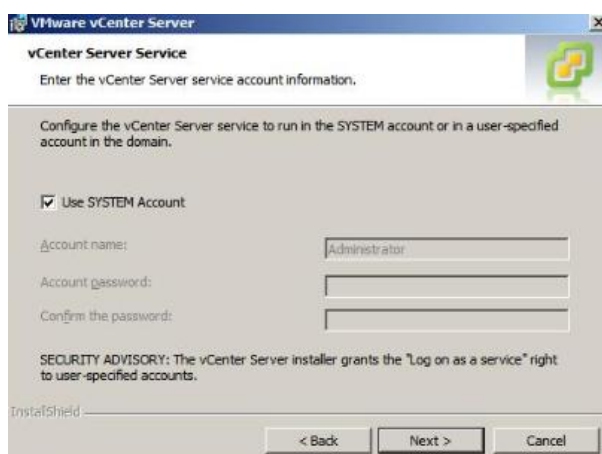
4.19 Luetaan ja hyväksytään lisenssiehdot.



4.20 Täytetään käyttäjä ja organisaatio tiedot ja virallinen lisenssiavain, mikäli ei käytetä kokeiluversiota (60pv).



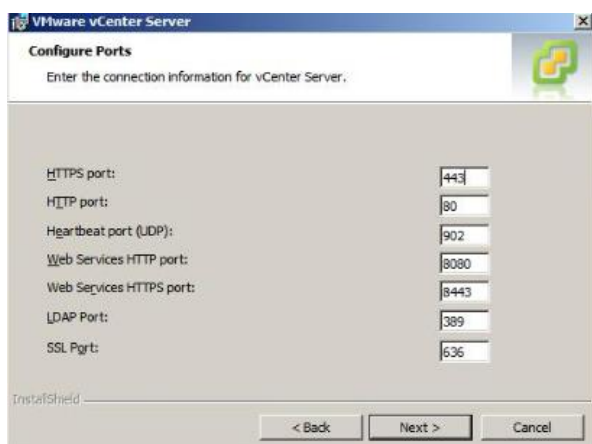
4.21 vCenter vaatii tietokantaohjelmiston toimiakseen. vCenterin asennuspaketin mukana tulee Microsoft SQL Server 2005 Express edition, jota voidaan käyttää uuden tietokannan luomiseen. Tuotantoympäristössä on syytä käyttää kehittyneempää versiota SQL Serveristä, Express Editionin tietokannan kokoa koskevien rajoitteiden vuoksi. Testiympäristössämme käytimme asennuspaketin tarjoamaa versiota.



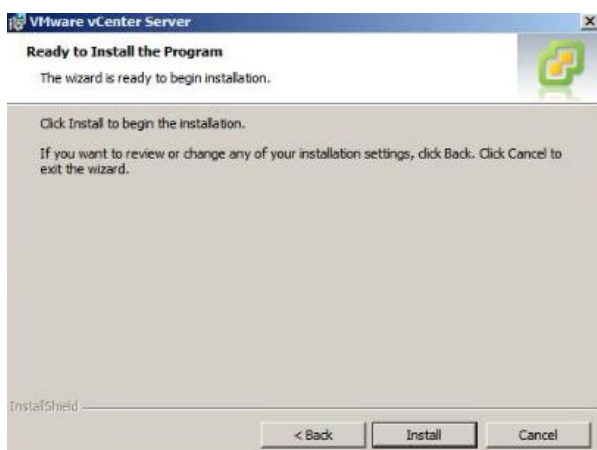
4.22 Määritetään vCenterin hallinointiin käytettävä järjestelmänvalvojan tunnus.



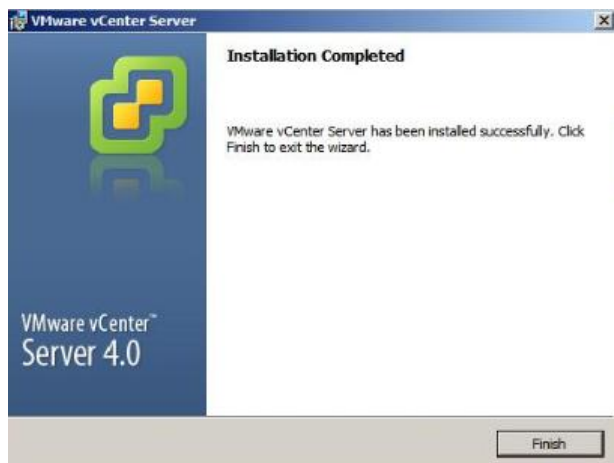
4.23 Tässä kohdassa voidaan valita asennetaanko VMware vCenter standalone vai linked mode asennuksena. Ensimmäinen vCenter Server palvelimen vaatimuksena on standalone, joten valitaan ”Create a standalone VMware vCenter Server instance”. Tarvittaessa voidaan asentaa toinen VMware vCenter Server linked mode asennuksena.



4.24 Tässä kohdassa voidaan määrittellä järjestelmän käyttämien tietoliikenneporttien asetukset halutun laiseksi. Testiympäristössä hyödynsimme oheisia oletusportteja.



4.25 Valitaan ”Install” asennuksen käynnistämiseen.



4.26 Ja viimeistellään asennus valitsemalla ”finish”.

5. VMware View Connection Server 4

VMware View Connection Server 4 voidaan asentaa joko erilliselle palvelimelle tai kuten testiympäristössämme virtuaalisesti ESX 4.0 palvelimelle. Ennen varsinaista asennusta loimme virtuaalisen Server 2003sp2 palvelimen. Virtuaalipalvelimen asennus tapahtuu ottamalla yhteys ESX-palvelimeen vSphere clientilla samalla tavalla kuin aiemmin vCenterin asennuksessa.

