

Standardimikrojen ylläpitojärjestelmä

Hannu Kulokari

Tietotekniikkaosasto

Tietotekniikkaosaston standardimikrojärjestelmä huolehtii Windows-työasemien keskeisten sovellusohjelmien asennuksesta ja päivityksistä, tarvittaessa myös käyttöjärjestelmän asennuksesta. Muilta osin työasemien ylläpito on edelleenkin paikallisten tukihenkilöiden vastuulla.

Standardimikrojen nykyinen ylläpitojärjestelmä tulee joulukuussa kaksivuotiaaksi. Varovaisen alun jälkeen on järjestelmään liitettyjen koneiden määrä kasvanut tasaisesti, ja on tätä kirjoitettaessa jo lähes 3000.

Nimitys ”standardimikro” on jo hieman vanhentunut. Itse mikroja tai niiden laitekoonpanoa ei ole mitenkään standardoitu – paitsi kaupallisessa mielessä, puitesopimusten kautta. Niiden ohjelmistoja ylläpidetään kuitenkin vakiomenetelmin. Vielä kaksi vuotta sitten tilanne oli toinen; silloin kaupasta saattoi ostaa valmiiksi konfiguroituja koneita, joihin oli asennettu tietty ohjelmistovarustus. Tähän vanhaan standardimikrokonseptiin ei kuitenkaan liittynyt minkäänlaista ylläpitoa.

Vieläkään ei standardimikroille ole yliopistossa tarjolla kokonaisvaltaista ylläpitopalvelua, vaan koneiden asennus ja toiminnan valvonta on edelleenkin tiedekunta- ja laitostasoisten järjestelyjen varassa. Standardimikroista onkin saatu parhaat kokemukset siellä, missä koneiden ylläpito on muutenkin järjestyksessä ja vastuuhenkilö hyvin juonessa mukana. Eri ihmisillä on erilaisia näkemyksiä siitä, kannattaako yliopiston kaltaisessa organisaatiossa keskitettyyn kokonaisvaltaiseen työasemaylläpitoon edes pyrkiä.

Seuraavassa yritän kuvata, mitä standardimikropalveluun nykyisin sisältyy ja miten se toimii, sekä kertoa jotain myös tulevaisuuden suunnitelmista.

Järjestelmän rakenne

Standardimikropalvelu koostuu kahdesta toisistaan periaatteessa riippumattomasta komponentista:

- * Windows-käyttöjärjestelmän asennus uusiin koneisiin RIS-palvelun (*Remote Installation Services*) avulla.
- * Yleisimmin tarvittujen sovellusohjelmien konekohtainen asennus ja päivittäminen.

Lisäksi standardimikrot käyttävät WSUS-palvelua (*Windows Server Update Services*), jolla asennetaan käyttöjärjestelmän ja tulevaisuudessa myös Microsoft Office -ohjelmiston korjauspäivitykset. Useimmat koneista käyttävät myös virussuoja- ja palomuuriohjelmiston keskitettyä ylläpitopalvelua. Näitä käyttävät myös muut kuin standardimikrot. Etenkin WSUS-palvelu, kuten edeltäjänsä SUS, on osoittautunut suurmenestykseksi; sitä käyttää yliopistossa jo noin 9000 konetta. Tuosta voidaan päätellä sekini, että standardimikropalvelulla on vielä paljon kasvupotentiaalia.

Ylläpitojärjestelmä perustuu tietotekniikkaosaston ylläpitämän Windows-domainin tarjoamiin välineisiin. Domain on Windows-tietokoneiden joukko, jolla on yhteinen käyttäjätietokanta, jossa niin käyttäjillä kuin domainiin kuuluvilla koneillakin on ”tili”, eli tunnus ja siihen liittyvä salasana. Käyttäjätietokantaa jäsentää ja täydentää hierarkkinen hakemisto (*Active Directory*, AD). Jokainen käyttäjä ja kone on jossain hakemiston ”lokerossa”, ja näihin lokeroihin kohdistuu Group Policyiksi

kutsuttuja hierarkkisesti periytyviä määrityskokoelmia, joilla käyttäjiä ja koneita voidaan monin tavoin hallinnoida.

Group Policy -mekanismi toimii niin, että kun työasema käynnistyy tai käyttäjä kirjautuu koneeseen, luetaan domainin hakemistosta koneeseen tai käyttäjään kohdistuvat Group Policy -määritykset ja toimitaan niiden mukaan. Lisäksi tarkistetaan säännöllisin väliajoin Group Policyihin tehdyt muutokset, mutta aivan kaikkia niihin sisältyviä määrityksiä ei toteuteta tämän ns. *background refresh* -toimenpiteen yhteydessä.

