

KIMMO ROUSKU

Windows Server 2008

KR TT-koulutuskiertue – OULU

Kimmo Rousku

9.12.2008

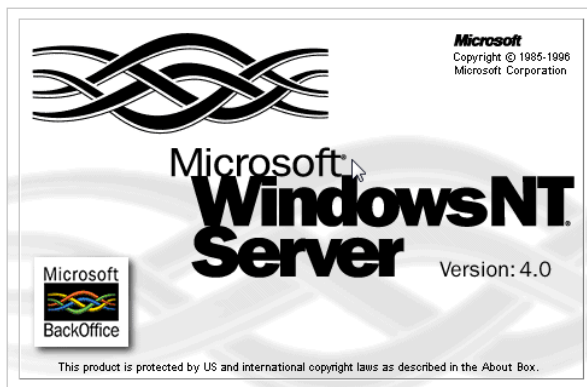


Materiaalin edelleen levittäminen on ehdottomasti kielletty.

1. Windows Server 2008 - kohti 2010-luvun palveluita

Microsoft Windows Server 2008 on yli viiden vuoden tuotekehityksen tulos. WS 2008 sisältää monia Vistassa olleita käyttöliittymä-, apu- ja järjestelmätyökaluparannuksia. Huomattavia parannuksia on tullut myös palvelinpuolelle. Voidaan hyvin todeta, että WS 2008 tarjoaa organisaatioille oivan työvälineen niin oman kuin asiakkaiden toiminnan tehostamiseksi.

Kaikki alkoi NT:stä

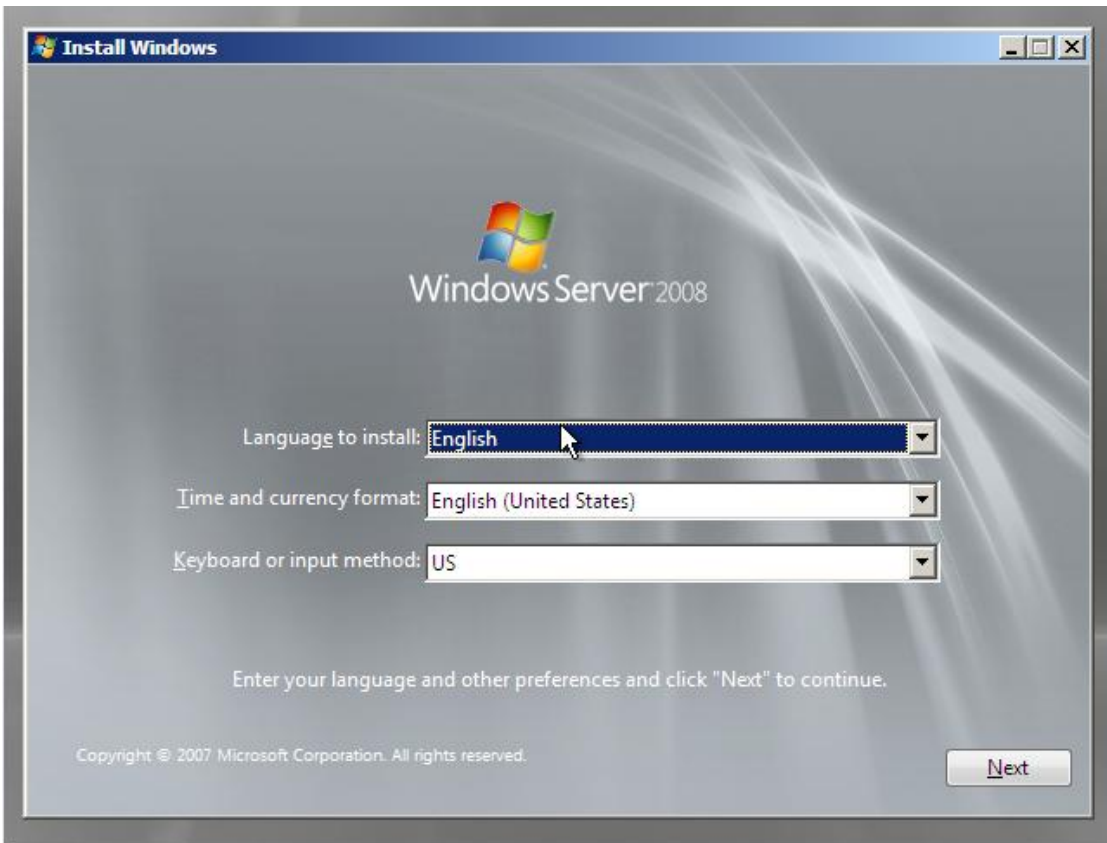


Aluksi pieni katsaus tietotekniikan historiaan. Kaikkien nyt markkinoilla olevien Windows-versioiden juuret voidaan johtaa 1980-luvun loppupuolelle ja Windows NT-projektiryhmään, jonka vetäjäksi Microsoft oli palkannut Digital Electric Corporationissa eli DECissä käyttöjärjestelmiä menestyksekkäästi kehittäneen Dave Cutlerin. NT 3.1:n merkittävimpiä, vielä tänä päivänä toimivia ominaisuuksia ovat esimerkiksi ntfs-tiedostojärjestelmä sekä Win32-api-rajapinta. Kuten oheisesta taulukosta nähdään, 90-lukua hallitsi Windows NT-teknologia, josta siirryttiin 2000-luvulla Windows 2000-versioon ja Active Directory-aikakauteen. AD-hakemistoa ja sen myötä Group Policy-ryhmäkäytäntöjä voidaan pitää merkittävimpänä 2000-luvun parannuksena.

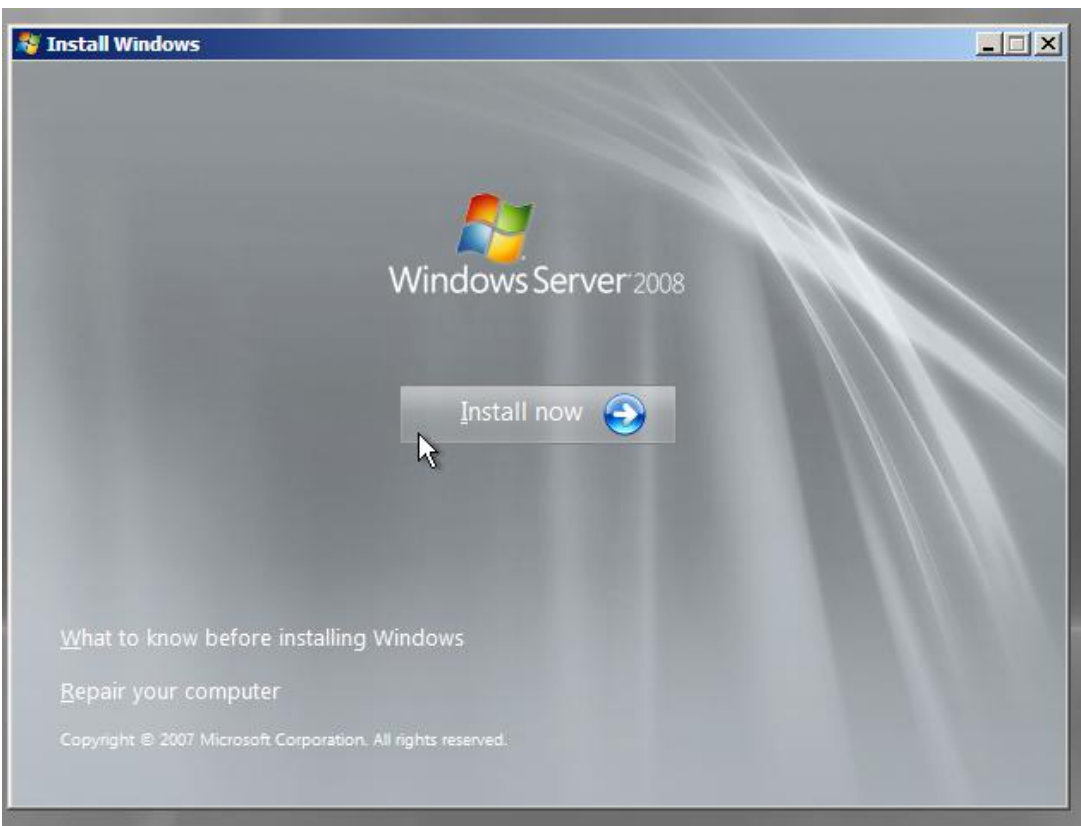
Windows-servereiden ytimien kehittyminen ja käyttöjärjestelmien julkaisuajankohdat

NT-versio	käyttöjärjestelmä	build-versio	julkaisupvm
NT 3.1	Windows NT 3.1	528	27.7.1993
NT 3.5	Windows NT 3.5	807	21.9.1994
NT 3.51	Windows NT 3.51	1057	30.5.1995
NT 4.0	Windows NT 4.0	1381	29.7.1996
NT 5.0	Windows 2000	2195	17.2.2000
NT 5.1	Windows XP	2600	25.11.2001
NT 5.2	Windows Server 2003 sekä 64-bittinen Windows XP	3790	24.4.2003
NT 6.0 Windows Vista		6000	30.1.2007
NT 6.0 Windows Vista SP1 ja Windows 2008 SP1		6001	4.2.2008
NT 6.1 Windows "Seven"		69xx	x.x.2009

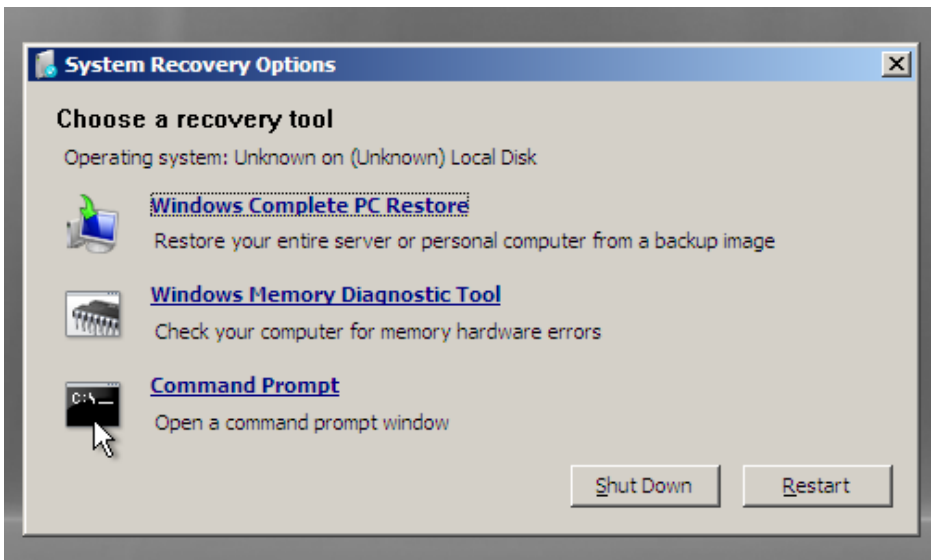
Windows NT 4.0:sta muodostui 90-luvun merkittävin Windows-palvelinkäyttöjärjestelmä, joka saattaa olla käytössä vielä satunnaisesti yksittäisissä palvelimissa yli 10 vuotta sen julkistamisen jälkeen!"



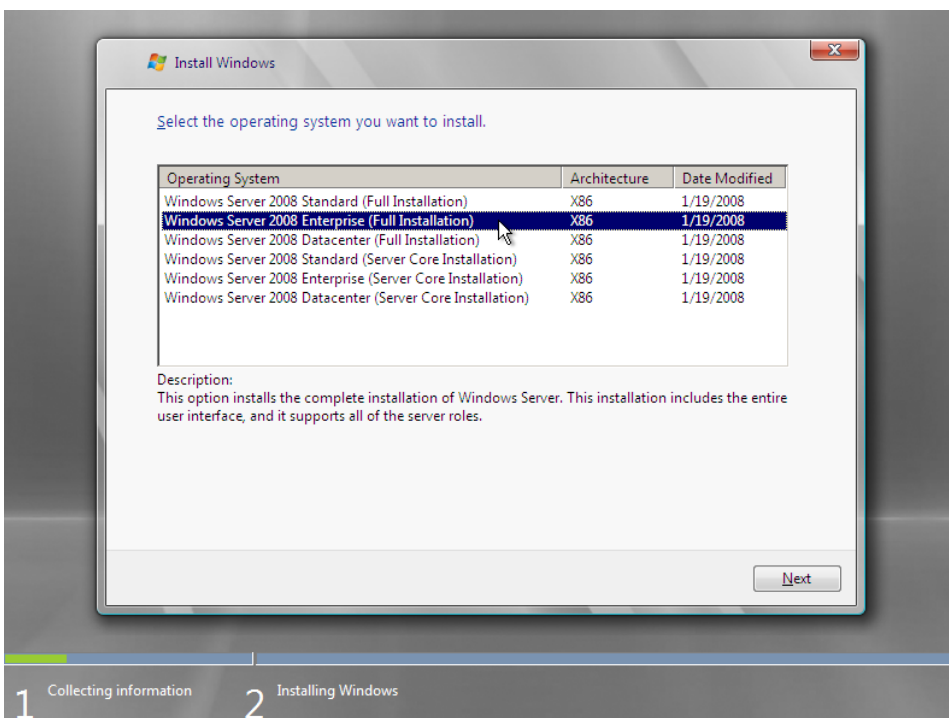
Älä valitse suomalaisia asetuksia, jos käytössä 64-bittinen versio, koska Hyper-V ei muuten toimi!