5.1 Asennus käynnistetään Connection Server asennuspaketista.



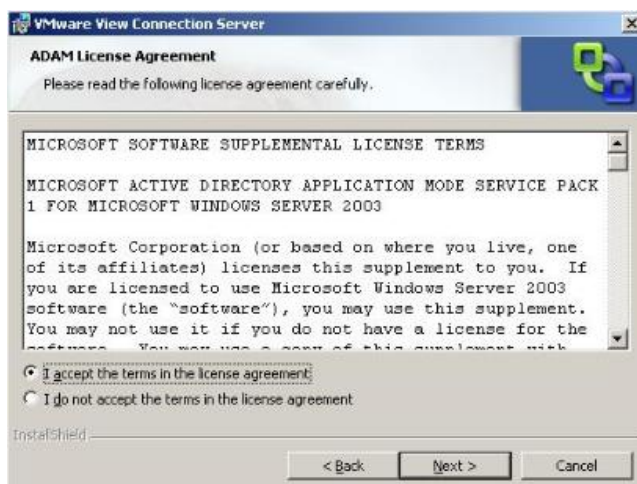
5.1 Asennus käynnistetään Connection Server asennuspaketista.



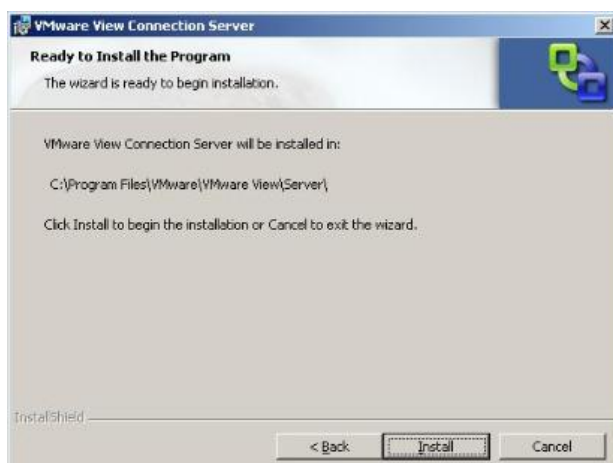
5.2 Valitaan kohdesijainti asennukselle.



5.3 Ensimmäinen Connection Server tulee asentaa Standard-versiona. Mikäli halutaan tehdä useampi Connection Serveri pohjautuen aikaisempaan asennukseen, valitaan Replica-määritys.



5.4 Luetaan ja hyväksytään lisenssiehdot.



5.5 Valitaan "Install" asennuksen aloittamiseksi.

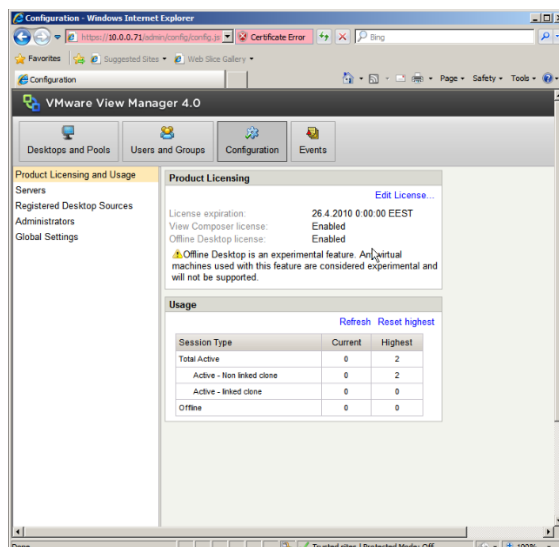


5.6 Viimeistele asennus ”finish” painikkeella.

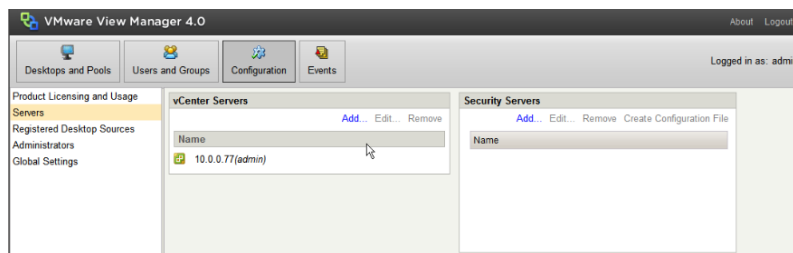
6. MÄÄRITYS

6.1 View managerin konfigurointi ja hallinta

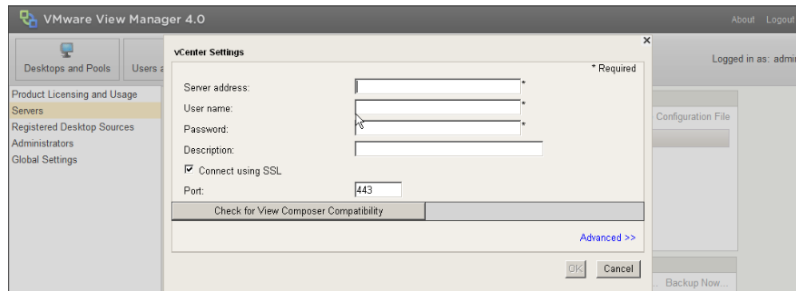
Mennään selaimella osoitteeseen 10.0.0.71 ja kirjaututaan sisään domain administrator - tunnuksilla.



6.2 Lisensointi, Configuration välilehdeltä valitaan ”Product Licensing and Usage” ja syötetään lisenssiavain



6.3 VMware vCenter Serverin lisäys, Configuration välilehdeltä vasemmalta valitaan Servers kohta ja valitaan ”Add” VirtualCenter Servers paneelin kohdalta.