Standardimikropalvelun kannalta tärkein Group Policy -määritysten alalaji säätelee sovellusten asentamista ja päivittämistä. Näin voidaan toteuttaa yksinkertainen sovellusten jakelumekanismi, jossa asennusten kohdistuminen eli koneiden sovellusvalikoima ensisijaisesti perustuu konetilin sijaintiin hakemistossa. Varsinaisesta asennuksesta vastaa työaseman oma *Windows Installer* -järjestelmäpalvelu, joka myös huolehtii sovellusten käytönaikaisesta eheystarkistuksesta.

Sovellusten asennusmääritykset käsitellään vain koneen käynnistyksen ja käyttäjän kirjautumisen yhteydessä, ei *background refresh* -toiminnon aikana, koneen ollessa jouten. Tämä on selvä puute, koska jos kone on käynnissä jatkuvasti, ei siihen tule mitään päivityksiä. WSUS-järjestelmä onneksi toimii toisin. Jotkut käyttäjät myös häiriintyvät siitä, että koneen käynnistyminen saattaa päivitysten asentamisen vuoksi joskus hieman kestää. Eikä asennuksia voi mitenkään ajastaa tai lykätä tuonemmaksi. Vakava puute on myös se, että mihinkään ei kirjaudu tietoa siitä, onko kone X saanut asennettua sille määrättyjä sovellukset. Tämä selviää vain käymällä katsomassa sitä konetta. ”Keskitetty ohjelmajakelu” siis jättää tehtäviä myös paikallisille tukihenkilöille.

Käyttäjätunnukset

Domainiin liitettyyn standardimikroon voi kirjautua koneen paikallisella käyttäjätunnuksella tai Netware-asiakasohjelman luomalla tilapäisellä tunnoksella, mutta täyden hyödyn saamiseksi toivotaan käyttäjien hankkivan itselleen domainin käyttäjätunnuksen. Tällöin ovat käytettävissä seuraavat lisäpalvelut:

- * Asennettujen sovellusten automaattinen tai manuaalinen eheystarkistus, joka vaatii lukuoikeuden domainin tiedostopalvelimiin
- * Mahdollisuus asentaa tarjolle asetettuja lisäsovelluksia omaan käyttöön ilman järjestelmävalvojan oikeuksia
- * Tiedostopalvelu profiilien ja kotihakemistojen säilömistä varten
- * Mahdollisuus julkaista tulostimia domainin hakemistossa ja käyttää näin julkaistuja tulostimia

Windows-domainin käyttöluvut tunnetaan yliopistossa nimellä ”AD-lupa”. Niitä on tällä hetkellä voimassa noin 4400 kpl, joista vajaa puolet lääketieteellisen tiedekunnan alidomainissa.

Lääketieteellisessä tiedekunnassa AD-lupa annetaan myös opiskelijoille, Netware-mikroverkkoluvan sijasta. Muualla AD-lupia ovat tähän mennessä hankkineet vain ne, jotka ovat sitä erityisesti tarvinneet, joko standardimikropalvelua varten tai Metaframe-palvelimen (mm. WinOodi- ja yleislaskutussovellukset) käyttöä varten.

AD-lupa soveltuu haltijansa pääkäyttölupaksi ja kaikkiin tavanomaisiin käyttäjätunnustarkoituksiin. Sen haltija ei siis välttämättä tarvitse muita käyttölupia, jos ei käytä esimerkiksi unix- tai Netware-palveluita.

Ohjelmistovalikoimat ja hallinta

Koneisiin asentuvan ohjelmistovalikoiman määrää konetilin ”lokero” eli tilin sijainti hakemiston hierarkiassa. Tarjolla on muutama kaikille avoin perusvaihtoehto, lisäksi on eräille tiedekunnille ja

suurille laitoksille perustettu omat räätälöidyt lokerot. Näitä voidaan perustaa lisääkin, kunhan lokeroon tulee riittävästi koneita ja sille löytyy selkeä vastuutaho.

Konetilin hallintaoikeus on normaalisti vain sen perustajalla. Siten vain hänellä on oikeus liittää kone tiliä käyttäen domainiin. Ensimmäisellä kerralla tästä ei aiheudu ongelmia, mutta jos kone joudutaan asentamaan uudelleen, ja ylläpitäjä on vaihtunut, tarvitaan domainin järjestelmänvalvojan apua.