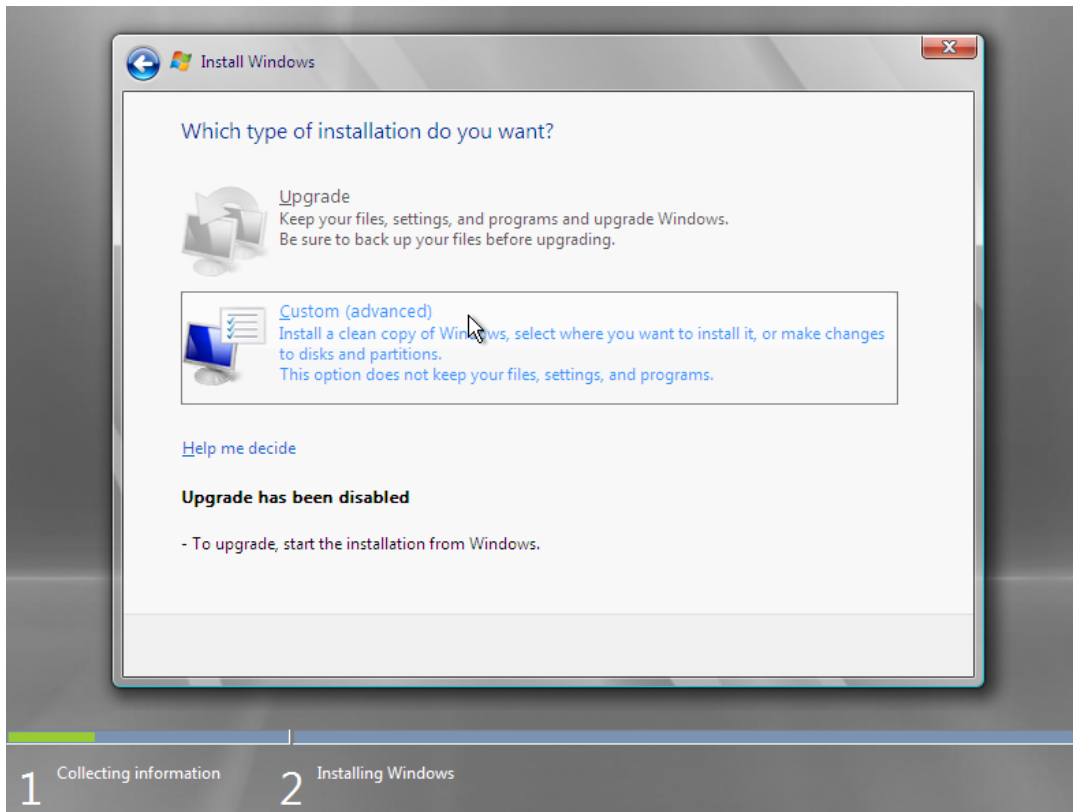
Välitse Install Now - huomaa kuten Vistassa: **Repair your computer**



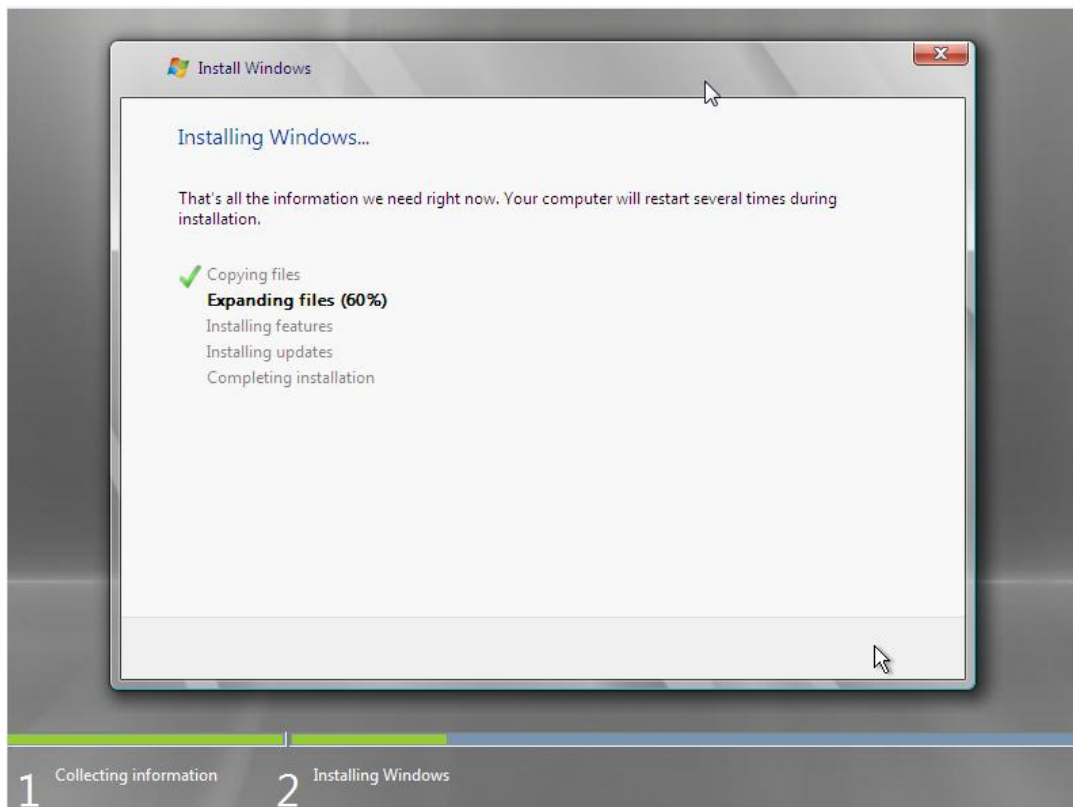
2008:n system recovery-valinnat eivät ole aivan yhtä laajat kuin Vistassa, mutta vaarallisin kohta eli Command Prompt löytyy tästäkin. Sen avulla pääset Windows-tietokoneisiin administrator + system-käyttöoikeudella tekemään **MITÄ TAHANSA**. Ainoa takuuarma keino suojautua tällaisia murto-ohjelmia vastaan on kiintolevyn salakirjoitusohjelmistot, 2008-palvelimen tapauksessa BitLocker.



Huomaa alimmaisena olevat Server Core-asennusvaihtoehdot.



Päivittäminen ei yleensä ole aktiivinen esimerkiksi uusissa palvelimissa.



Tämä vaihe kestää pisimpään...



Salasana pitää vaihtaa asennuksen yhteydessä.

2. Windows 2008:n neljä pääversiota

27.2. virallisesti julkistettu Windows Server 2008 -tuotelinja koostuu neljästä palvelinversiosta, jotka ovat Standard, Enterprise, Datacenter ja Windows Web Server 2008. Näiden ohella on erikseen Standard-versio Itanium-suorittimella. Lisäksi kolmesta ensin mainitusta voidaan hankkia versio ilman Hyper-V-nimellä kutsuttua virtualisointitekniikkaa. Tällainen versio on suositeltava silloin, kun ollaan varmoja siitä, ettei kyseisessä palvelimessa ole tarvetta ajaa virtualisoituja käyttöjärjestelmiä. Tällöin palvelimeen ei asennu lainkaan Hyper-V:n tarvitsemaa arkkitehtuurikerrosta.

Jos nyky-ympäristössä on käytössä 2003 Standard-versio, organisaatio tulee todennäköisesti tarvitsemaan samaa versiota myös tulevissa 2008-palvelimissa. Eräs mahdollinen syy on muistintarve. Mikäli 32-bittiseen palvelinversioon tarvitaan enemmän kuin 4 Gt muistia ja palvelimella käytettävät sovellukset tukevat PAE-laajennusta, 2008 Enterprise versio tukee 32-bittisenä 64 Gt keskusmuistia. Luonnollisesti suositeltavampaa olisi käyttää 64-bittistä versiota, jolloin Standard-versiossakin tuetaan 32 Gt-keskusmuistia.

View basic information about your computer

Windows edition

Windows Server® Enterprise

Copyright © 2007 Microsoft Corporation. All rights reserved.

Service Pack 1



System

Processor:	Intel(R) Core(TM)2 Duo CPU T7700 @ 2.40GHz
Memory (RAM):	1.00 GB
System type:	32-bit Operating System

Napsauttamalla Win+Pause saat esille ohjauspaneelin System-kohdan, josta löydät palvelimen keskeiset tiedot kuten version, 32/64-bittisyyden sekä muita keskeisiä laitetietoja.

Vanhan 200x-palvelimen voi päivittää vastaavaksi 2008-palvelinversioksi tai 2003 Standard-version tapauksessa myös 2008 Enterprise-versioksi. On huomattava, että mitään versiota ei voi päivittää uudeksi Server Core-versioksi. Vastaavasti Server Core-versiota ei voi päivittää graafisella liittymällä varustetuksi versioksi.

3. Server Core - paluu komentokehoitteeseen

Eräs arkkitehtuurisesti merkittävä WS 2008 -toiminnallisuuteen liittyvä muutos kulkee nimellä Server Core. SC tarkoittaa WS 2008 -asennusta, joka asennetaan ilman GUI:ta eli graafista käyttöliittymää (Graphical User Interface). Tällöin asentamatta jää esimerkiksi perinteinen työpöytä, Internet Explorer-selain, muut ikkunointijärjestelmän toiminnot sekä osa palveluista.

Server Core ei sovi aivan kaikenlaiseen käyttöön. Se tukee ennen kaikkea seuraavia infra-tyyppisiä rooleja (roles):

- Active Directory Domain Services (AD DS)
- Active Directory Lightweight Directory Services (AD LDS)
- DHCP Server
- DNS Server
- File Services
- Print Services
- Streaming Media Services
- Internet Information Services (IIS)
- Windows Virtualization

Sen sijaan esimerkiksi päätepalvelut tarjoava Terminal Services-palvelua ei voi ajaa Server Core -palvelimella, vaan se edellyttää taustalla perinteistä graafista käyttöliittymää ja Dot Net Framework -rajapintaa. Mm. tämän takia SC:ssä ei voida ajaa IIS:ssä Asp.net-sovelluksia. Palvelinroolien ohella Server Core tukee seuraavia 2008:n ominaisuuksia (features):

- Microsoft Failover Cluster
- Network Load Balancing
- Subsystem for UNIX-based Applications
- Windows Backup
- Multipath I/O
- Removable Storage Management
- Windows Bitlocker Drive Encryption
- Simple Network Management Protocol (SNMP)
- Windows Internet Naming Service (WINS)
- Telnet client
- Quality of Service (QoS)

Mitä etuja Server Core tarjoaa verrattuna graafisella liittymällä varustettuun perinteisempään WS 2008-asennukseen?

- Tietoturvallisuus
- Korkea käytettävyys
- Helpompi ylläpidettävyys
- Pienempi levytilan kulutus

SC:n voi olettaa toimivan tietoturvallisemmin, koska käyttöjärjestelmän ydintä ja suoritettavan koodin määrää voidaan pienentää ja tällöin mahdollisesti ongelmia sisältävän ohjelmakoodin määrä rajoittuu melkoisesti.

SC sisältää vähemmän päivitettäviä ja vika-alttiita ohjelmistokomponentteja, jolloin tarve kuukausittaisille tietoturvapäivityksille ja sitä kautta syntyville käyttökatkoille tulee olemaan pienempi, millä voidaan parantaa järjestelmien käytettävyyteen liittyviä HA-lukemia (High Availability). Palvelinkäytössä GUI:n ei voi juurikaan sanoa hidastaneen itse palvelimen toimintaa, mutta GUI:n ja muiden palveluiden tiputtamisella pois voidaan säästää suorituskyvyssä muutama prosentti, näin ainakin teoriassa.

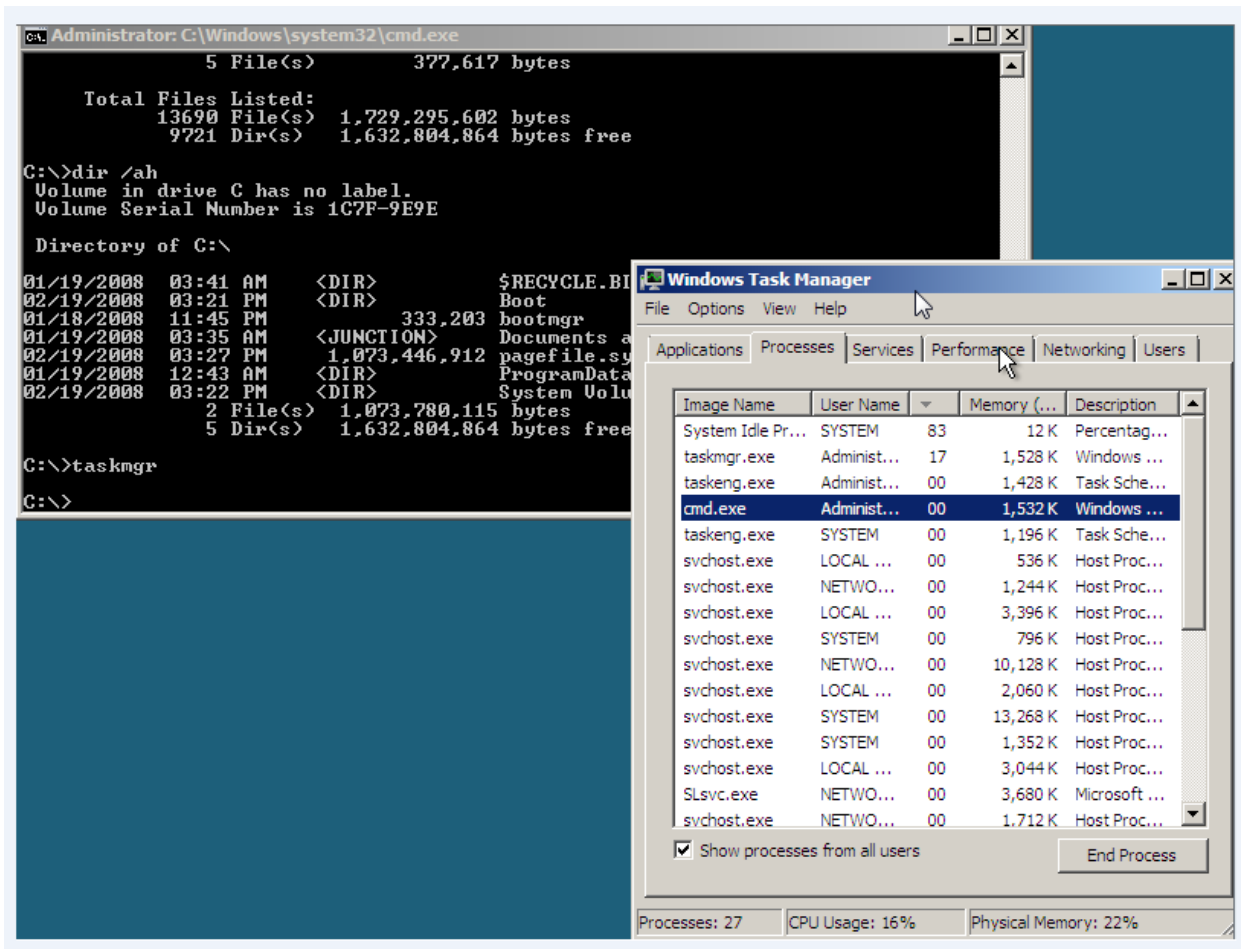
Puhdas SC-asennus koostuu 13 690 tiedostosta, jotka vievät levytilaa vain 1,7 Gt, johon on laskettu mukaan 1 Gt-kokoinen virtuaalimuistitiedosto. Käytännössä SC-ydin vie reilut 600 Mt. Vastaavasti GUI:lla varustettu Enterprise-asennus, joka sisältää DC-roolin, koostuu 38 357 tiedostosta, jotka vievät levytilaa 6,3 Gt sisältäen virtuaalimuistitiedoston.

Ylläpidon kannalta SC on hieman kaksijakoinen. Koska käytettävissä olevia rooleja on vähemmän, SC-palvelimen ylläpito on helpompaa. Toisaalta hallinta voi olla hankalampaa, koska se tapahtuu paikallisesti komentokehotetason komennoilla ja PowerShell-skripteillä. PowerShell-skriptauksen osaaminen ei ole edellytys, mutta siitä on etua. Onneksi valtaosa hallinnoinnista voidaan suorittaa etänä toiselta 2008-palvelimelta tai sellaiselta Vista-tietokoneelta, johon on asennettu uudet Remote Server Administration Tool-hallintavälineet (RSAT).

Olen aina todennut, että DOS ei kuole koskaan, se vain muuttaa olotilaa. Nyt Server Coren yhteydessä voidaan sanoa, että "DOS iskee takaisin" ja tässä tapauksessa SC:n komentokehotetason muodossa, kun palvelinhallinnointi ei edellytä ylimääräisiä graafisia työkaluja. Valtaosa nykyisistä skriptikieltä puhumattomista ylläpitäjistä tarvitsee SC:n hallintaan samoja, mutta erilliseltä palvelimelta käytettäviä, graafisia työvälineitä joita käytetään muiden GUI:lla varustettujen WS 2008 –palvelimien pyörittämisessä.

Valitettavasti Remote Desktop-etätyöpöytähallinnastakaan ei ole apua; sillä pääsee SC-palvelimeen kiinni, mutta edelleen vain sen komentokehotetasaan. Vinkki: Onneksi AIVAN kaikki ei toimi cmd-tasossa; voit kokeilla esimerkiksi komentoja taskmgr (tehtävienhallinta) ja notepad (muistio).

Vinkki: SC-asennus ei tue niin laajaa määrää rooleja kuin täysiasennus, mutta valtaosalle organisaatioista Standard-versio riittää mainiosti. Tosin kannattaa huomata, että vikasietoisemman ratkaisun saa rakennettua klusteroimalla SC Enterprise/Datacenter -versioissa.



Valtaosa Server Core-työskentelystä tulee tehdä cmd-tasossa, mutta muutama yksittäinen sovellus voidaan ajaa myös graafisesti, kuten kuvassa näkyvä Tehtävienhallinta (Task Manager).