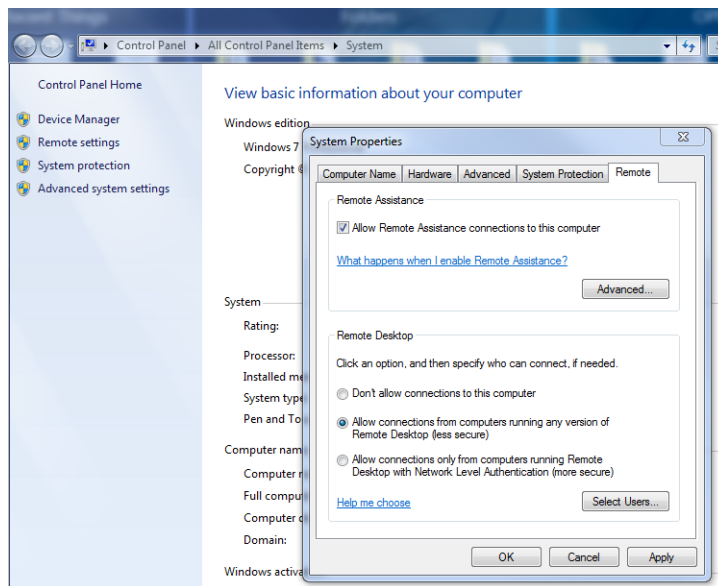


6.4 Syötetään Server address kohtaan VMware vCenter Serverin IP-osoite tai FQDN (full qualified domain name)
Syötetään vielä vCenterin järjestelmänhaltijan käyttäjänimi ja salasana niille varattuihin kohtiin.

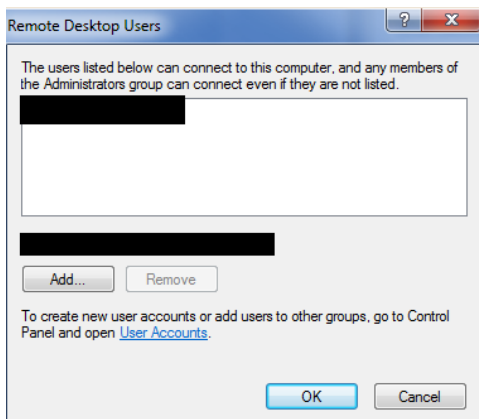
7. VIRTUAALISTEN TYÖPÖYTIEN LUOMINEN

Lähtökohtana on kaksi valmiiksi luotua virtuaalikonetta, joihin on asennettu valmiiksi Windows 7 Enterprise käyttöjärjestelmä. Virtuaalikoneiden luominen tapahtuu kohdassa 4.2 esitetyn ohjeen mukaisesti. Virtuaalikoneet on liitetty toimialueeseen. Koneisiin on sallittu ja määritetty käyttäjät etätyöpöytäyhteydelle. Kaikissa testiympäristön koneissa palomuurit on kytketty pois päältä. Tämän jälkeen voidaan asentaa VMware View Agent virtuaalikoneisiin, jotta View Manager pystyisi hallinnoimaan niitä. Agent asennetaan valmiista .msi-asennus paketista.

Agentin asentamisen jälkeen työpöydät ovat valmiita kustomoinnille. Ennen käyttöönottoa työpöytiin määritetään halutut asetukset ja ohjelmistot. Kun halutut määrittelyt on tehty, voidaan työpöytiin luoda palatuspiste (snapshot).



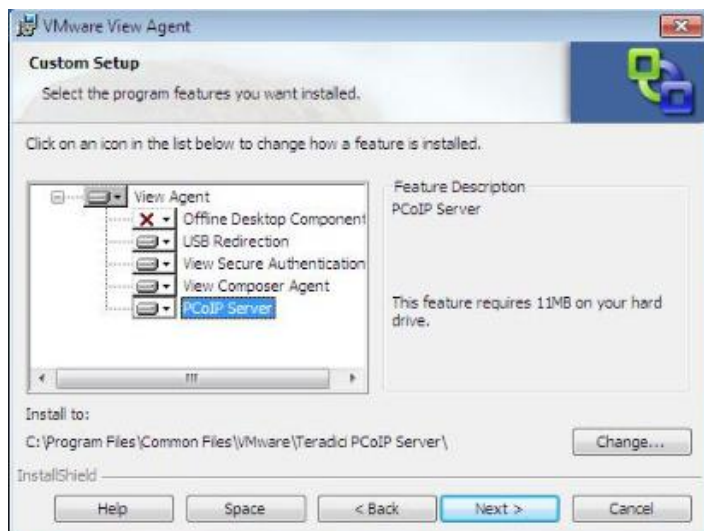
7.1 RDP-yhteyden salliminen ja käyttäjien lisääminen
Etäyhteyden salliminen tapahtuu kohdasta My Computer -> Properties -> Remote Settings



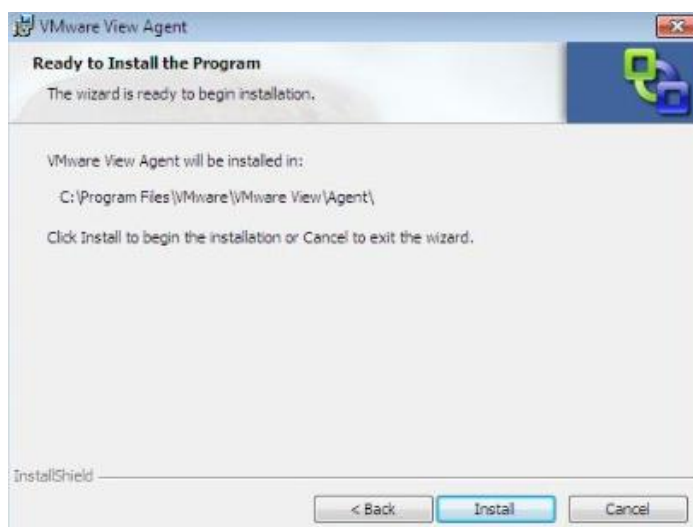
7.2 Sallittujen käyttäjien ja ryhmien lisääminen tapahtuu kohdasta "Select Users", josta aukeaa yllä olevan kuvan mukainen ikkuna. Valitse "Add" lisätäksesi halutut käyttäjät ja ryhmät.