Jos esimerkiksi tiedekunnan koneille on järjestetty oma lokero, konetilien hallintaoikeus voidaan antaa ryhmälle, johon kuuluvat tiedekunnan kaikki tukihenkilöt. Tässä yhteydessä voidaan tehdä muitakin hallintaa helpottavia järjestelyitä.

Käyttöönotto käytännössä

Uuden koneen käyttöönotto standardimikropalvelun avulla tapahtuu seuraavasti:

- * Luetaan ohjeet sivulta <http://rontti.helsinki.fi/pctuki/std/>.
- * Hankitaan ainakin koneen ylläpitäjälle tai asentajalle AD-lupa.
- * Perustetaan koneelle tili sellaiseen domainin hakemiston lokeroon, jonka ohjelmistovalikoima vastaa käyttötarpeita.
- * Jos käyttöjärjestelmä halutaan asentaa RIS-palvelun avulla, asetetaan verkkokäynnistys (PXE) käyttöön koneen BIOS-asetuksista, ja käynnistetään työasema sitä käyttäen. Kun RIS-palvelin vastaa, autentikoidutaan ja valitaan haluttu asennusvaihtoehto, jos tarjolla useampia. Asennus sujuu tämän jälkeen automaattisesti.
- * Liitetään kone domainiin, jolloin koneeseen asentuu seuraavien uudelleenkäynnistysten yhteydessä konetilin hakemistolokeron määräämä sovellusvalikoima. RIS-asennusta käytettäessä domainiin liittäminen tapahtuu automaattisesti
- * Tehdään koneeseen tarvittavat säädöt ja vaihdetaan järjestelmänvalvojan salasana sekä asennetaan mahdolliset lisäsovellukset. Tämän jälkeen työasema on valmis varovaiseen käyttöön.
- * Ensimmäisten käyttötuntien aikana kone hakee WSUS-palvelimelta käyttöjärjestelmän korjauspäivitykset sekä virusvahti- ja palomuuriohjelmiston hallintapalvelimelta uusimmat viruskuvaustiedostot ja palomuurin asetukset. Vasta tämän jälkeen työasema on turvallisessa käyttökunnossa.

Palvelukokonaisuudessa RIS on epäoleellinen joskin tukihenkilöille ilmeisen hyödyllinen osa. Käyttäjän kannalta on samantekevää, millä tekniikalla peruskäyttöjärjestelmä on koneeseen asennettu, kunhan se on konfiguroitu järkevästi. RIS-asennuksen onnistumisen edellytyksenä on, että RIS-palvelimella on tarjota asiakaskoneelle tarvittavat laiteajurit. Käytännössä palvelu kykenee asentamaan käyttöjärjestelmän useimpiin niistä työasemista, joita yliopistoon on viime vuosina ostettu puitesopimuskumppaneilta, tai jotka ovat laitetasolla näiden koneiden kaltaisia. Ainakin kaikkien nykyisten puitesopimuskoneiden tarvitsema ajurivalikoima pyritään pitämään saatavilla.

Kannettavat koneet

Koska ylläpitojärjestelmä perustuu verkon ja Windows-domainin palveluiden käyttöön, luonnollisesti edellytetään, että koneet ovat verkossa kiinni, vieläpä sellaisessa verkossa, josta saa yhteyden domainin palvelimiin jo konetta käynnistettäessä. Kannettavat koneet eivät useinkaan täytä tätä vaatimusta, eivät myöskään ne koneet, jotka kytkeytyvät yliopiston verkkoon VPN-yhteyttä käyttäen.

Suositukseni domainiin liitettyjen kannettavien koneiden käyttäjille on se, että jos konetta ei saada kaapelilla kytkettyä yliopiston sisäverkkoon, niin laitetta käynnistettäessä irrotetaan mahdollisesti muuhun verkkoon kytketty verkkokaapeli ja suljetaan WLAN-sovittimen radio, ja kytketään

verkkoyhteys vasta sitten, kun koneeseen on ensin kirjauduttu. Toimitaan siis aivan kuin käytettäisiin modeemia. Näin menetellen vältetään monenlaiset sotkut ja viiveet, jotka aiheutuvat siitä, että kone käynnistyessään luulee olevansa verkossa, mutta ei kuitenkaan saa yhteyttä domainin palvelimiin.