4. Kevyet laitevaatimukset nykyraudalle

Palvelinraudan puolella voi todeta, että mitä enemmän muistia, prosessoreita ja ytimiä on käytettävissä, sitä suuremman hyödyn WS 2008:sta saa. Vaikka WS 2008 asentuu tarvittaessa vanhaan laitteistoon, jossa on 1 Ghz suoritin ja 512 Mt ram-muistia, ei sitä sellaiseen kannata asentaa. Koska laitteiston hinta on laskenut merkittävästi parin viimeisen vuoden aikana, nyt kannattaa investoida uuteen palvelinteknologiaan.

Arkkitehtuurisesti merkittävin kysymys on, halutaanko jatkaa stand-alone-palvelimien kanssa, loikata keskitetympään virtuaalipalvelinympäristöön vai kenties ottaa käyttöön blade-kehikkopalvelinteknologiaa. Yhtä oikeaa ratkaisua tähän ei ole. Vaikka käytössä olisi vain muutama yksittäinen fyysinen palvelin, virtuaalipalvelimia voi WS 2008-käyttöjärjestelmässä ottaa käyttöön vaivattomasti, kunhan palvelimen tehot riittävät. Suosittelen tämän takia hankkimaan 4 Gt muistilla ja kahdella suorittimella varustettuja palvelinlaitteita, olipa käyttötarkoitus melkein mikä tahansa. Jos asennat 64-bittisen version, 2 Gt-muistipiirejä saa edullisesti, jolloin muistia kannattaa hankkia 8 Gt. Prosessorissa kahden ytimen sijaan neljästä ytimestä on hyötyä etenkin virtualisoinnissa tai muuten laskentatehoa edeltävissä palvelimissa, joten pitkän elinkaaren kannalta neljä ydintä on järkevä investointi.

Levyjärjestelmien puolella vahva suuntaus SAN-levyjärjestelmiin jatkuu. Esimerkiksi blade-palvelimissa ei ole levyjä lainkaan ja palvelin buutataan suoraan levyjärjestelmästä. Pienemmissä laitteistoympäristöissä ja yksittäispalvelimissa perinteinen useammasta levystä koostuva paikallinen levyjärjestelmä on edelleen toimiva ja suositeltava yhdistelmä. Mitä useammalle kiintolevyille saat tiedostot jaettua, sitä tehokkaampi on levyjärjestelmän suorituskyky. Laitteistoinvestoinnin osalta kannattaa ajatella, että uudella laitteistolla tullaan toimeen ainakin WS 2008 -aikakausi, siis vähintään seuraavat 3 vuotta.

5. NAP suojaa verkkoasi haittaohjelmilta

Kannettavat tietokoneet aiheuttavat monessa yrityksessä unettomia öitä ja harmaita hiuksia. Niiden varustaminen ”rautaa rajalle” -tyyliin kaikilla keskeisillä tietoturvaherkuilla ei valitettavasti takaa kannettavien tietokoneiden puhtautta. Tietoturva on uhattuna aina, kun kannettava tietokone palaa takaisin organisaation lähiverkkoon joko toimitiloissa tai yhä useammin erilaisten langattomien tietoliikenneyhteyksien kautta.

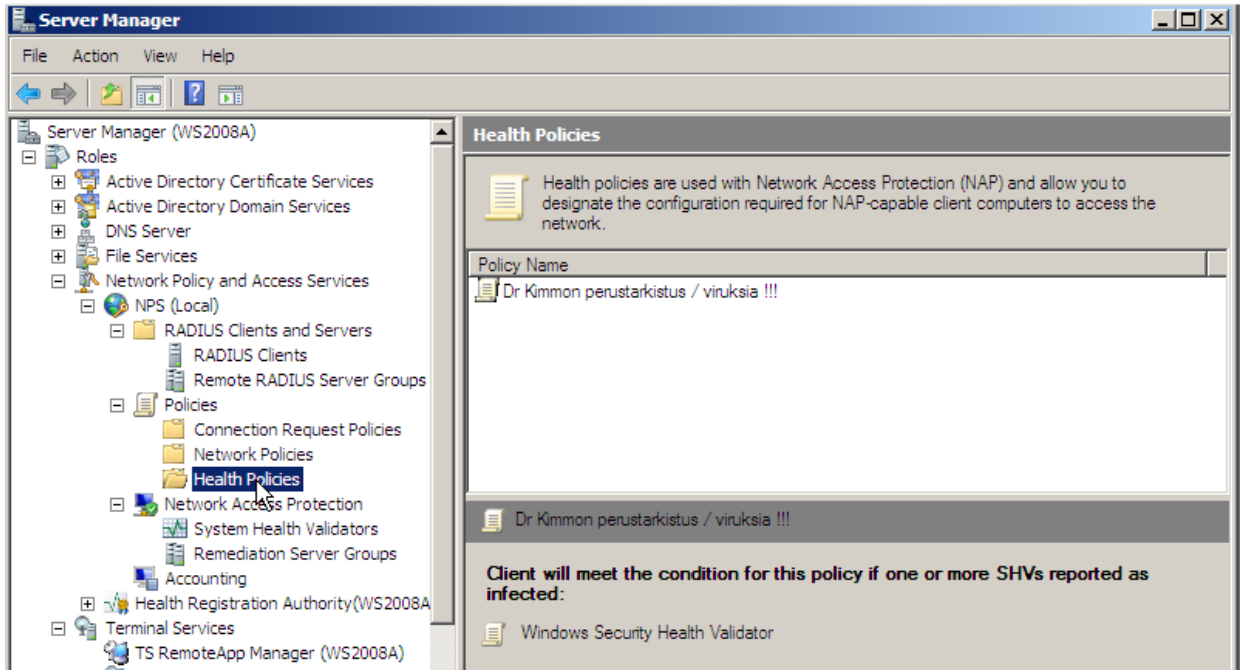
Tietoturvaohjelmat eivät toimi riittävän luotettavasti. Tällainen epävakaas aiheuttaa ikäviä yllätyksiä mm. erilaisten haittaohjelmien muodossa. Nyt näitä ongelmia vastaan taistellaan NAP-palvelulla eli Network Access Protection-tekniikalla. NAPia voisi verrata tilanteeseen, jossa työpaikkasi ulko-ovella jokainen saapuva työntekijä joutuisi terveydenhoitajan tarkastukseen. Ensin katsottaisiin kurkkuun, sitten mitattaisiin kuume ja kolesterolit, ja lopuksi laskettaisiin painoindeksi. Jos tulokset näyttäisivät huonoilta, töihin tulija voitaisiin ohjata edelleen lääkärintarkastukseen ja sieltä tarvittaessa tarkempiin laboratoriotutkimuksiin. Mikäli vain pulssi ja verenpaine olisivat lievästi koholla, työntekijä pääsisi hetkeksi lepohuoneeseen huilimaan, josta hänet sitten päästettäisiin työhuoneeseen työskentelemään.

NAP tekee tämän saman organisaation lähiverkkoon yrittäville tietokoneille, olipa kyseessä kannettava tietokone tai pöytäkone, joka yrittää päästä verkkoon omasta lähiverkosta tai erilaisten etätyöskentely-yhteyksien kautta. Jos tietokone ei läpäise yrityksen NAP-tietoturvapoliittikkaa, sitä ei päästetä liikennöimään lähiverkossa, vaan se ohjataan esimerkiksi eristettyyn karanteeniverkkoon, jossa siitä voidaan yrittää korjata ne viat, jotka estivät pääsyn lähiverkkoon. Esimerkiksi jos tietokoneessa ei ole ajan tasalla olevaa antivirusohjelmistoa tai palomuuuri ei ole ollut toiminnassa, voidaan nämä yrittää pistää kuntoon. Tämän jälkeen tietokoneelle voidaan tehdä uusi terveystarkistus. Jos tietokone läpäisee sen, kone on tervetullut lähiverkkoon. Muussa tapauksessa se tarvitsee kenties leikkauksen tai jopa elinsiirtoon verrattavaa manuaalista korjausta tullakseen terveeksi. Tätä korjausprosessia voidaan helpottaa erillisellä System Center-tuoteperheen Configuration Management-ohjelmistolla.

NAP-client on valmiiksi asennettuna Vista-työasemassa ja se saadaan myös Windows XP-käyttöjärjestelmiin esimerkiksi XP SP3-huoltokorjauksen myötä tai erillisenä client-ohjelmistona. Huomion arvoista on, että NAPin käyttöönotto ei edellytä uuden Active Directoryn käyttöönottoa, vaan pelkkä NAP 2008-palvelin riittää.

Teknisesti NAP on toteutettu siten, että 2008 DHCP-palvelin vastaa lähiverkossa tapahtuvasta ip-osoitteiden automaattisesta jakelusta. Kun työasema saa DHCP-palvelimen jakaman ip-osoitteeseen, se ottaa samalla yhteyden organisaation NAP-palvelimeen, joka suorittaa työasemaan politiikan mukaisen tarkastuksen. NAP voidaan ottaa käyttöön edellä mainitun DHCP:n ohella esimerkiksi seuraavien teknologioiden yhteydessä:

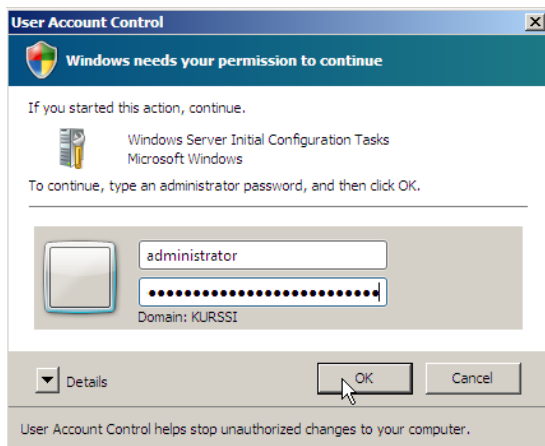
- Internet Protocol security (IPsec) -yhteydet
- IEEE 802.1X-tunnistamisessa, esimerkiksi WLANia käytettäessä
- VPN-yhteydet
- Terminal Server (TS) -yhdyskäytäväyhteydet



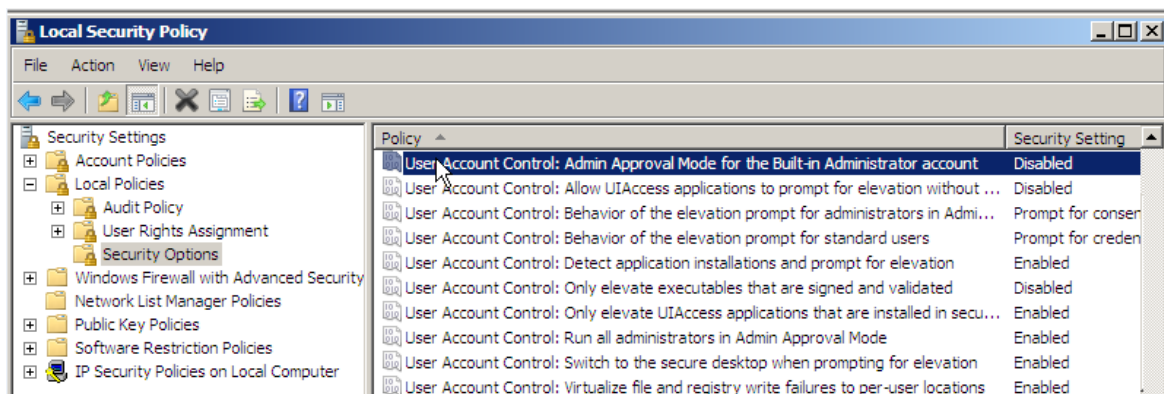
Server Manager-hallinnassa näkyvät keskeiset Network Policy and Access Services-hallintavälineen työkalut. NAPin käyttöönotto edellyttää useiden toimintaprosessien ennakkosuunnittelua.

6. Tietoturvallisuus on kaiken a ja o

Edellä kuvatun NAPin ohella WS 2008 sisältää lukuisia yksittäisiä tietoturvaparannuksia. Oletuksena palvelimessa ei ole päällä käyttäjätilien valvontaa eli UAC (User Account Control) -toimintoa, joka edellyttää jokaisen järjestelmänvalvojaoikeudella tehtävän toiminnon hyväksymisen. UAC on mahdollista ottaa käyttöön Start | Secu-komennolla käynnistämällä Local Security Policy ja valitsemalla Local Policies | Security Options -kohdassa valitsevia User Account Control-asetuksia.



Oletuksena käyttäjätilien valvonta eli UAC (User Account Control) on pois käytöstä. Sen toimintaa voidaan säätää Security Settings | Local Policies | Security Options-valinnasta löytyvillä uusilla User Account Control-asetuksilla.



Kun UAC on aktivoitu, voidaan jokainen järjestelmänvalvojaoikeutta edellyttävä toimenpide vahvistaa joko kuittauksella (Continue) tai kuten kuvan tapauksessa, tunnistautumisella.

Erityisesti organisaation sivutoimipisteissä sijaitsevien palvelimien suojaksi on kaksi uutta toiminnallisuutta, RODC ja BitLocker-salakirjoitus. RODC eli Read Only Domain Controller toimii DC-palvelimena, joka ei säilytä AD-tietokantaa palvelimella, vaan edelleenohjaa kaikki kyselyt organisaation varsinaisella toimipaikalla sijaitsevalle DC-palvelimelle.

RODC voidaan asettaa toimimaan siten, että se säilyttää välimuistissa muiden paitsi keskeisten järjestelmänvalvojatasoisten käyttäjien salasanat. Tämä nopeuttaa käyttäjien verkkokirjautumista säilyttäen kuitenkin tietoturvallisuuden siltä varalta, että joku varastaa kyseisen palvelimen. Vastaavalla tavalla sivutoimipisteen RODC-palvelin voi toimia paikallisena DNS-palvelimena, joka nopeuttaa sivutoimipisteen dns-kyselyitä. Paikallinen RODC/DNS-palvelin ei tue dynaamisia päivityksiä, jotka ohjataan päätoimipaikan dns-palvelimelle.

Mielenkiintoinen ominaisuus on mahdollisuus antaa jollekin paikalliselle käyttäjälle RODC-palvelimen järjestelmänvalvojaoikeus, joka toimii vain sivutoimipisteen RODC-palvelimella, ei muilla palvelimilla. Täten järjestelmänvalvojaoikeutta voidaan delegoida paikalliselle tukihenkilölle vaarantamatta koko toimialueen tietoturvasuutta.

BitLocker-salausta on kehitetty Vistaan verrattuna siten, että se mahdollistaa C:-aseman ohella myös kiintolevyn muiden levyosien salakirjoituksen. Tosin saman toiminnallisuuden saa Vistaan SP1-päivityksessä. Jos palvelimen kiintolevyosiot salakirjoitetaan BitLockerilla, mahdollinen varas ei pysty anastamaan levyillä olevia tietoja. Tässä kohdassa eteen tulee sama ongelma kuin Vistassa: missä säilytetään salauksen edellyttämää varmennetta? Tietoturvallinen ratkaisu on käyttää TPM-turvapiirillä varustettua palvelinta, jolloin suojaus tapahtuu läpinäkyvästi eikä edellytä avaimen tallentamista usb-muistille. TPM-turvapiirin hallintaa varten löytyy oma hallintaväline tpm.msc-nimellä.



Ennen kuin BitLocker-salaus voidaan ottaa käyttöön, pitää palvelimelta löytyä tätä varten vähintään 1,5 Gt levyosio, jota käytetään palvelimen käynnistyessä sekä TPM-turvapiiri. TPM-vaatimus voidaan ohittaa käyttämällä esimerkiksi usb-muistia salaustietojen tallentamiseen.