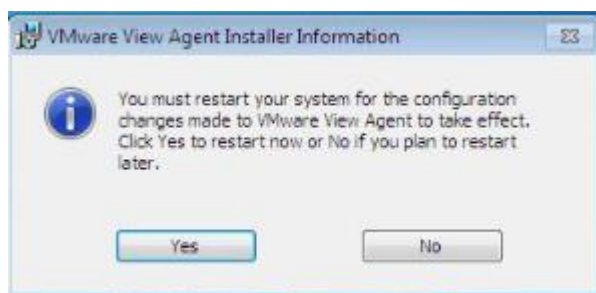
7.3 Käynnistetään VMware View Agent 4 asennus



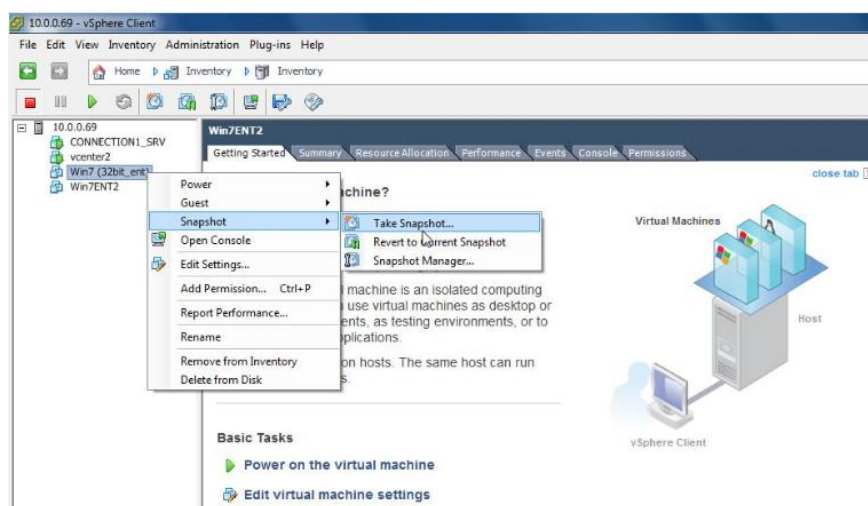
8.4 Asennusohjelma näyttää asennettavat komponentit. Jätimme valitsematta Offline Työpöydät sillä se ei ole testiympäristön tarkoitus.



7.5 Ennen asennuksen aloittamista tulostuu näytölle tieto siitä, mihin agentti asentuu.



7.6 Lopuksi pyydetään vielä käynnistämään järjestelmä uudestaan, jotta kaikki muutokset astuvat voimaan.



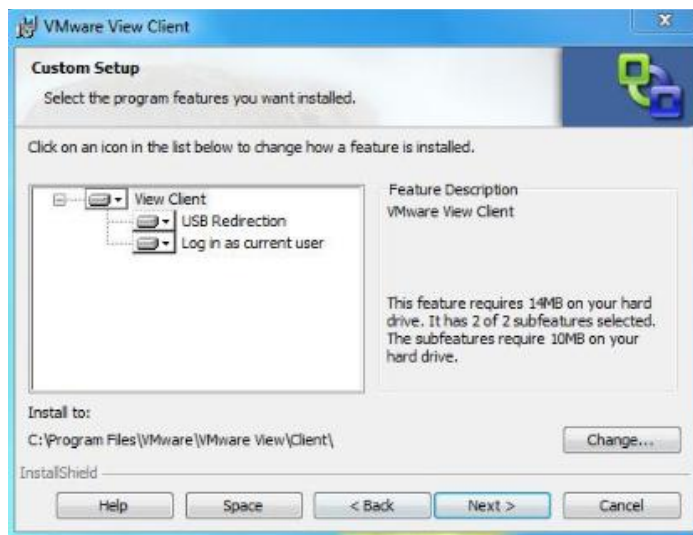
7.7 Palautuspisteen luonti tapahtuu vCenter hallintaliittymästä. Valitse hiiren oikealla painikkeella haluttu virtuaalikone ja navigoi Snapshot -> Take Snapshot. Voit nimetä palautuspisteen haluamallasi tavalla.

8. VMWARE VIEW CLIENT ASENNUS

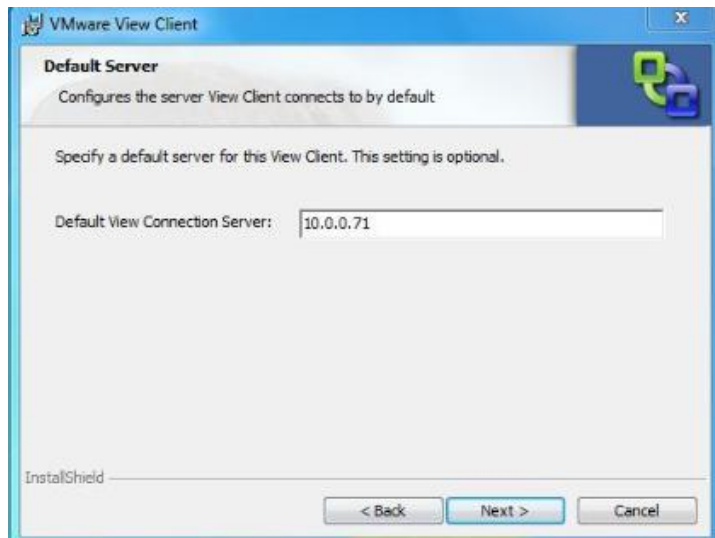
Tämä komponentti asennetaan fyysisiin työasemiin, joilta halutaan ottaa yhteys aiemmin luotuihin virtuaalisiin työpöytiin.