Jotta myös ohjelmapäivitykset saataisiin työasemaan, pitää se aika-ajoin kytkeä kaapelilla yliopiston sisäverkkoon, ja varautua siihen, että ensimmäinen käynnistys saattaa hieman kestää. Jos tuo kuulostaa liian hankalalta, pitää ylläpito järjestää jollain muulla tavoin, liittämättä konetta domainiin.

Myös RIS-asennuksen kannalta kannettavat ovat ongelmallisia, koska niissä on paljon erikoiskomponentteja ja merkkikohtaisia ohjelmistoja. Tiukka standardointi auttaisi tässä.

Kehityskohteita

Uusi sovellusten jakelujärjestelmä

Kuten edellä jo mainittiin, nyt käytössä olevassa yksinkertaisessa perusmekanismissa on eräitä puutteita, sekä itse asennusjärjestelmässä että etenkin raportoinnissa. Virallinen tapa asian kuntoon saattamiseksi olisi ottaa käyttöön Microsoftin SMS-järjestelmä (*Systems Management Server*). Sen avulla ”kaikki ongelmat ratkeavat” ja SMS-järjestelmällä voidaan ylläpitää myös sellaisia koneita, kuten kannettavia, joita syystä tai toisesta ei ole sopivaa liittää domainiin. Mutta SMS vaatisi merkittävää panostusta uuteen infrastruktuuriin, eikä sen ylläpitoon luultavasti nykyinen henkilöstö riittäisi. SMS merkitsisi myös pitkää askelta kohti keskitettyä kokonaisvaltaista ylläpitoa, mikä ei ehkä kaikkialla yliopistossa ole toivottu kehityssuunta. Asiaa harkitaan.

Tutkittavana on myös eräs huomattavasti kevyempi ja nyky-ympäristöön helpommin sopeutuva ratkaisu, jolla silläkin saadaan asennusmenettelyä parannettua, ja jonkinlaisia raporttejakin kertyy. Mutta kysymyksessä on aivan uusi tuote.

Sovellusvalikoiman kehittäminen

Periaatteena on ollut, että keskitettyyn ylläpitoon otetaan vain sellaisia sovelluksia, joita yliopistossa käytetään yleisesti ja joihin yliopistolla on vapaa (ilmainen tai ostettu) käyttöoikeus. Pienen piirin sovellukset ja erillistä lisenssiä vaativat ohjelmat jäävät paikallisen ylläpidon vastuulle. Lisäksi sovellusten on teknisesti sopeuduttava keskitettyyn asennusmenettelyyn, ja niiden käytön on oltava mahdollista peruskäyttäjän oikeuksin. Turhaa rinnakkaisuutta ei ole tarkoitus ylläpitää, esimerkiksi yksi Office varmaankin riittää. Ehdotuksia otetaan vastaan.

Lähituki

Tietotekniikkaosastossa on keskusteltu maksullisen lähituen tarjoamisesta standardimikrojen käyttäjille ja käyttöönottajille. Kenties tässä päästään alkuun. Itse järjestelmää suunniteltaessa on kuitenkin lähdetty siitä, että käytön pitää olla mahdollista myös ilman keskitettyä tukea.

Mikroverkkoinfrastruktuuri

Windows-domainissa on AD-luvan haltijoiden käytettävissä tiedostopalvelu, ja tulostuspalveluita voivat käyttäjätahot itsekkin rakennella domainin tarjoamin keinoin. Näiden palveluiden käytön soisin lisääntyvän. Perinteistä Netware-palvelua voi toki myös käyttää, jos siihen on jokin erityinen syy, mutta se on käyttäjälle hankalampaa ja yleensä täysin turhaa. Tämän alueen ajankohtainen kehityskohde on uuden kiintiöintijärjestelmän valinta ja käyttöönotto.

Luokkakäyttö

Standardimikrot eivät sellaisinaan sovellu eikä niitä ole tarkoitettu luokkakäyttöön. Luokkakoneet täytyy muun muassa käyttäjien oikeuksien osalta konfiguroida aivan eri tavalla kuin henkilökohtaiseen käyttöön tarkoitettuihin työasemiin. Group Policy -mekanismi kyllä tarjoaa tähän työkaluja, ja asiaa olisi

mielenkiintoista tutkia sopivan pilottiprojektin yhteydessä. Jotta konfigurointivälineet toimisivat, on koneita käytettävä domainin käyttäjätunnuksilla, joita esimerkiksi opiskelijoilla ei vielä juurikaan ole, paitsi lääketieteellisessä tiedekunnassa, jossa domainin avulla ylläpidettyjä luokkia onkin ollut jo pitkään käytössä.