WS 2008 sisältää oletuksena kaksisuuntaisen palomuurin, joka on oletuksena käytössä! Tämä saattaa aiheuttaa ongelmia sovelluspalvelinkäytössä. Ominaisuutta kannattaa testata huolella omassa testiympäristössä käytössä olevilla palvelinsovelluksilla.

Koska Vistan ja WS 2008:n ydinkoodi on identtinen, sisältää WS 2008 kaikki keskeiset palveluiden toiminnan tiukentamiseen liittyvät parannukset. Palveluiden toimintaa on rajattu siten, että niiden ei sallita käyttävän sellaisia toimintoja, joihin niillä ei ole tarvetta. Käytännössä jokaiselle palvelulle on laadittu oma profiili, jonka mukaisesti sille on annettu oikeuksia. Esimerkiksi harva palvelu tarvitsee tcp/ip-yhteyttä, joten sitä ei sallita sellaisille palveluille, jotka eivät sitä tarvitse. Palveluita ei ajeta automaattisesti system-oikeuksilla, vaan palveluiden toiminnasta vastaa useampi eritasoinen sisäänrakennettu tili. Palomuri on nyt myös linkitetty palveluiden toimintaan tuoden verkkoa tarvitseville palveluille lisäsuojan.

Päivityksistä vastaava Windows Update-toiminto on vihdoin irrotettu Internet Explorer-selaimesta ja toimii erillisenä apuohjelmana. Kuten Vistan yhteydessä, suosittelen palvelimen tietoturvapäivitysten automatisoimista joko ilmaisella WSUS-ohjelmistolla tai käyttäen System Center-järjestelmänvalvonta tuoteperheen tuotteita.

2003-palvelimesta tuttu Security Wizard-ohjelma on päivitetty sisältämään 2008:n uudet ominaisuudet. Ohjelmalla voit luoda tietoturvapoliitikan yhdelle 2008-palvelimelle ja ajaa sen jälkeen tekemäsi politiikan suoraan muille vastaavanlaisille 2008-palvelimille.

7. IIS 7.0 - lisää modulaarisuutta

IIS-web-palvelinohjelmiston versio 7 sisältää perinteisten tietoturvapäivitysten lisäksi kauan kaivatun integroidun PHP-tuen ja se lisää modulaarista hallittavuutta. IIS-palveluun asentuu vain ne komponentit, joita siinä tarvitaan. Jos esimerkiksi et tarvitse basic-tason tunnistusta, voidaan se poistaa käytöstä. Tietoturvan ohella tämä parantaa suorituskykyä.

IISiä on kehitetty siihen suuntaan, että yhdellä palvelimella voidaan konsolidoida entistä useampia www-sivustoja yhteen palvelimeen (jopa 2 000-4 000-sivustoa). Sivustojen ylläpitäjien ei tarvitse toimia palvelimen järjestelmänvalvojina, vaan heille voidaan delegoida myös admin-hallintaoikeuksia. Hallinta onnistuu mmc-hallintavälineen ohella myös selaimella Web admin-työkaluilla. Asetuksia voidaan hallita myös suoraan xml-tiedostoilla, jolloin sivuston siirtäminen palvelimesta toiseen on vaivatonta.

IIS:n toimintaa voidaan ohjata WMI:n avulla. Tämä, sekä uudet api-rajapintakutsut mahdollistavat aikaisempaa helpomman sovelluskehityksen, joten IIS 7:n myötä markkinoille tulee enemmän kolmansien osapuolien apuohjelmia.

Web Server -versio on selvä vastaisku edullisille Linux/Apache -ratkaisuille, ja on mielenkiintoista nähdä, mihin suuntaan markkinaosuudet kääntyvät vuoden 2008 aikana kilpailuilla web-palvelinmarkkinoilla.

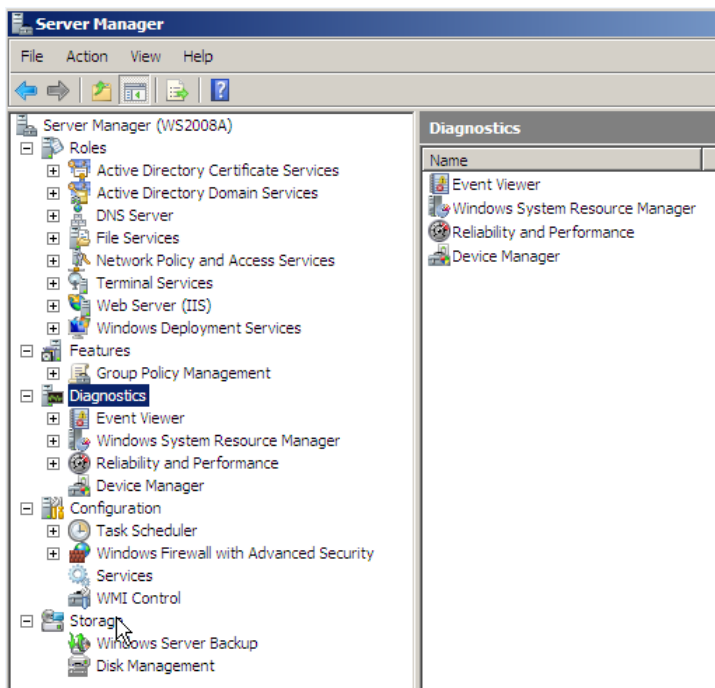


IIS 7.0 on uudistunut ominaisuuksien osalta myös visuaalisesti hallintavälineen osalta.

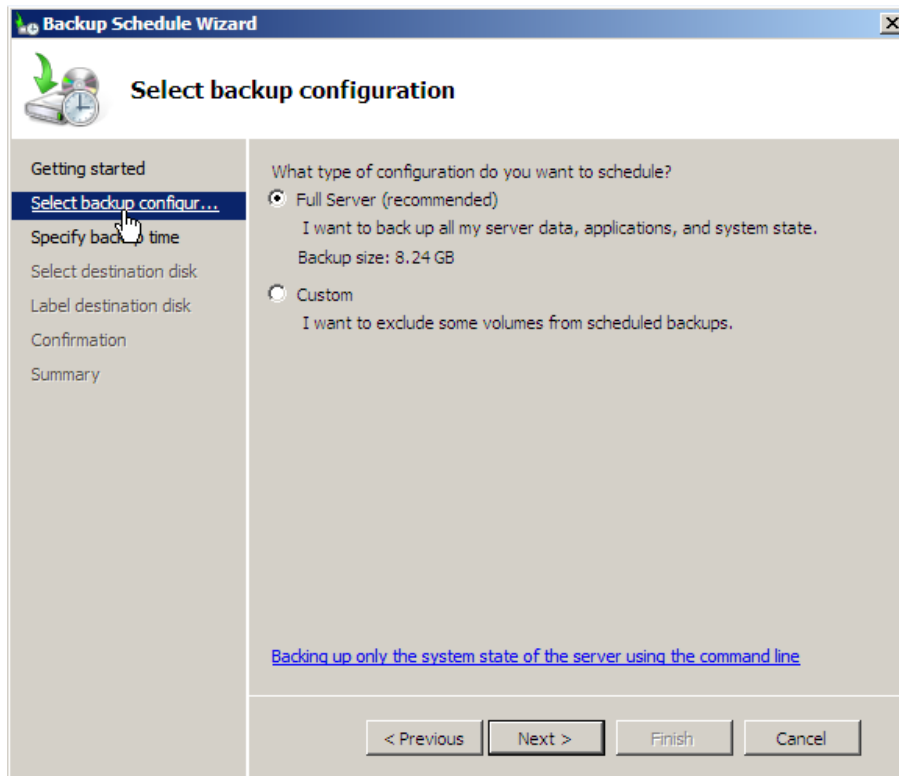
8. Server Manager yhdistää hallintavälineet

Koska WS 2008:ssa on paljon uusia palvelinrooleja (roles) ja toiminnallisuuksia (features), on näiden hallinta keskitetty uuteen Server Manager -ohjelmaan. Tämä helpottaa erityisesti satunnaisen ylläpitäjän työskentelyä, jonka ei tarvitse miettiä ja ihmetellä millä hallintavälineellä jokin toiminto saadaan tehtyä, koska lähes kaikki tarvittava löytyy yhden hallintaohjelman alaisuudesta. Edellisten ohella hallintaväline sisältää työvälineet vikaselvitykseen (Diagnostics), asetuksiin (Configuration) sekä tallennusjärjestelmiin (Storage). Storagen yhteydestä löydät myös kokonaan uudistuneen varmistusohjelmiston, jota voidaan käyttää myös cmd-tasolla wadmin-komennolla. Ohjelmisto pitää lisätä erikseen käyttöön uutena toiminnallisuutena (feature).

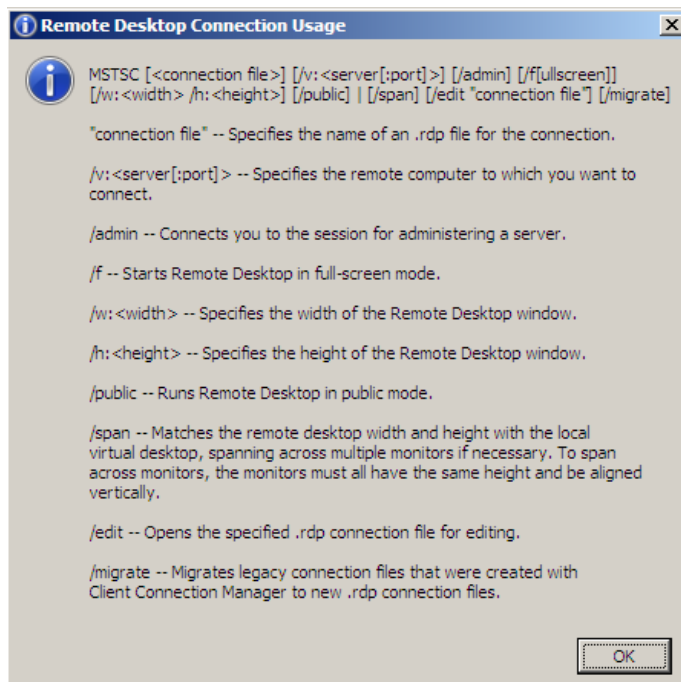
Vinkki: Kuten aikaisemminkin, palvelin voidaan ottaa etähallintaan RDP-etätyöpöytäohjelmiston avulla. On hyvä muistaa, että WS 2008:n ytimen suojausta on muutettu siten, että mstsc-etätyöpöytäohjelman /console -valitsin ei enää toimi, ja sen on korvannut /admin-valitsin. Tämä sen takia, että konsoli-istunto ei saa enää toimia ytimen 0-tasossa, vaan se on siirretty tietoturvalisemmälle ulommalle tasolle. 2003-palvelimella tarvitaan tätä 0-tasoa tiettyjen sovellusten asennusta varten, mutta nyt se on korvattu /admin-valitsimella, joka kytkee etätyöpöytäistunnon sen hetkiseen konsoli-istuntoon. Palvelimella avoimena olevat TS-istunnot voi tarkistaa qwinsta-komennolla.



Hallintavälineet on konsolidoitu pääosin yhden ainoan eli Server Manager-sovelluksen alaisuuteen. Käy läpi huolella kaikki roolit ja etenkin reilut 30 toimintoa, joiden varaan WS 2008:n toiminnallisuuden rakennat!



Vanha, legendaarinen ntbacup on saanut seuraajan. Velholla toteutetun varmistuksen avulla pyritään helppokäyttöisyyteen. Käytettävissä on myös cmd-tasolla toimiva wbadm-in-komento.



Etätyöpöytäyhteys eli mstsc-ohjelma sisältää uusia valitsimia, joita tärkeimpänä /admin-valitsin.

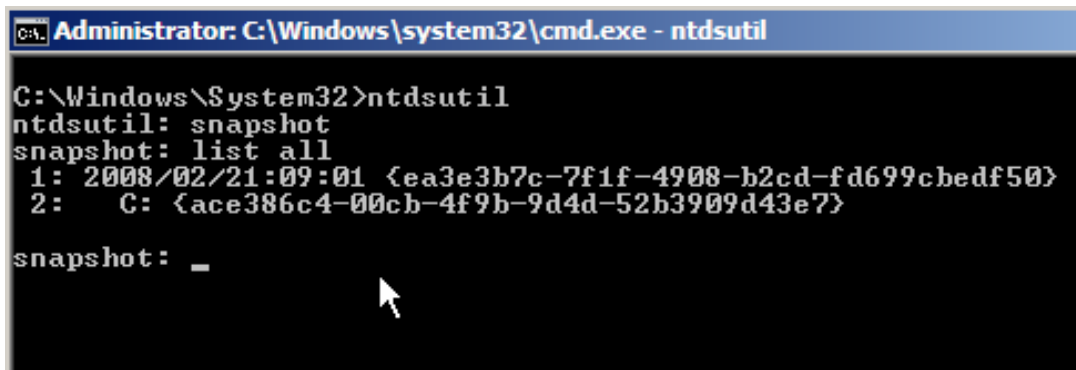
Active Directory - viisi erilaista roolia

AD:n toimintaa on muutettu nimeämällä käytössä olevat roolit uudelleen sekä tuomalla näihin uusia toiminnallisuuksia. Uudet nimet ja roolit ovat:

- Active Directory Domain Services (AD DS)
- Active Directory Federation Services (AD FS)
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Rights Management Services (AD RMS).
- Active Directory Certificate Services (AD CS)

Käsittelen erikseen ryhmäkäytäntöihin liittyviä muutoksia. AD:n ylläpidon kannalta merkittävä parannus liittyy AD:n tietokantaan. Edeltävissä 2000/2003 AD-toteutuksissa kaikki AD:n syväiset huolto- ja korjaustoimet edellyttivät DC-palvelimen käynnistämistä erilliseen viankorjaustilaan (Directory Services Restore Mode). WS 2008 mahdollistaa tietokannan ajamisen alas, jonka jälkeen huoltotoimenpiteet voidaan tehdä ilman palvelimen uudelleenkäynnistämistä.

Uusi AD:n luotettavuutta kasvattava toiminto on snapshot-ominaisuus. Voit ottaa ntdsutil-komennon snapshot-valitsimella tilannekuvan AD-hakemistostasi. Mahdollisessa ongelmatilanteessa sen palauttaminen takaisin järjestelmään on helpompaa. Suosittelen erittäin lämpimästi tutustumista Microsoftin Windows 2008 Step-by-Step-ohjeisiin, joista löytyy lukuisia hyödyllisiä käytännön esimerkkejä siitä, miten WS 2008:n uusia ominaisuuksia voidaan hyödyntää. Ohjeista löytyy myös esimerkki snapshot-toiminnosta. Snapshotin yhteydessä kannattaa muistaa komento dsamain.exe, joka mahdollistaa tilannekuvan tutkimisen.