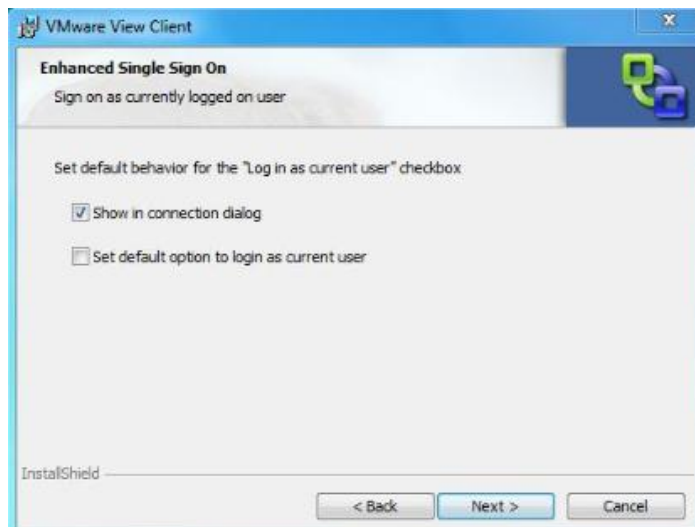
8.1 VMware View Clientin asennus käynnistetään asennuspaketista



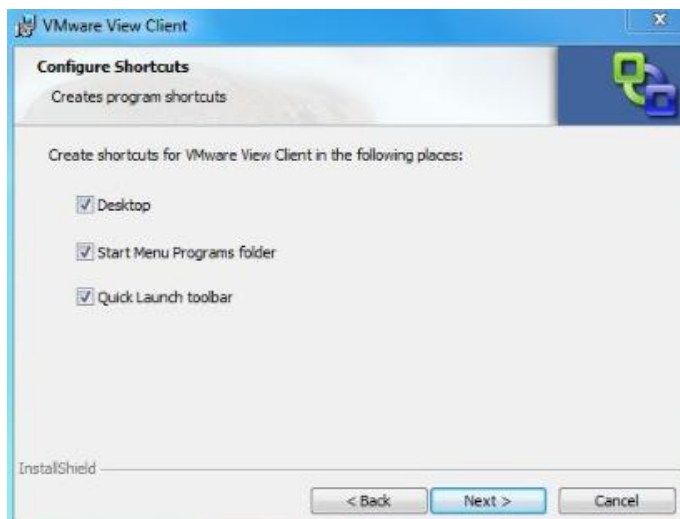
8.2 Valitse haluamasi asetukset. Oletusasetuksina käyttäjillä on mahdollisuus käyttää USB-laitteita ja kirjautuminen tapahtuu sillä käyttäjätillillä, millä koneelle on kirjauduttu. Käyttäjän kannalta on helpompaa, mikäli työpöydälle päästään yhdellä kirjautumisella (SSO-Single Sign On). Tässä voit vaihtaa asetuksia, mikäli on syytä. Oletusasetukset sopivat testiympäristön asetuksiin.



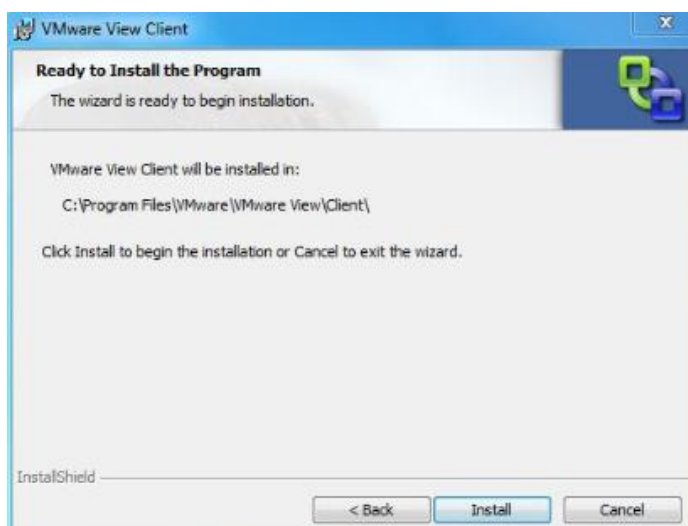
8.3 Syötä VMware View Connection Serverin IP-osoite, johon clientin halutaan ottavan yhteyttä. Testiympäristössämme View Connection palvelimen osoite on ”10.0.0.71”.



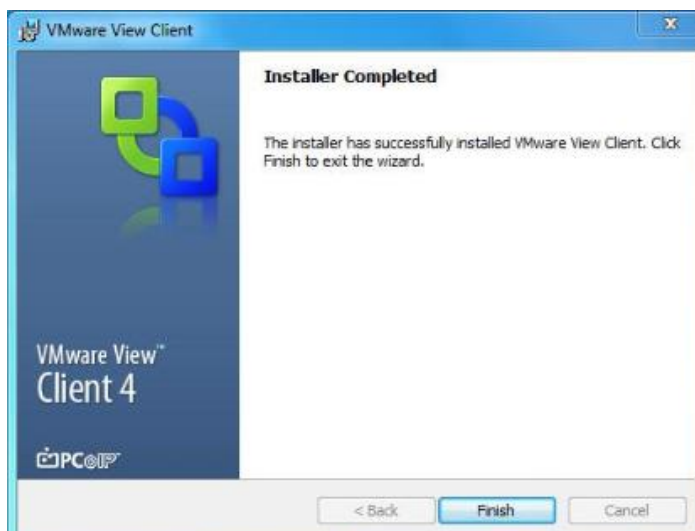
8.4 Tässä kohtaa määritellään oletusasetukset kirjautumiselle. Valinnalla ”Show in connection dialog” käyttäjälle näytetään kirjautumisen yhteydessä tietoja yhteydenluonnin edistymisestä.



