

Käyttöluvan elinkaari

Jonne Viljanen
Hannu Kulokari
Visa Rauste
Tietotekniikkaosasto

Käyttöluvan tie keskitetystä *Master*-tietokannasta eri tietokonejärjestelmien toimivaksi tunnukseksi vaatii monta vaihetta. Lupien ja niihin liittyvien tietojen hallinta on räätälöity kullekin järjestelmälle erikseen.

Novell- eli eDirectory-tunnukset

eDirectory-tunnusten elinkaaren hallinnoinnista vastaa yhdellä mikroverkkopalvelimella toimiva ohjelmistokokonaisuus, joka sisältää erikoistuneita automaatteja tunnuksen hallinnan eri vaiheiden ylläpitoon.

Monet automaattit toimivat siten, että ne määrääjoin tarkistavat, onko Master-tietokantaan tehty tunnustietojen muutoksia. Esimerkiksi uusia tunnuksia luova ohjelma käy 10 minuutin välein tarkistamassa, onko Master-kantaan ilmestynyt uusia eDirectory-järjestelmään tarkoitettuja tunnuksia. Mikäli näitä löytyy, käy ohjelma noutamassa palvelinkohtaiset erityisasetukset siltä mikroverkkopalvelimelta, johon tunnus on määritelty luotavaksi. Tämä tarjoaa laitoksille joustavan mahdollisuuden määritellä tunnuksia varten omia erityisasetuksiaan.

Saatuana luontiin tarvittavat tiedot kerätyksi ohjelma tekee tunnuksen eDirectory-tietokantaan. Lisäksi sovellus asettaa tunnuskohtaiset parametrit, liittää tunnuksen määritelyihin ryhmiin, aktivoi käyttäjälle iFolder-palvelun, luo kotihakemiston ja tietyissä laitospalvelimissa myös postihakemiston sekä antaa tarvittavat käyttöoikeudet ja kiintiöt mainittuihin hakemistoihin. Tämän jälkeen tunnus on käytettävissä ilman muita erityistoimenpiteitä. Novell-mikroverkossa on tavallisten käyttäjätunnuksien lisäksi myös ns. kevyttunnuksia sekä unix-tulostustunnuksia, joiden luonti toteutetaan periaatteessa samalla mekanismilla.

Käyttäjätunnuksella on kaksi sen käyttöön ja elinkaareen vaikuttavaa oleellista muuttujaa; salasanan sekä itse tunnuksen päättymispäivät. Näiden valvontaan tarvitaan omat automaattinsa.

Tunnuksen päättymispäivän hallintiohjelma sisältää toimintalogiikan tilanteisiin, joissa joko vanhentunut tunnus herätetään uudelleen henkiin tai voimassaoleva tunnus vanhennetaan ennen määräaikaansa. Ohjelma hakee muuttuneet päättymistiedot Master-tietokannasta ja toimii 10 minuutin jaksoissa.

Salasanojen päättymistä valvova ohjelma lukee päättymispäivän suoraan eDirectory-hakemistosta, sillä salasanaan liittyviä tietoja ei siirretä Master-kantaan. Automaatti toimii ennakkoidusti lähettäen käyttäjälle sähköpostiviestin toimintaohjeineen hyvissä ajoin ennen salasanan vanhentumista. Varsinainen salasanan vaihto on luonnollisesti jätetty käyttäjän omalle vastuulle.

Kotihakemiston koolle ja atk-asemilla tapahtuvalle tulostukselle on määritelty kiintiöt, joiden avulla voidaan jakaa käytettävissä olevat resurssit tasapuolisesti. Laitosten atk-yhdyshenkilöt voivat muuttaa kyseisiä kiintiöitä oman vastualueensa mikroverkkotunnusten osalta. Nämäkin muutokset tehdään Master-tietokantaan, josta ne päätyvät lopulta erillisten kiintiöhallintaohjelmien kautta käyttäjän eDirectory-mikroverkkotunnukselle.

Koska Master on luotetun tiedon lähde tunnuksen päättymispäivän, nimi-, laitos-, ja sähköpostiosoitetietojen osalta, ajetaan kaikille eDirectory-tunnuksille säännölliset tarkistukset, joilla varmistetaan näiden tietojen ajantasaisuus.

Windows-domain

Windows-domainin käyttäjätunnusten eli AD-tunnusten luonnista huolehtii domainin palvelimella toimiva ohjelma, joka hakee kerran tunnissa Master-tietokannasta muutokset (uudet luvat sekä lupien jatkamiset ja poistot) sekä toteuttaa ne. Samassa yhteydessä tehdään Metaframe-palveluun oikeutetuille käyttäjille tarvittavat profiili- ja kotihakemistot. Varsinaiset Windows-domainin profiili- ja kotihakemistot voi niitä tarvitseva käyttäjä perustaa itse WWW-sovelluksella; näitä hakemistoja ei siis luoda automaattisesti.

Domainin LDAP-hakemistoon ("Active Directory") talletetaan kustakin käyttäjästä nimi, sähköpostiosoite, laitoskoodi ja suhde yliopisto (opiskelija, henkilökunta tai muu). Tunnuksen sijainti domainin "lokerikossa" eli OU-hierarkiassa sekä jäsenyys eräissä käyttöoikeuksia säätelevissä ryhmissä riippuu laitoskoodista ja suhteesta yliopistoon. Kerran päivässä tarkistetaan, että nämä tiedot ovat ajan tasalla eli vastaavat Master-tietokannan sisältöä.

Salasana pitää vaihtaa kerran vuodessa. Salasanojen vanhenemisesta varoittavia viestejä lähetetään kerran viikossa hakemistoon merkittyyn sähköpostiosoitteeseen alkaen neljä viikkoa ennen salasanan kelpoisuusajan päättymistä.

Unix

Unix-käyttäjätunnusten tekniseen hallinnointiin on omistettu pieni palvelin, joka saa Master-tietokannasta kerran tunnissa muutokset (uudet luvat, lupien jatkamiset ja poistot sekä poistettujen uudelleenaktivoinnit), päivittää ne omaan tietokantaansa ja jakaa tiedot 11 interaktiiviselle unix-palvelimelle. Hallinnointipalvelin käsittelee myös salasanojen vaihdot ja välittää muutostiedot muille palvelimille viiveettä.