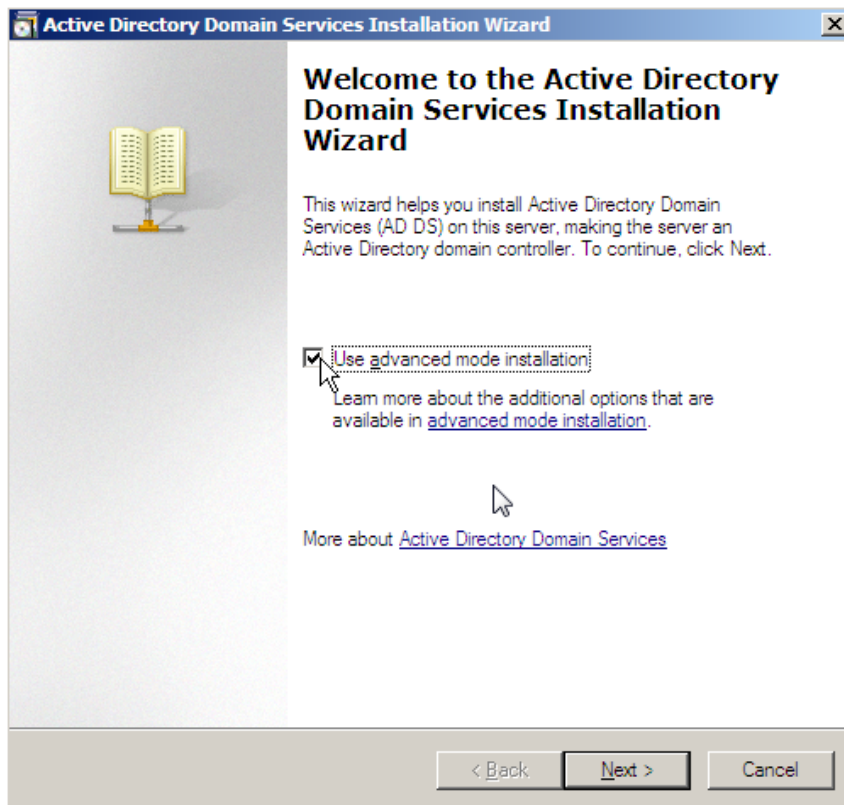
```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
C:\Windows\System32>ntdsutil
ntdsutil: snapshot
snapshot: list all
1: 2008/02/21:09:01 <ea3e3b7c-7f1f-4908-b2cd-fd699cbedf50>
2: C: <ace386c4-00cb-4f9b-9d4d-52b3909d43e7>
snapshot: _
```

Kauan toivottu ominaisuus on AD-tietokannan käsitteleminen offline-tyyppisesti. Nyt voit ntdsutil-komennon snapshot-ominaisuudella ottaa AD-tietokannasta varmuuskopion.

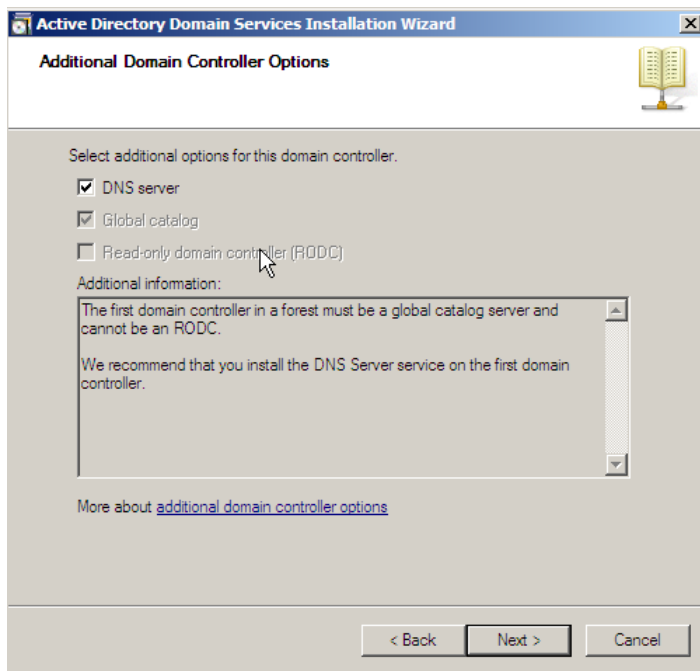
AD:n toimintaa voidaan valvoa ottamalla käyttöön uudenlainen valvontakäytäntö (Directory Service Changes), jonka avulla tapahtumienvälvontaan voidaan lokittaa tapahtumienvälvönnon security-lokiin sekä vanha että muuttunut AD:n objektin tai attribuutin arvo.

Eräs keskeinen tietoturvallisuuteen liittyvä parannus on salasanaikäytäntöjen kohdistaminen toimialueen sijaan yksittäiseen käyttäjään tai global security-ryhmään. Tämä mahdollistaa eritasoiset salasanat niin salasanojen pituuden, vaihtamisvälin, monimutkaisuuden kuin lukitsemiskäytännön osalta. Salasanapolitiikkaa ei voi suoraan kohdistaa esimerkiksi OU-tasoon, vaan se onnistuu siirtämällä OU:n käyttäjät ns. varjo-eli shadow-ryhmän kautta global security-ryhmän jäseneksi, jonka jälkeen siihen voidaan kohdistaa halutunlainen salasanapolitiikka.

Vinkki: Asennettuasi AD DS-roolin, varsinainen AD:n käyttöönotto tapahtuu edelleen komennolla dcpromo. Saat lisäasetuksia joko valitsimella /adv tai laittamalla rastin kohtaan Use advanced mode installation.

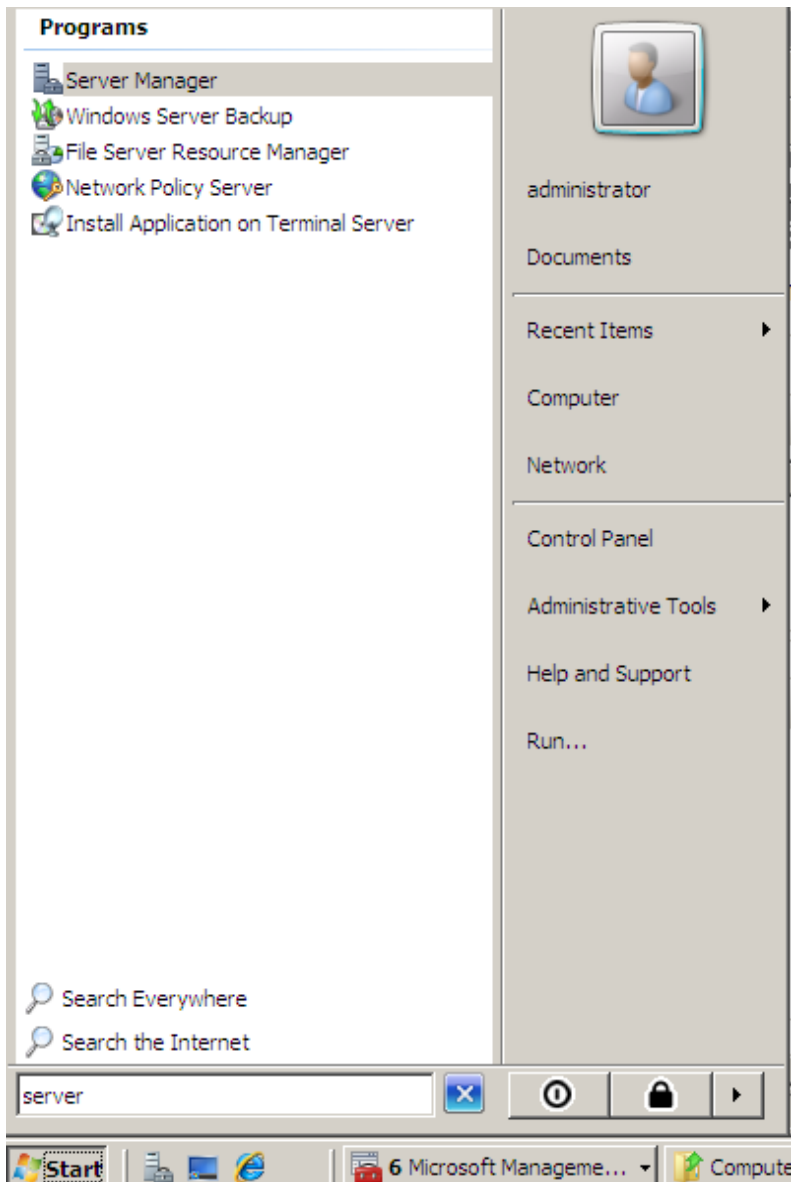


AD:n asentaminen tapahtuu AD DS-roolin lisäämisen jälkeen dcpromo-komennolla. Saat uusia ominaisuuksia käyttöön rastittamalla ruudun tai käyttämällä dcpromo /adv-valitsinta.



Vistasta lainattua

WS 2008 sisältää lukuisia alun perin Vistassa esiteltyjä uusia ominaisuuksia. Käyttöliittymän Start-valikko sisältää saman todella kätevän hakutoiminnon kuin Vista. Kokeile esimerkiksi hakusanoja server, secu ja net. Hiiren kakkospainikkeesta löytyy uusia toiminnallisuuksia, kuten pikakuvakkeiden nopea lisääminen pikakäynnistykseen tai pikakuvakkeen lisääminen Start-valikkoon.



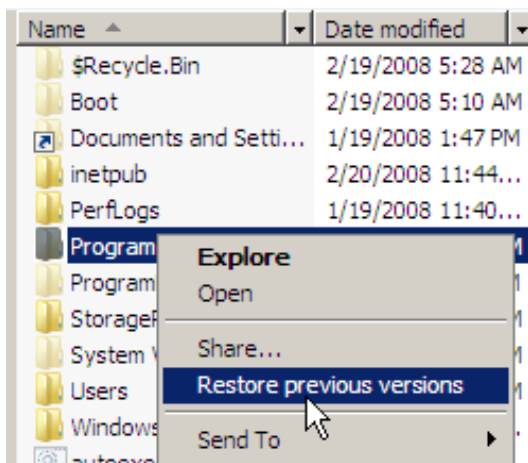
Opettele keskeisimpien ohjelmien nimestä muutama alkukirjain niin nopeutat palvelimen hallintaa merkittävästi. Huomaa alareunan virta-painike ja saman rivin lopussa oleva kolmio, josta palvelin uudelleenkäynnistetään.

Tehtäväpalkin ominaisuudet ovat myös identtiset ja niitä kannattaakin käydä säätämässä. Esimerkiksi Start-valikossa voi kasvattaa oletuksena näytettävien ja eniten käytettyjen sovellusten lukumäärää (oletusarvo 9).

Resurssienhallinta (Win+e-pikanäppäin) aukaisee samanlaisen resurssienhallinnan kuin Vistassa. WS 2008 sisältää samanlaisen indeksoinnin kuin Vista, mutta se on oletuksena pois päältä. Ota indeksointi käyttöön valinnalla Server Manager | Roles | Add | File Services. Valitse ainakin Windows Search Service. Älä asenna Windows Server 2003 File Services:n alaisuudessa olevia toimintoja kuten Indexing Service.

Sen sijaan eräs Vistan hyödyllisimmistä ominaisuuksista - palauta edelliset tiedostot eli Previous versions - toimii WS 2008:ssa samalla lailla kuin Vistassa. Voit palauttaa palvelimelta poistettuja tai muuten hävinneitä tiedostoja hiiren kakkospainikkeen Restore previous versions-komennolla. Ennen kuin toiminto on käytettävissä, pitää se aktivoida kiintolevyn ominaisuuksista Shadow Copies-valinnasta. Sen sijaan WS 2008 ei sisällä System Restore- eli järjestelmän palautus-toimintoa, koska esimerkiksi Domain Controller-palvelimella väärinkäytettynä se saattaisi sotkea Active Directoryn toimintaa perusteellisesti.

Ennen kuin voit palauttaa kansioista tai tiedostoista edellisiä versioita, varjokopiot pitää ottaa käyttöön kiintolevyn ominaisuuksista Shadow Copies-valinnasta. Voit ajastaa sekä säätää toiminnon käytettävissä olevaa levytilaa Setting-asetuksista.

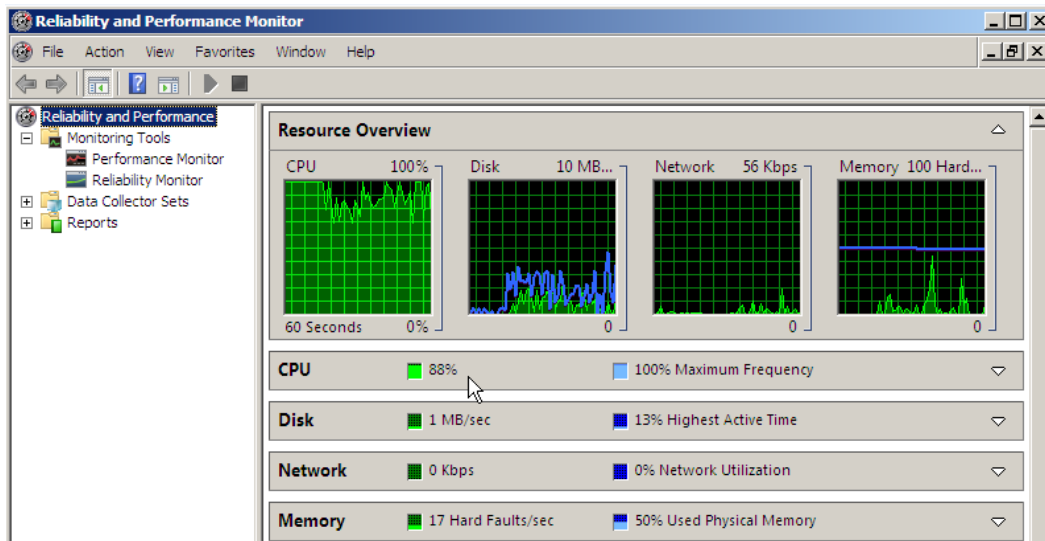


Kun varjokopiot ovat toiminnassa, voit palauttaa kansiota tai tiedostoja hiiren kakkospainikkeen komennolla.

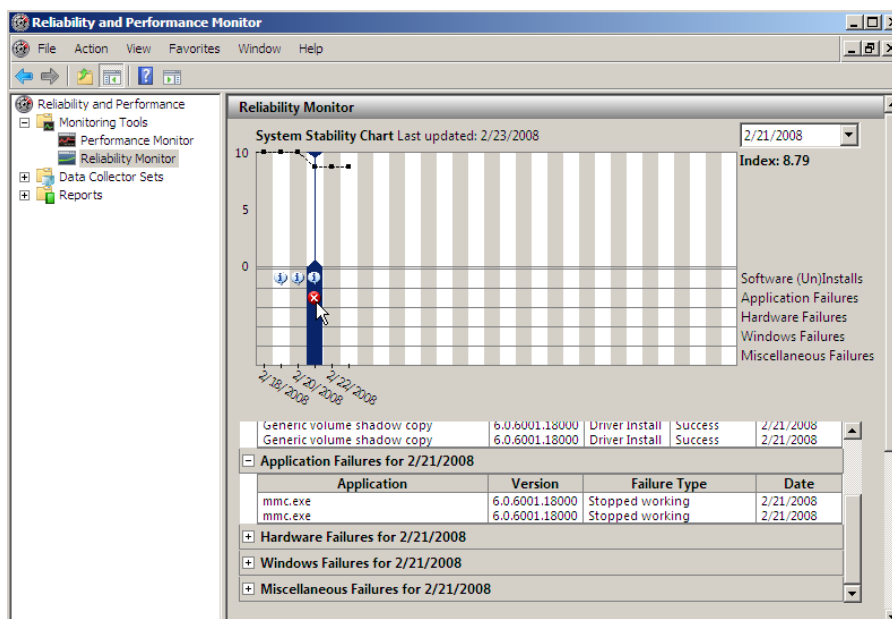
voit lisätä Server Manager-ohjelman Add Features-kohdasta Desktop Experience-toiminnallisuuden, jolla voit lisätä joitakin Vistan ominaisuuksia, kuten esimerkiksi Windows Media Playerin, teemat ja valokuvien käsittelytoimintoja.