8.5 Asennuksessa voidaan määrittää minne VMware View Client luo pikakuvakkeen.



8.6 Ennen asennuksen aloittamista, näet vielä minne Client asentuu.

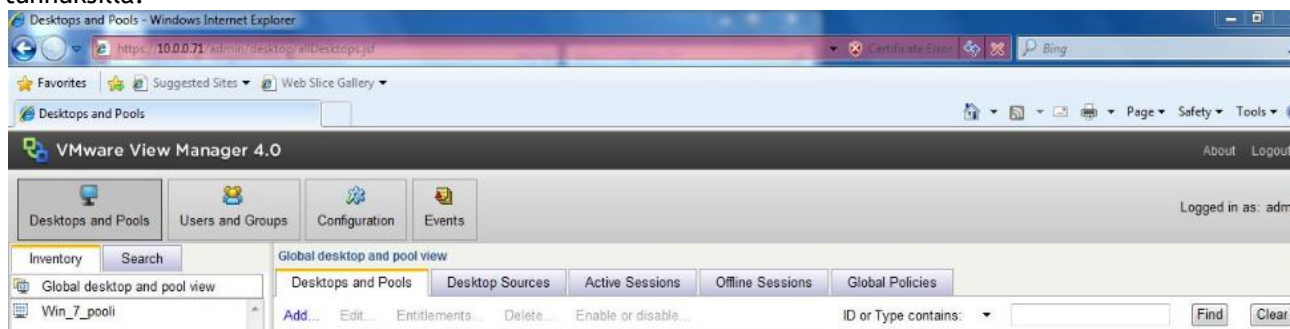


8.7 Asennus on onnistuneesti suoritettu ja "Finish" valinnalla siirrytään eteenpäin.

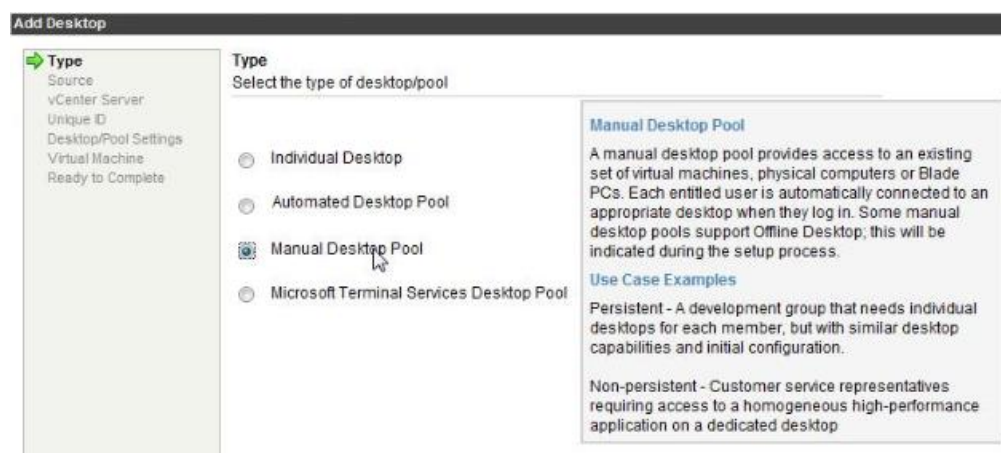
9. VMWARE VIEW MANAGER KONFIGUROIINTI

Kaikki vaadittavat komponentit on nyt vCenterin osalta asennettu ja määritetty. Seuraavaksi määritellään Connection serverille virtuaalikoneiden sijainti.

9.1 Mennään selaimella osoitteeseen 10.0.0.71 ja kirjaututaan sisään domain administrator-tunnuksilla.



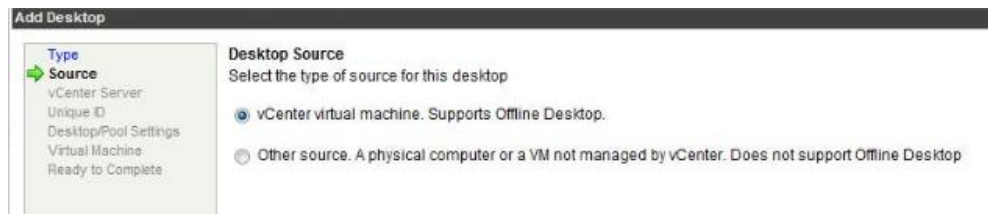
9.2 Poolin rakentaminen ja työpöytien liittäminen alkaa klikkaamalla kohtaa ”Desktops and Pools”.



9.3 Avautuvasta ikkunasta päästään määrittelemään minkälaista poolia ollaan rakentamassa. Valintoina ovat:

- Individual Desktop mahdollistaa yksittäisen työaseman tai Blade-pc:n käytön poolissa. Määritetyt käyttäjät voivat kirjautua tälle koneelle yksi kerrallaan.
- Automated Desktop Pool sisältää yhden tai useamman työpöydän, jotka ovat automaattisesti luotu sekä määritetty View Managerin toimesta. Työpöydät pohjautuvat vCenterillä olevaan virtuaalikoneiden mallitiedostoon (template). Jokainen käyttäjä yhdistetään automaattisesti sopivaan työpöytään heidän kirjautuessa järjestelmään. Automaattisessa vaihtoehdossa voidaan määrittää joko pysyvä (persistent) tai ei-pysyvä (non-persistent) työpöytien varanto. Pysyvä vaihtoesto soveltuu hyvin ympäristöihin joissa useat käyttäjät tarvitsevat samankaltaisen työpöydän, joka sisältää samat sovellukset. Väliaikaista vaihtoehtoa voidaan hyödyntää sellaisissa kohteissa, joissa työpöytiä tarvitaan ainoastaan tilapäisesti ja ne voidaan tuhota käytön jälkeen.
- Manual Desktop Pool mahdollistaa pääsyn aiemmin luotuihin virtuaalikoneisiin, fyysisiin työasemiin tai Blade-pc:siin. Kirjautuessaan järjestelmään käyttäjälle annetaan vapaa kone varannosta. Tässäkin vaihtoehdossa voidaan valita