9. Vistan parhaat apuohjelmat mukana

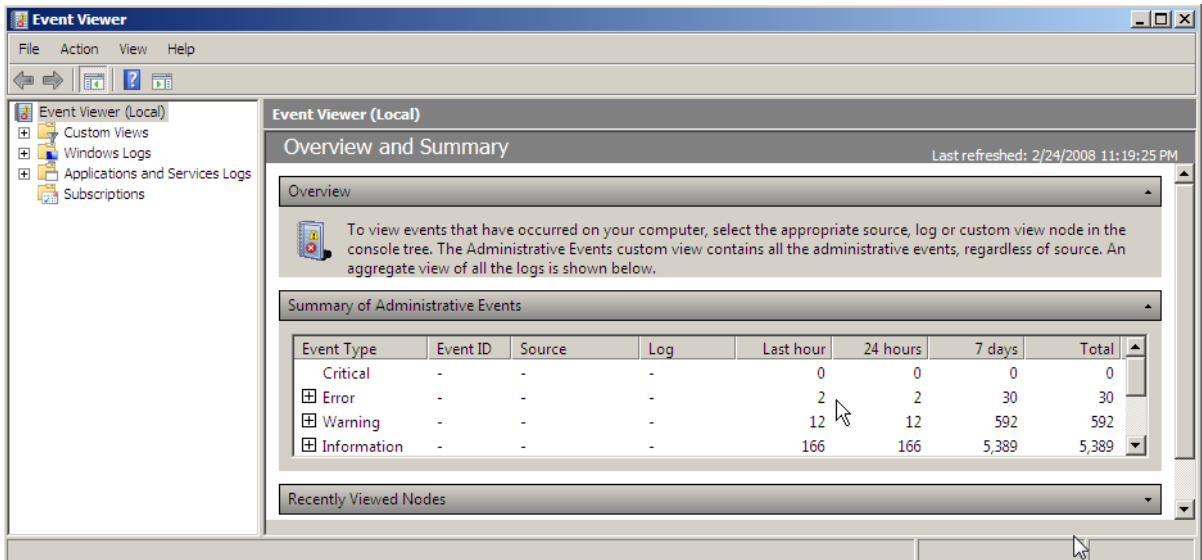
Vistasta on lainattu myös vianselvityksen ja järjestelmän syvällisemmän toiminnan analysointiin tarkoitettut Luotettavuuden ja resurssien valvonta eli WS 2008:ssa Reliability and Performance Monitor sekä tapahtumienvälvonta- eli Event viewer-ohjelmat. Edellä mainituilla saat kattavan resurssikatsauksen tietokoneen sen hetkisestä suorituskyvystä ja voit porautua neljään keskeiseen suorituskyvyn osa-alueeseen eli suorittimen, levyjärjestelmän, lähiverkon ja muistin toimintaan löytääksesi mahdollisen pullonkaulan tai palvelimen suorituskkyä muuten häiritsevän tekijän. Reliability Monitor -kohdan System Stability Chart on jatkossa oiva työväline osoittaa tietohallinnolle ja organisaation johdolle, kuinka hyvin palvelimet ovat suoriutuneet SLA-vaatimuksista.



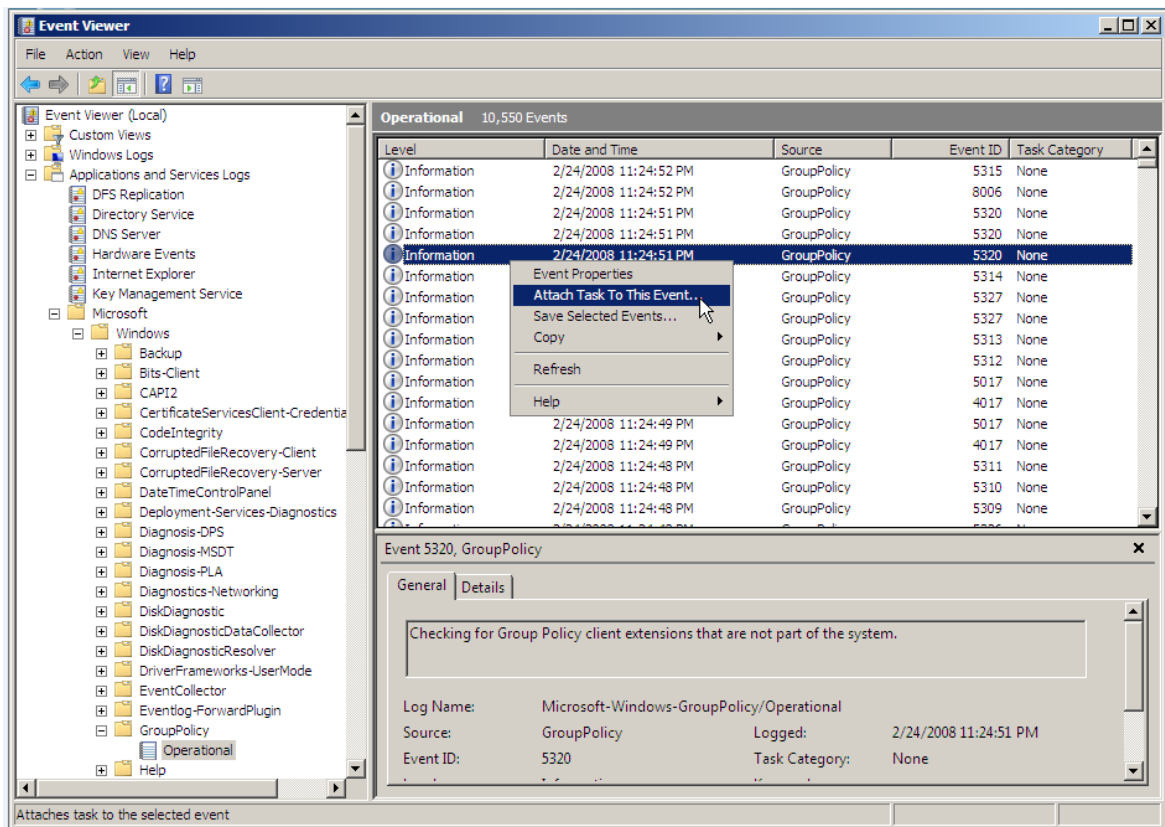
Suorituskyvyn selvittelyyn Reliability and Performance Monitor tarjoaa uusia aseita.



Palvelimen käytettävyyttä voidaan selvittää System Stability Chartin avulla. Voit keskitetysti tutkia sekä 2008:n että Vistan näitä tietoja System Center-tuotteilla.

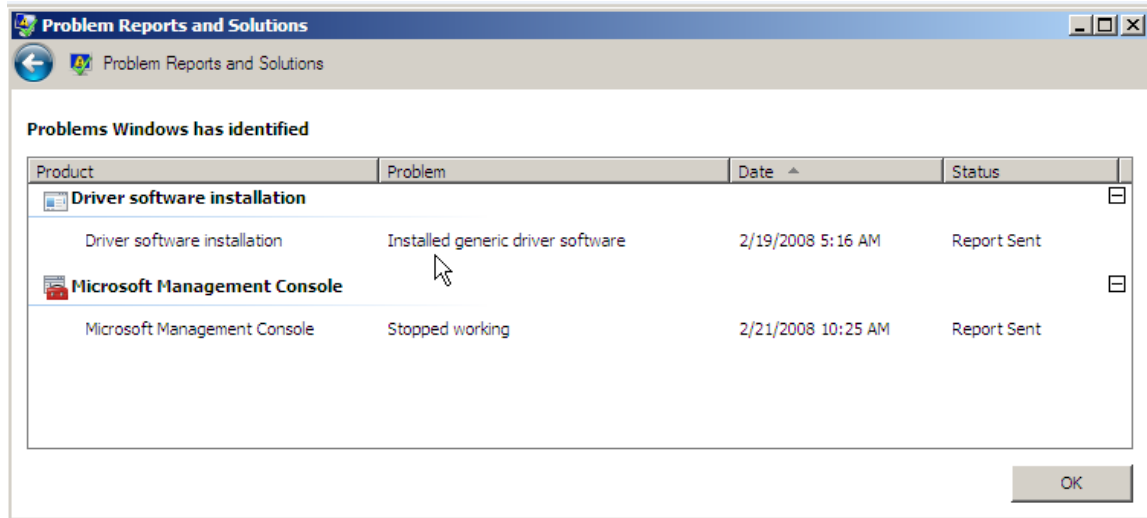


Event viewer on uudistunut perusteellisesti. Perusnäkömään avulla saat heti käsityksen palvelimen toimintakunnosta virheiden ja varoitusten lukumäärää tutkimalla.



Edistyneempää vikadiagnostiikkaa varten tapahtumienvälvonta sisältää WS 2008:n palvelu- ja toimintokohtaisia lokitietoja, jotka kannattaa ensimmäisenä ongelmatilanteissa tutkia.

Kolmantena apuohjelmana kannattaa muistaa Problem Reports and Solutions, josta valinnalla View problem history saat esille palvelimen tunnistamat ongelmat. Voit etsiä ratkaisuja löydettyihin ongelmiin valinnalla Check for new solutions.



Mikäli ongelmia on havaittu paljon, on palvelimen stability chart-indeksi yleensä myös vastaavasti laskenut eli tässä olevien ongelmien lukumäärä indikoi myös yleisemmin palvelimen hyvinvointia.

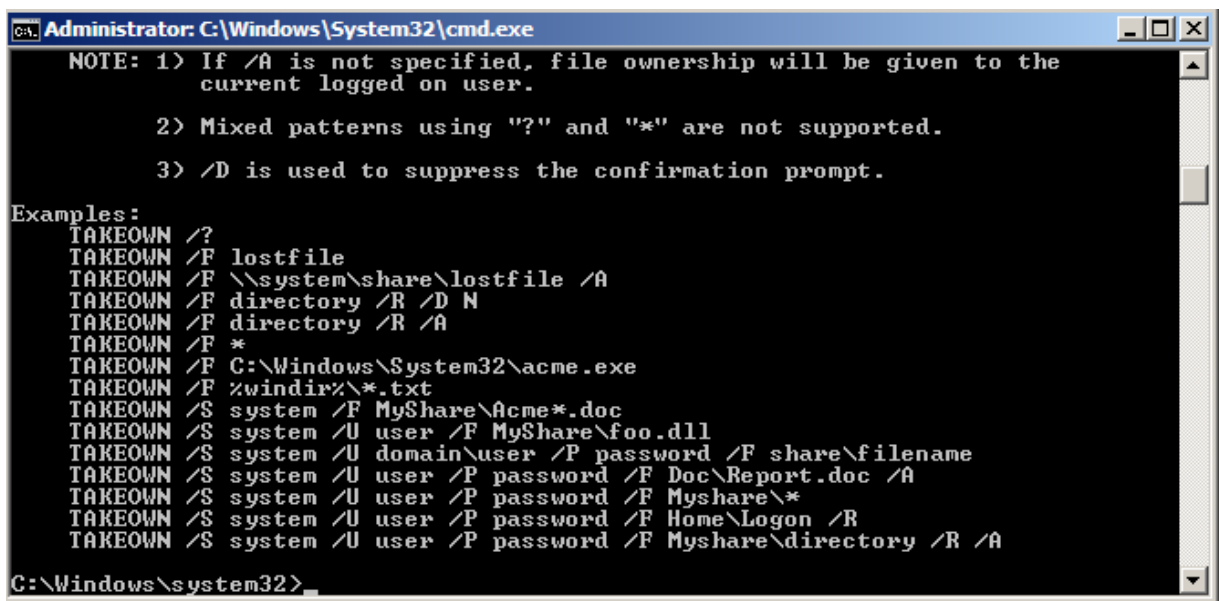
Kolme edellä mainittua saat käyntiin nopeasti muistamalla: Win + rel, Win + eve, Win + pro ja painamalla enter. Jatkossa tätä Start-valikon hakutoimintoa kannattaa hyödyntää siten, että opettelet keskeisten ohjelmien nimestä kaksi tai kolme ensimmäistä kirjainta, joilla saat haettua haluamasi ohjelman Start-valikosta.

Periaatteessa WS 2008 voi toimia jopa IT-ammattilaisen työasemana. Voi olla, että kaikki ohjelmat eivät välttämättä asennu, mutta sitä varten voit ajaa Hyper-V:n alaisuudessa esimerkiksi Windows XP:tä, jossa ajat sellaiset sovellukset, jotka eivät muuten asennu. Vinkki: Miten Mesen saa toimimaan WS 2008:ssa? Googleta "download live 8.1".

10. Käyttöoikeuksien ja levyresurssien hallintaan uutta ryhtiä

WS 2008:n resurssien jakamiseen ja käyttöoikeuksien antamiseen liittyvät asiat ovat muuttuneet maltillisesti. Ikkunoiden ulkoasu on hieman muuttunut, mutta periaatteet kansioden ja tiedostojen käyttöoikeuksien antamisella ovat pysyneet muuttumattomina.

Voit käyttää nyt komentokehötteen komentoa takeown ottaaksesi kansioden ja tietojen käyttöoikeudet hallintaasi, myös verkon ylitse. Jos olet aikaisemmin hallinnoinut käyttöoikeuksia cmd-tasolla cacls-komennolla, käytä jatkossa sen sijaan icacls-komentoa. Sillä voit hallinnoida acl-käyttöoikeuksien ohella myös kansioden ja sovellusten Windows integrity control-asetusta, jolla säädetään kansion tai sovelluksen suojaustasoa. Integrity control on uusi ominaisuus, jolla Vistan & 2008:n tietoturvasuus parantuu oleellisesti edeltävän sukupolven Windows-ytimiin verrattuna.



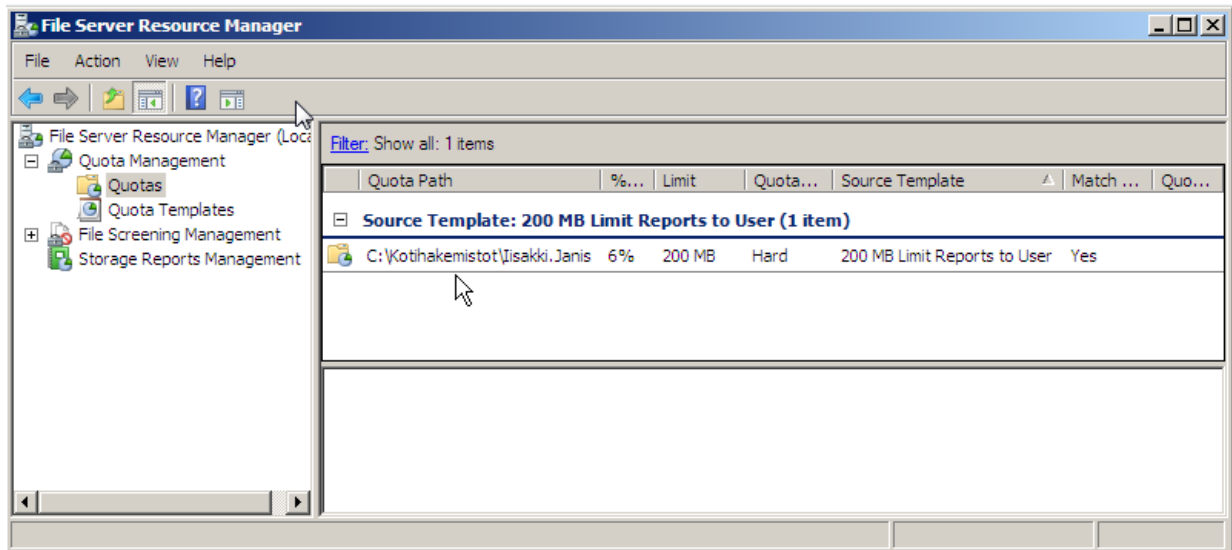
```
Administrator: C:\Windows\System32\cmd.exe
NOTE: 1) If /A is not specified, file ownership will be given to the
       current logged on user.
       2) Mixed patterns using "?" and "*" are not supported.
       3) /D is used to suppress the confirmation prompt.

Examples:
TAKEOWN /?
TAKEOWN /F lostfile
TAKEOWN /F \\system\share\lostfile /A
TAKEOWN /F directory /R /D N
TAKEOWN /F directory /R /A
TAKEOWN /F *
TAKEOWN /F C:\Windows\System32\acme.exe
TAKEOWN /F %windir%\*.txt
TAKEOWN /S system /F MyShare\Acme*.doc
TAKEOWN /S system /U user /F MyShare\foo.dll
TAKEOWN /S system /U domain\user /P password /F share\filename
TAKEOWN /S system /U user /P password /F Doc\Report.doc /A
TAKEOWN /S system /U user /P password /F Myshare\*
TAKEOWN /S system /U user /P password /F Home\Logon /R
TAKEOWN /S system /U user /P password /F Myshare\directory /R /A

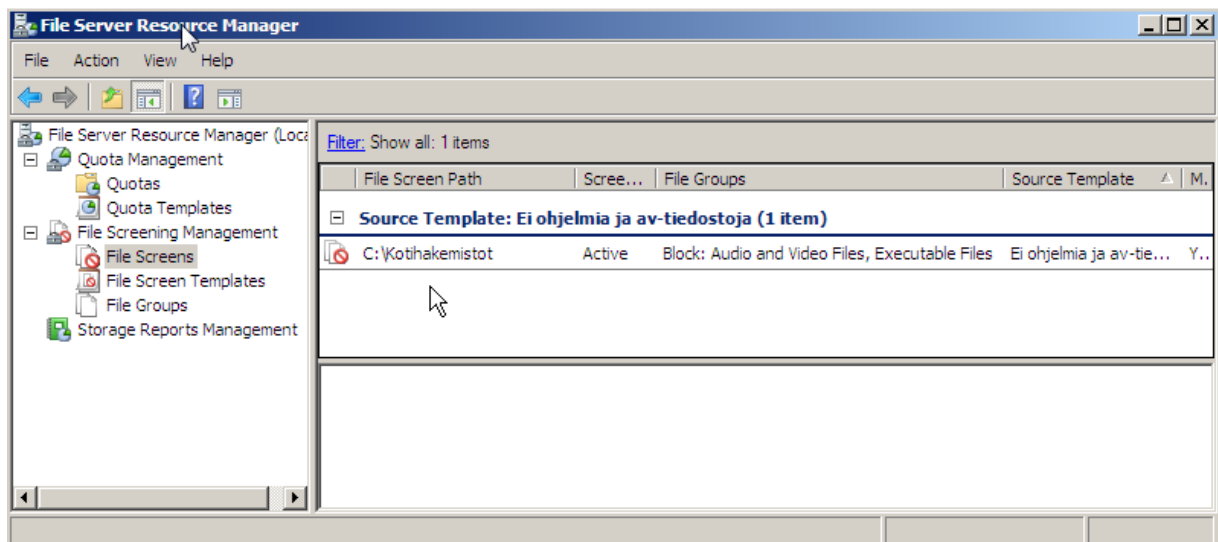
C:\Windows\system32>
```

Kansioden ja tiedostojen haltuunotto onnistuu jatkossa sujuvasti myös verkon yli cmd-tason takeown-komennolla.

Jaettujen kansioden hallintaan saat ryhtiä 2003 R2-palvelimesta tuttujen kehittyneiden levykiintiö (quota) tallennussuodatusten (file screening) avulla. Quotan avulla voit rajoittaa tallennustilaa käyttäjäkohtaisuuden sijaan kansiokohtaisesti ja tuottaa levytilan käytöstä kattavia raportteja. File screeningin avulla voit sallia tiettyjen (esimerkiksi Office-tiedostojen) tallentamisen tai estää tiettyjen (esimerkiksi ääni- ja videotiedostojen) tallentamisen palvelimelle. Myös näistä voidaan ajaa kattavia raportteja sekä järjestelmän ylläpitäjälle tai käyttäjille ja jaella ne myös esimerkiksi sähköpostitse.



Vaikka levytila on halpaa, sen varmistaminen ja hallinnoiminen vie aikaa ja rahaa. Tämän takia quota-eli levykiintiö kannattaisi tiedostopalvelimilla ottaa käyttöön.

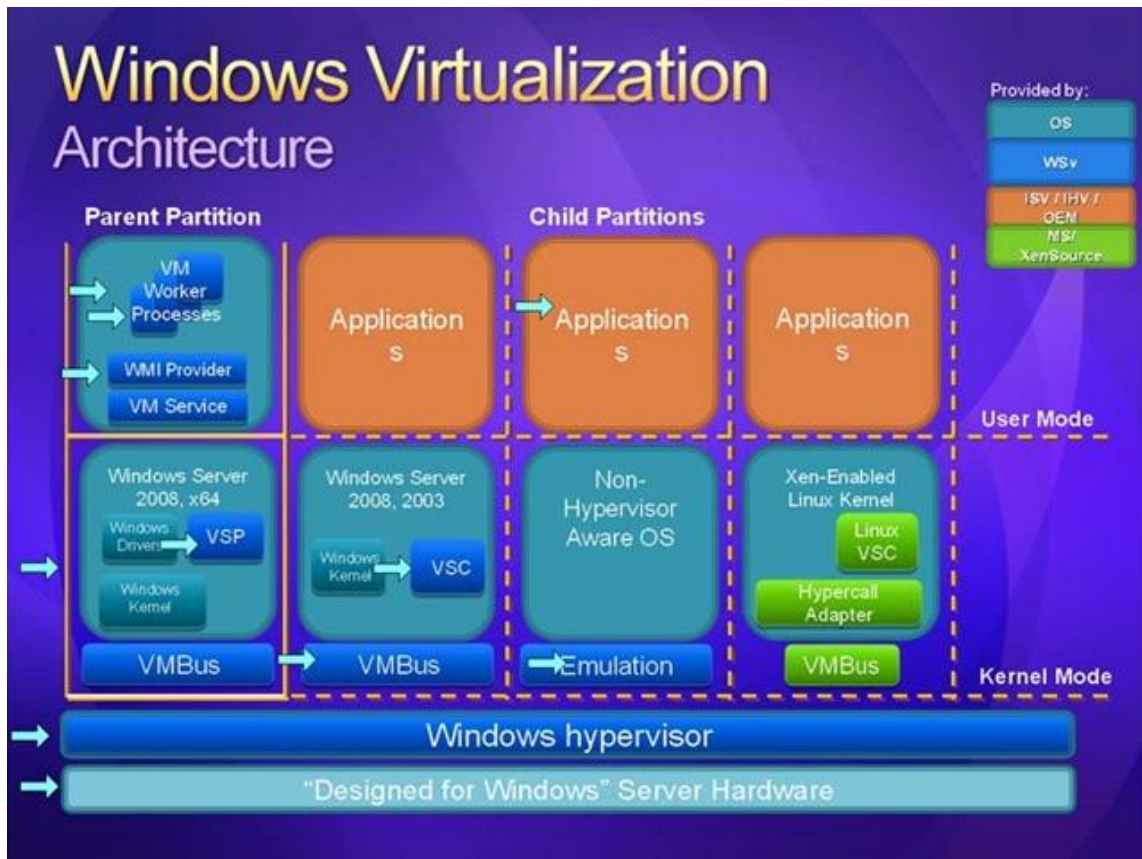


Tutkimukset osoittavat, että tiedostopalvelimilla saattaa sijaita jopa yli 50% muuta kuin työtehtäviin liittyviä tiedostoja. Suodatuksella voit joko white- tai black list-tyyppisesti määrittää, mitä palvelimelle saa tallentaa.

Eräs verkkoliikennettä nopeuttava seikka on uusi SMB-versio. Todella pitkään käytössä olleesta SMB (Server Message Block) -tiedostoprotokollasta on tehty uusi SMB2-versio, joka nostaa isokokoisten tiedostojen levytoimintojen tehokkuutta jopa useita kymmeniä prosentteja, mikä näkyy myös käytännössä! Omissa kokeiluissani olen huomannut, että kopiointi 2003-palvelimelta kesti 90 sekuntia, mutta 2008-palvelimelta alle 60 sekuntia. SMB 2 toimii vain 2008-palvelimien kesken tai 2008- ja Vista-työasemien välillä; se ei nopeuta Windows XP-työasemien verkkoliikennettä.

11. Hyper-V - virtualisoinnin uusi ulottuvuus

WS 2008:n julkistuksen myötä virtualisointi on lyönyt itsensä lopullisesti läpi. Osa uusista palvelinohjelmistoista sisältävät Hyper-V -nimellä kulkevan virtualisointitekniikan, jolla voidaan virtualisoida fyysisesti 64-bittisessä palvelimessa sekä 64- että 32-bittisiä käyttöjärjestelmiä. Nyt tuettuna ovat vihdoinkin "Linux and others". Palvelimen pitää olla 64-bittinen, sen pitää tukea laitteistopohjaista virtualisointia (Intel VT ja AMD-V) sekä tukea DEP-suojausta (Data Execution Protection).



Hyper-V on merkittävä parannus ja aiheuttaa VMwarelle paineita päivittää tuotteitaan seuraavalle tasolle, koska nyt vakiona on esimerkiksi kehittynyt SMP-moniprosessorituki, Network Load Balancing (NLB) -kuormantasaus virtuaalikoneille sekä työväline, jolla olemassa oleva fyysinen palvelin voidaan migroida virtuaalipalvelimeksi. Jopa ikivanhalla raudalla pyörivä vanha Windows 2000 voidaan nyt siirtää alustariippumattomaksi virtuaalipalvelimeksi. Näiden ohella WS 2008:n klusterointipalvelu tukee myös Hyper-V:tä, jolloin tuotteella on kaikki mahdollisuudet tulla palvelinsaleihin tuotantokäyttöön kilpailijoiden rinnalle.

Vinkki ennen palvelimen asennusta: jos haluat kokeilla Hyper-V-virtualisointia, sinun PITÄÄ ASENTAA palvelin oletus- eli Yhdysvaltalaisilla maa-asetuksilla, koska muussa tapauksessa Hyper-V ei asennuksen jälkeen toimi vaan antaa virheilmoituksen: The service changed to an unexpected state. Asennettuasi ja saatuasi Hyper-V:n toimintaan, voit vaihtaa maa-asetukset haluamaksesi.

Ennen kuin ryntäät ottamaan Hyper-V:n tuotantokäyttöön, sinun tulee huomata, että Hyper-V on mukana beta-versiona. Microsoft on luvannut lopullisen tuotteen 180 päivän sisällä, mikä tarkoittaa lopullisen version rantautuvan viimeistään kesällä.

Aikaisemmista Microsoftin virtualisointitekniikoista poiketen virtualisointi ei ole ns. add-on-tuote, vaan se on sijoitettu nyt osaksi käyttöjärjestelmän arkkitehtuuria, jolla saavutetaan edellisiä versioita parempi suorituskyky ja luotettavuus. Hyper-V koostuu seuraavista arkkitehtuurikomponenteista:

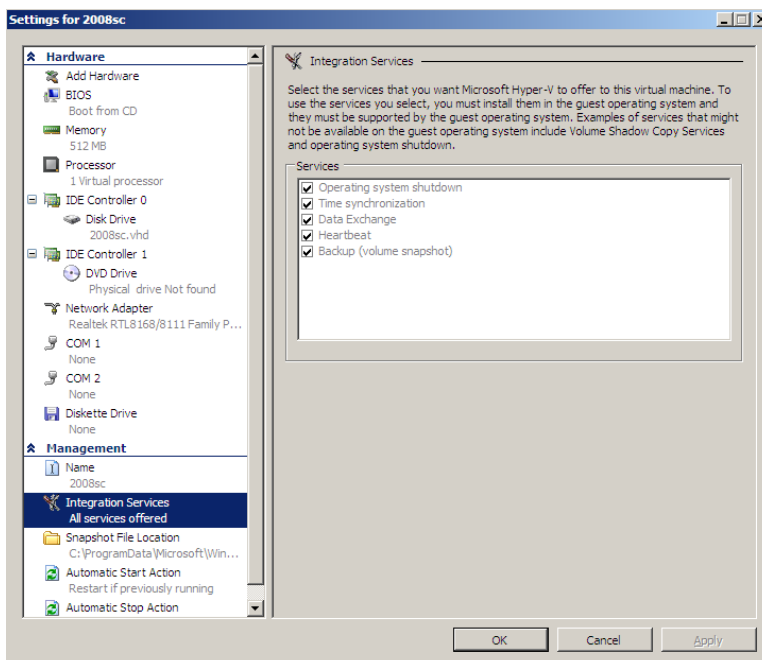
Korkeaa käytettävyyttä parantaa ja vikatilanteista toipumista edistää snapshot-toiminto, jolla virtuaalipalvelimesta voidaan ottaa ”jäädetyt” levykuva eli image esimerkiksi ennen uuden ohjelmaversioon tai tietoturvapäivitysten asennusta. Jos asennuksessa tulee ongelmia, voidaan snapshotin avulla palata nopeasti takaisin asennusta edeltäneeseen tilanteeseen.

Lisenssiteknisesti WS 2008 Standard -versio sallii ajettavaksi yhden fyysisen ja yhden virtuaalikoneen, Enterprise versio sallii neljä virtuaalikonetta ja DataCenter-palvelinkeskusohjelmisto sallii rajoittamattoman määrän virtuaalikoneita. Tehokkaassa laitteistossa (4 kpl neliydinsuorittimia ja 128-Gt ram-muistia) voidaan kuvitella ajettavan useita satoja virtuaalipalvelimia.

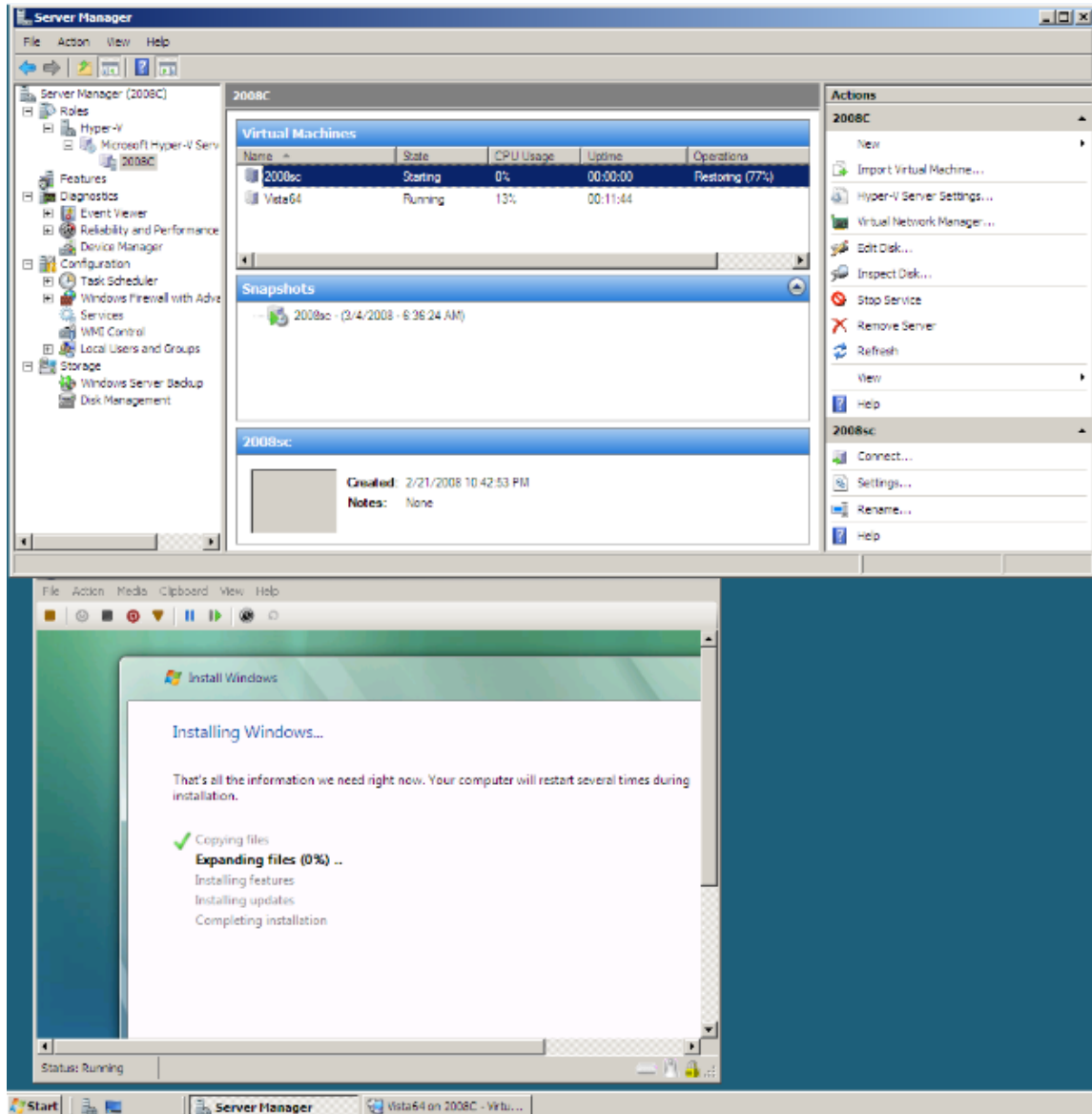
Hallinta tapahtuu perustasolla WS 2008:n mukana tulevalla hallintavälineellä. Vinkki: voit asentaa RSAT-työvälineistä Hyper-V Tools-hallintavälineet myös 32-bittisille palvelimille ja aikanaan myös Windows Vistaan. Jos käytät TS-tekniikkaa, voit julkaista hallintavälineet käyttöösi sitä kautta.