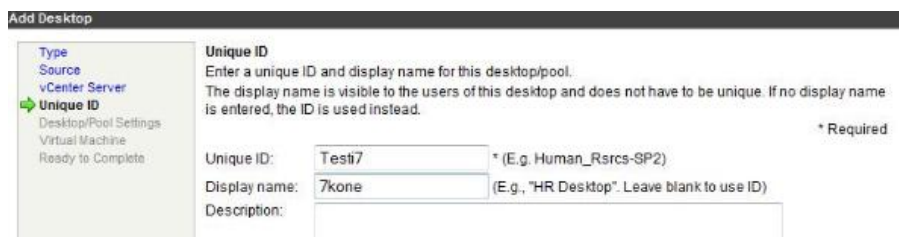
- Microsoft Terminal Services Desktop Pool valinnalla voidaan osoittaa Terminal Server tarjoamaan sessiopohjaisia istuntoja työpöytinä VMware View käyttäjille. Tässä ratkaisussa Terminaalipalvelimen istuntoja hallitaan View Serverillä kuin normaaleja työpöytiä.
- Valitsimme Manual Desktop Pool vaihtoehdon, tällöin pystyimme hyödyntämään aikaisemmin luotuja virtuaalisia työasemia.



9.4 Valitaan työpöytien lähteeksi vCenter virtual machine



9.5 Asennus näyttää mitä vCenter-palvelinta käytetään. Tässä tapauksessa vaihtoehtoja on vain yksi, koska asennettuja vCenter-palvelimia on vain yksi. Siirrytään valinnalla "next" seuraavaan vaiheeseen.



9.6 Tässä kohtaa määritetään poolille yksilöllinen ID-tunnus. Valinnaisina kenttinä ovat Display name ja Description. Syötimme Display name -kenttään tunnisteen, joka näkyy loppukäyttäjälle. Description -kentällä voidaan määrittää kuvaus poolista.

Add Desktop

Type
Source
vCenter Server
Unique ID
➔ Desktop/Pool Settings
Virtual Machine
Ready to Complete

Desktop/Pool Settings
Specify the desktop settings

General

State: Enabled

When VM is not in use: Do nothing (VM remains powered on)

Automatic logoff after disconnect: Never

Connection server restrictions: None

Allow users to reset their desktop

Display Protocol

Default display protocol: PCoIP

Allow users to override the default protocol

**Max number of monitors: 2 Only applicable for PCoIP

**Resolution of each monitor: 1600x1200 Only applicable for PCoIP

**Existing virtual machines need to be powered off and then on for the settings to take effect.

Adobe Flash

Adobe Flash quality: Medium
Lower quality results in more bandwidth savings

Adobe Flash throttling: Moderate
More aggressive throttling results in more bandwidth savings

< Back Next > Cancel

9.7 Desktop/Pool Settings kohdassa päästään määrittämään mm. työpöydän tiedonsiirtoprotokolla, flash:in laatu, näyttöjen määrä, näyttöjen resoluutio ja koneen käyttäytyminen verkko-yhteyden katketessa.

Add Desktop

Type
Source
vCenter Server
Unique ID
Desktop/Pool Settings
➔ Virtual Machine
Ready to Complete

Desktop Source Selection
Select a single virtual machine for this desktop to use

Name, Type or Path contains: Find Clear

Name	Type	Path
Win7 (32bit_ent)	Microsoft Windows 7 (32-bit)	/vSphere datacenter/vm/Win7 (32bit_ent)
Win7ENT2	Microsoft Windows 7 (32-bit)	/vSphere datacenter/vm/Win7ENT2

9.8 Nyt päästään valitsemaan työpöydät joita pooli käyttää. Valitsimme alla olevat Windows 7 Enterprise koneet, jotka teimme jo aikaisemmin.

Add Desktop

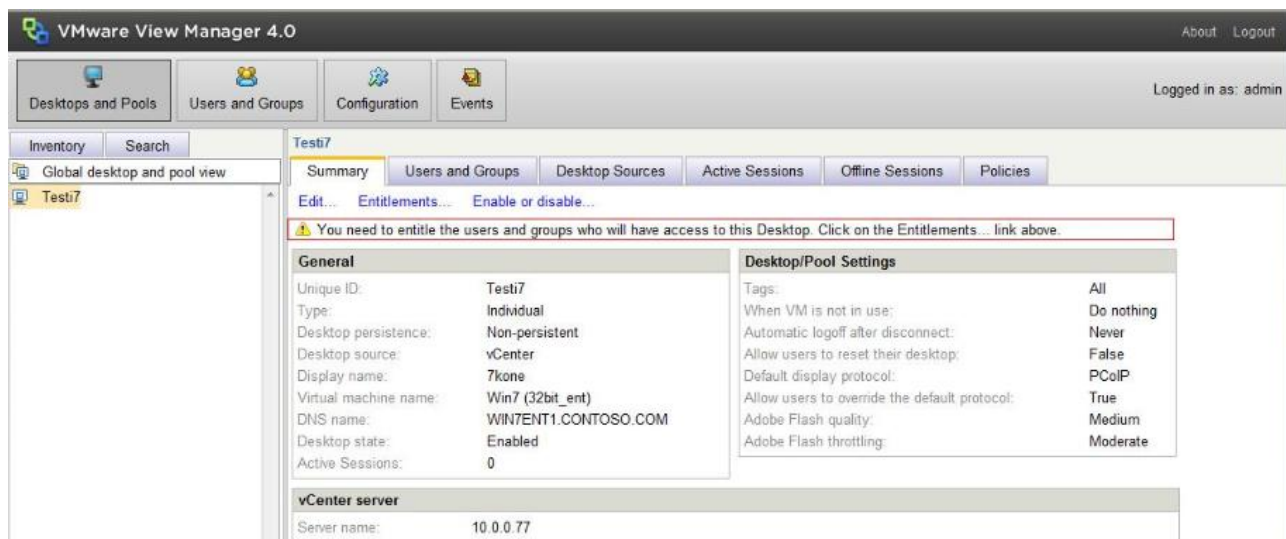
Type
Source
vCenter Server
Unique ID
Desktop/Pool Settings
Virtual Machine
➔ Ready to Complete

Ready to Complete
Review the options and click Finish

Type:	Individual Desktop
Desktop source:	vCenter virtual machine
vCenter server:	10.0.0.77
Unique ID:	Test7
Display name:	7kone
State:	Enabled
When VM is not in use:	Do nothing
Allow users to reset their desktop:	False
Connection server restrictions:	All
Automatic logoff after disconnect:	Never
Default display protocol:	PCoIP
Allow users to override the default protocol:	True
Max number of monitors:	2
Resolution of each monitor:	1600x1200
Adobe Flash quality:	Medium
Adobe Flash throttling:	Moderate
Virtual machine:	/vSphere datacenter/vm/Win7 (32bit_ent)
Description:	

9.9 Lopuksi tulee vielä yhteenveto asetuksista joita pooliin tehtiin.

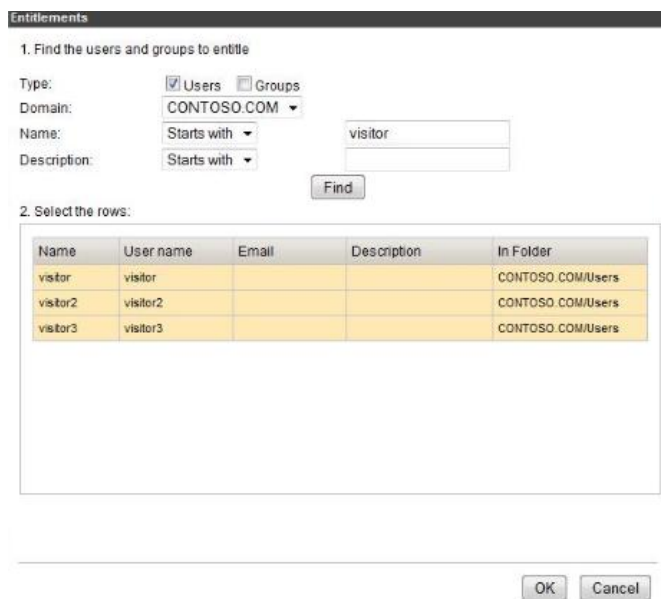
10. POOLIN KÄYTTÄJÄRYHMIEN MÄÄRITTELY



Poolille täytyy määritellä sallitut käyttäjät ja ryhmät. Valitaan Entitlements -linkki niin ponnahdusikkuna aukeaa, josta voimme lisätä halutut käyttäjät ja ryhmät.



10.1 Add -toiminnolla lisätään halutut käyttäjät tai ryhmät luodulle poolille.



10.2 Etsi ja lisää haluamasi käyttäjät tai ryhmät. Lisäsimme aikaisemmin luomamme visitor-tunnukset poolin käyttäjiksi.

Entitlements		
Entitled users and groups can use this desktop/pool		
Name	Domain	Email
CONTOSO.COM\visitor	CONTOSO.COM	
CONTOSO.COM\visitor2	CONTOSO.COM	
CONTOSO.COM\visitor3	CONTOSO.COM	
CONTOSO.COM\admin	CONTOSO.COM	

10.3 Lopuksi näet vielä yhteenvedon poolin käyttäjistä.

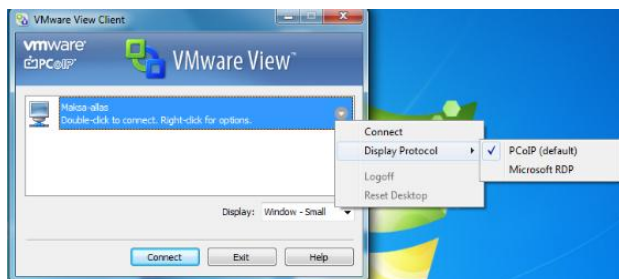


11. POOLIN TOIMIVUUDEN TESTAUS

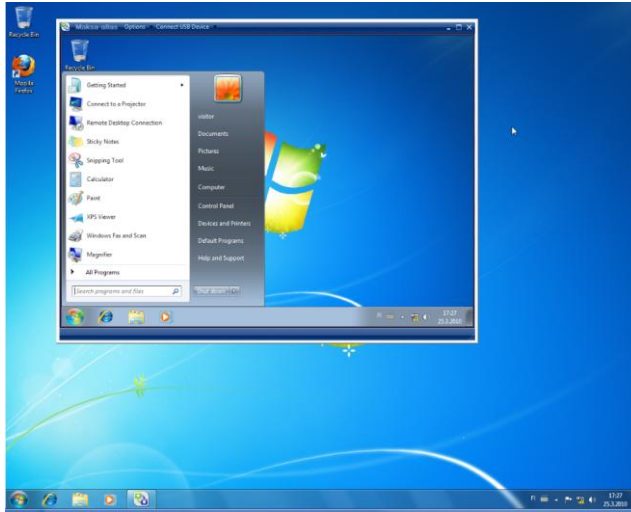
Avaa VMware View Client ja painetaa Connect jolloin client ottaa yhteyttä valittuun Connection Serveriin. Mikäli haluat käyttää kirjautumiseen samoja tunnuksia kuin isäntäjärjestelmässä, merkitse kohta "Log in as current user:".



11.1 Kirjaututaan sisään.



11.2 Tässä kohtaa käyttäjä voi valita käytetäänkö tiedonsiirtoprotokollana PCoIP vai Microsoft RDP, mikäli hänelle on annettu oikeus se valitsemiseen.



11.3 Käyttäjälle "visitor" avautui virtuaalinen työpöytä.