Kun virtualisoinnista halutaan saada kaikki teho irti, esiin astuvat niin System Center Virtual Machine Manager kuin System Center Operations Manager. Testiympäristöön kannattaa luonnollisesti tällöin lisätä myös System Center Configuration Manager ja tutkia, miten näiden kolmen tuotteen avulla voit keskittää virtuaalipalvelimien hallinnan ohella kaiken muun olemassa olevan IT-infrasi hallinnan ennen lopullista hankintapäätöstä. System Center-tuotteista on saatavilla 120-päivän koekäyttöversio.

Hyper-V tuo nyt Linux/Unix-käyttöjärjestelmät vihdoin hallittavaksi Windowsin alaisuuteen. Yhteistyö Citrixin kanssa kantaa hedelmää ei pelkästään Terminal Server-kehitystyön osalta, vaan Citrixin hankittua XenSourcen, Linux-maailma voidaan liittää entistä tiiviimmin osaksi Windows-maailmaa.



Jos olet aikaisemmin hallinnoinut mitä tahansa virtuaaliympäristöä, WS 2008:n mukana tulevat hallintavälineet on nopeasti onaksuttavissa.



12. Terminal Services - kohti läpinäkyvämpiä päätepalveluita

Mikäli virtualisointi on eräs 2008:n tärkeimpiä uusia toiminnallisia muutoksia, toinen merkitykseltään tärkeään rooliin noussut palvelu on Terminal Services-päätepalvelu.

TS tarjoaa nyt uudenlaisia tapoja käyttää sovelluksia internetin yli RDP over https -tekniikalla, jossa SSL-suojatun http-liikenteen sisässä ajetaan TS-palveluiden käyttämää RDP-protokollaa (Remote Desktop Protocol). Tällä tavalla TS Web Access ja TS Gateway -toiminnallisuudet tuovat organisaatioon jälleen yhden uuden etäyhteystavan jo muutenkin varsin kirjavan valikoiman rinnalle.

TS Session Broker mahdollistaa käyttäjän uudelleenkirjautumisen takaisin järjestelmään kuormantasauksella varustetussa TS-palvelinfarmissa. Vastaavasti TS Session Broker Load Balancing-ominaisuus mahdollistaa istuntojen jakamisen maksimissaan viiden palvelimen farmissa.

TS RemoteApp -toiminnolla voidaan julkaista käyttäjille sovelluksia ajettavaksi päätepalvelimella siten, että peruskäyttäjä sovelluksia ajaessaan ei enää tiedosta, ettei sovellusta ajeta omassa tietokoneessa vaan päätepalvelimella. Nyt kun sekä virtualisointi että päätepalvelutoiminnot ovat kehittyneet WS 2008:ssa näin merkittävästi, voi hyvin todeta, että keskitetysti hallittu ja vikasietoinen virtuaalipalvelimilla toteutettu käyttöympäristö pitäisi pikku hiljaa olla arkipäivää.

TS-palvelu on siinä mielessä erikoisessa roolissa, että sen kehittämisessä Citrixin merkitys on edelleen suuri. Usein esitetty kysymys kuuluu, miksi organisaation tulisi hankkia Terminal Server-lisenssien ohella käyttöön lisäksi Citrixin tuotteita, eikö pelkän TS:n avulla tulla toimeen? Ne organisaatiot, jotka käyttävät tällä hetkellä pelkkää TS:ää, toteavat ilolla WS 2008:n mukana tulevat uudet ominaisuudet. Sen sijaan nykyiset Citrix-asiakkaat tulevat edelleen jatkamaan Citrixin käyttöä, koska TS 2008:sta puuttuu edelleen muutamia keskeisiä ominaisuuksia.

Toivomuslistalla olevia asioita ovat esimerkiksi mahdollisuus sovellusten julkaisemiseen kaikkien käyttäjien sijaan vaikkapa suojausryhmäkohtaisesti. Mikäli käytössä on useampia TS-palvelimia, käytössä ei ole keskitettyä hallintaa, vaan sovellukset pitää julkaista jokaisella palvelimella erikseen. Raportointi- ja lokitusominaisuudet ovat myös hieman kilpailijoita jäljessä. Samoin Java- tai Linux-clientilla olisi varmasti kysyntää! TS-päätepalveluiden rinnalla kilpailee lukuisat SSL VPN-ratkaisut, joten ennen kuin rynnit hankkimaan TS CAL-käyttöoikeuslisenssejä, tutustu keskeisiin SSL VPN-ratkaisuihin!



Remote-Apin avulla on jaettu neljä sovellusta. Huomaa, tämä on kätevä tapa jakaa Server Manager-hallintaväline käytettäväksi muissa kuin 2008/Vista-koneissa.

15. Uusia ryhmäkäytäntöjä ja suosituksia

Yksi Active Directoryn mukanaan tuomista IT-tukea helpottava ominaisuus on ollut ryhmäkäytännöt (Group Policies). WS 2008 mahdollistaa nyt sujuvasti myös Vistan ryhmäkäytäntöjen hallinnoimisen, joka 200x-palvelimilla ei ole mahdollista, vaan edellyttää Windows Vista-työaseman käyttämistä. Vistan myötä GP-asetusten lukumäärä on noussut XP SP2:n noin 1400 asetuksesta lähes 2 500 asetukseen. Kun mukaan otetaan Office 2007:n GP-laajennukset, päästään asetuksissa yli 3 000:n. Määrä ei aina korvaa laatua, valtaosa uusista GP-asetuksista Vistan osalta liittyy Vistan mukana tulevien uusien toimintojen käytön estämiseen tai ominaisuuksien rajaamiseen.

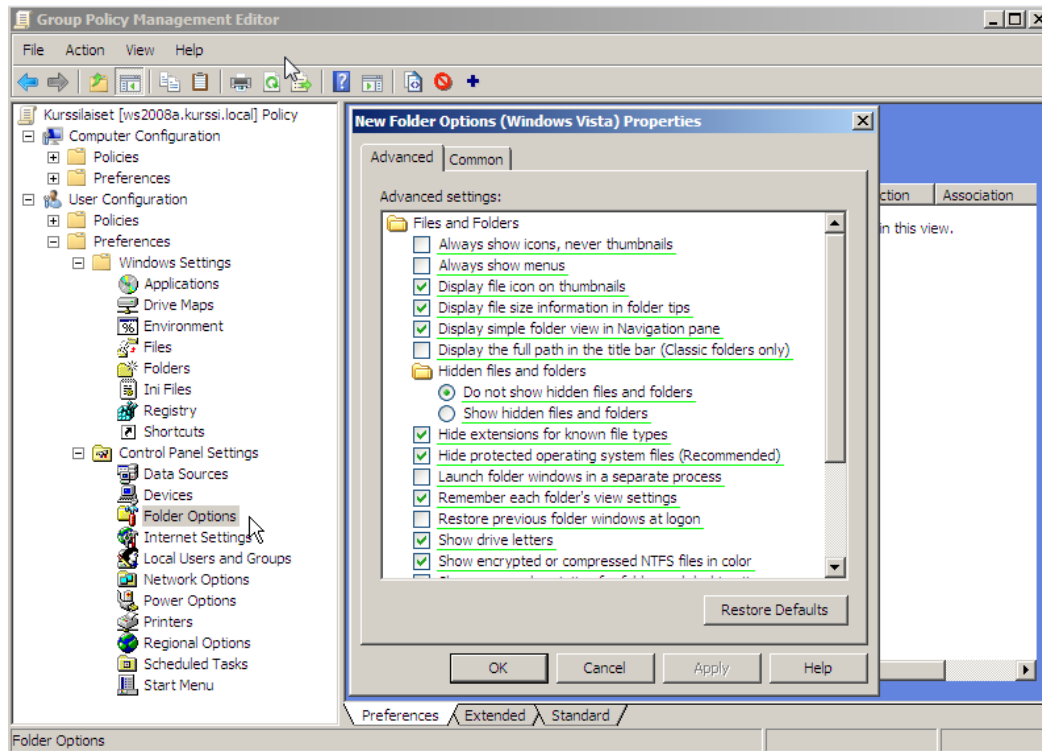
2008:n keskeisin ryhmäkäytäntöjen hallintaväline on Group Policy Management Console eli gpmmc.msc. Saat auki tämän hallintavälineen Start-valikosta gpmmc.msc-komennolla.

Nyt voit sekä hakea käytettävissä olevia ryhmäkäytäntöasetuksia että liittää tekemiisi GP-asetuksiin tarkentavia kommentteja. Kenties paras uusi toiminnallisuus on Preferences-nimellä kulkevat käyttäjäasetukset, joiden avulla voidaan käyttäjälle laittaa useita, aikaisemmin ryhmäkäytännöistäkin puuttuneita asetuksia oletukseksi päälle siten, että käyttäjä voi istuntokohtaisesti myös muuttaa niitä. Normaali GP-asetus on joko päällä tai poissa, sitä käyttäjä ei voi muuttaa. Preferences-toiminnallisuus tulee myös erikseen ladattavaksi Windows 2003-palvelimille sekä se tukee myös Windows XP-työasemia!

Preferences-asetusten avulla voit säätää esimerkiksi osaa työaseman ohjauspaneelin asetuksista kuten myös kansionäkymien oletusasetuksia, palvelimelta käytettäviä levyresursseja sekä käytettävissä olevia oletustulostimia. Erityisesti tulostimien käyttöönnotossa 2008 GP ja Preferences tarjoavat edellisiä Windows-palvelinversioita monipuolisemmat ominaisuudet. Erinomainen "Group Policy Preferences Overview" -white paper löytyy <http://ict-tuki.fi/preferences> -linkin takaa.

Mikäli organisaatiossasi on käytössä SA-ylläpito työasemakäyttöjärjestelmälle, saat käyttöösi Microsoft Desktop Optimization Pack for Software Assurance (MDOP SA) -ohjelmiston. Ohjelmisto mahdollistaa ryhmäkäytäntöjen hallitumman ja keskitetyimmän hallinnan isommissa AD-organisaatioissa. Ohjelmistolla voidaan tarvittaessa verrata tehtyjä asetusmuutoksia ja palata myös rollback-tyyppisesti edeltäviin asetuksiin.

Asetuksia voidaan kokeilla ensin offline-tyyppisesti ennen niiden ajamista tuotantoympäristöön.



Ryhmäkäytäntöjen keskeisin uudistus on **preferences**, joiden avulla saat voimaan useita sellaisia asetuksia, jotka aikaisemmin edellyttivät asetusten vakioimista suoraan käyttäjäprofiili-tasolla.

16. 2008 uutta ominaisuutta?

Omat kokeiluni niin Beta- kuin RC-versioilla ennen lopullista RTM-versiota osoittivat WS 2008:n sisältävän tuhkimotarinan aineksia. Microsoftin palvelimelle asettamat toiveet ja odotukset eivät ole katteettomia, tosin mikään ei tule ilmaiseksi. Kun organisaatio ottaa käyttöön WS 2008-palvelinympäristön, erittäin oleellinen seikka on huomioida voimassa olevat ylläpitosopimukset. Mikäli voimassa oleva sopimus sallii ilmaisen päivittämisen uusimpaan markkinoilla olevaan versioon, en näe mitään syytä, miksi tätä mahdollisuutta ei tulisi hyödyntää.

Koska WS 2008 sisältää todella paljon ”käytössä kokeiltua” Vista SP1:n sisältämää teknologiaa, kannattaa sen käyttöönottoa vakavissaan harkita ilman odottelua. Onkin odotettavissa, että useissa organisaatioissa huhkitaan ensi kesänä WS 2008-päivitysprojektien parissa. Osa odottaa loppuvuotta tai alkuvuotta 2009 ja väistämätöntä 2008 SP2-päivitystä. Kuinka niin SP2? Microsoft on nimennyt 2008 SP1-versioksi, koska käytännössä se sisältää ydintasolla niin paljon jo Vistan ytimen tasolla testattua koodia, että se voidaan uudelleennumeroida suoraan SP1-versioksi. Käytännössä siis Vistan SP1 ja WS 2008 SP1 ovat ytimen kooditasolla identtisiä ja tämän takia tätä aluksi oudolta vaikuttavaa nimeämistä voidaan pitää oikeutettuna. Jatkossa sekä Vistan että WS 2008:n service packit kulkevat käsi kädessä.

Jos organisaatiolla ei ole voimassa olevaa ylläpitosopimusta, pitää TCO-laskelmissa ottaa huomioon, että vaikka varsinaiset palvelinlisenssit saattavat vaikuttaa kohtuuhintaisilta, pitää jokainen olemassa oleva CAL-työasemalisenssi (Client Access License) saattaa WS 2008-tasolle. Mikäli TS-päätepalvelut alkavat kiinnostaa, edellyttää se joko kokonaan uusien TS CAL-lisenssien hankkimista tai vanhempien TS CAL-lisenssien päivittämistä. Kaikissa CAL-laskelmissa tulee aina huomioida, kumpi vaihtoehto eli laitekohtainen CAL (device) vai käyttäjäkohtainen CAL (user) tulee organisaatiolle edullisemmaksi. Jos taas virtualisointi tuntuu järkevältä, kannattaa miettiä jo alusta alkaen, mikä WS 2008-palvelinversio ja fyysinen palvelinlaitteisto muodostaa kustannustehokkaimman vaihtoehdon.

Edellisten lisenssikustannusten ohella tulee laskea oma tai ulkopuolelta hankittava päivitysprojektissa tarvittava työpanos, joka ei ole koskaan ilmaista.

Kannattaako odottaa?

Microsoft on julkistanut, että jatkossa näitä yrityspuolen suurempia päivityksiä tulee viiden vuoden välein, kuten nyt 2003 -> 2008 -loikassa. Jakson puolivälissä on sitten pienempi päivitys. Tämä osaltaan puoltaa ja suosii 2008-aikakauteen siirtymistä, koska arviolta vuoden 2010 kieppeillä markkinoille ilmestyvän Windows Vistan seuraajan Windows Sevenin yhteydessä on odotettavissa mitä ilmeisimmin vain pienempi server-päivitys, todennäköisesti 2008 R2-versio. Käytännössä palvelin tulee olemaan Windows Server 7 aka 2008 R2 ja se on pienempi välipäivitys.