Yliopiston LDAP-käyttäjähakemisto

Ismo Aulaskari
Tietotekniikkaosasto

Yliopistolla käytetään LDAP-hakemistoa keskitetyn käyttäjätunnistuksen apuna. Se toimii eri tietojärjestelmille käyttäjätietojen selauspaikkana.

Tietotekniikkaosastolla on syksystä 2003 ollut käyttäjätietohakemistona OpenLDAP-pohjainen toteutus ja sitä on hyödynnetty keskitettyyn käyttäjätunnistukseen. Tämä sisäinen LDAP-hakemisto vastaa yliopiston verkon sisällä eri järjestelmien ja sovellusten LDAP-yhteyskäytännöllä tekemiin kyselyihin. Yliopistolla on myös Mainari-henkilöhakemisto, joka on toinen LDAP-protokollaa tukeva julkinen palvelu.

Sisäinen LDAP-hakemisto sisältää tarpeellisimmiksi katsotut tiedot yliopiston käyttäjista ja organisaatiosta. Jokainen käyttäjätunnus ja organisaatioyksikkö ovat hierarkkisessa hakemistossa ns. LDAP-oliona, eli tietoa ei käsitellä tauluina tai riveinä vaan aina olio kerrallaan. Myös Alma-portaalissa hallinnoidut työryhmät säilytetään LDAP-hakemistossa olioina. Niin työryhmistä kuin automaattisesti generoiduista laitosryhmistäkin ylläpidetään jäsenistön sähköpostilistoja.

Hakemiston tiedot on koottu useista taustajärjestelmistä, kuten Master-käyttölupatietokannasta, opiskelun ja opetuksen Oodi-järjestelmästä sekä Dawa-tietovarastosta. Tiedot pohjautuvat käyttäjien pääkäyttölupaan ja salasanatarkistukset ohjataan OpenLDAP-palvelusta Radius-palvelimelle. Tiedot synkronoidaan sisäiseen LDAP-hakemistoon tärkeysasteessa riippuen joko päivittäin tai 15 minuutin välein.

Hakemiston tarkoituksena ei ole toimia varastona kaikelle mahdolliselle tiedolle, mutta sisältöä kehitetään silti jatkuvasti käyttötarpeiden mukaan. Usein tarvitaan informaatiota esimerkiksi käyttäjän sijoitusyksiköstä, opiskelustatuksesta tai työsuhteesta yliopistoon..

Käyttäjähakemiston hyödyntäminen

Käyttäjätunnusten juuri hakemistossa on *dc=helsinki,dc=fi*. Yliopiston lyhyessä muodossa oleva käyttäjätunnus löytyy nimellä *uid=käyttäjätunnus,dc=helsinki,dc=fi*. Yhteys täytyy salata joko StartTLS- tai LDAPS-salauksella tai SSL-tunnelointia käyttäen. Varmenteena käytetään HY-CA-sertifikaattia. Tarkempia tietoja LDAP-palvelimesta ja sen hyödyntämisestä saa sähköpostitse.

LDAP-hakemistoa pystytään käyttämään valmiilla asiakasohjelmilla, kuten avoimella graafisen käyttöliittymän JXplorer-selaimella tai Apache-palvelimen Mod-Auth-LDAP-autentikointimoduulilla. Omissa sovelluksissa hyödynnetään usein ohjelmointikielien LDAP-kirjastoja, joissa yleensä on myös tuki vähintään LDAPS-salaukselle. Tällaisia ovat esimerkiksi Javan JNDI, Perlin Net::LDAP ja PHP:n LDAP Functions.

LDAP-autentikoinnilla voidaan yksinkertaisimmillaan vain varmistaa käyttäjän voimassaoleva käyttölupa yliopistolla. LDAP on tarkoitettu helpoksi kyselyrajapinnaksi tietokantojen ja käyttäjien välille ja valmiista lähdekoodeista ja ohjelmista on runsaudenpulaa. Yleensä otetaan hakemistosta kaikki hyöty irti ja tunnistuksen jälkeen saatavilla käyttäjän tiedoilla voidaan käyttäjä oikeuttaa sovelluksen eri toimintoihin, luoda yhteenvetoja, esitäyttää lomakkeita, muodostaa yhteyksiä käyttäjän tietoihin toisissa järjestelmissä tai liittää käyttäjän kotihakemistoja.

Jokaisella hakemiston käyttäjätunnuksella on autentikoinnin jälkeen

lukuoikeudet omiin tietoihinsa. Joskus kuitenkin on tarve käsitellä kerrallaan useamman käyttäjän tietoja, tai tehdä eräajoja ilman käyttäjän toimenpiteitä. Tällöin on mahdollista luoda vahvempi sovelluskohtainen LDAP-tunnus, jolla on laajat lukuoikeudet esimerkiksi kaikkien käyttäjien opiskelijanumeroihin.

Sisäistä LDAP-palvelinta käytetään tällä hetkellä mm. Alma-portaalin ja kansallisten Shibboleth-yhteyksien tietolähteenä yliopiston osalta, UHL-Linuxin verkkolevyjen osoitukseen, ja siltana oppimisympäristöihin, Oodi- sekä Dawa-järjestelmiin.

Lisätietoja

atk-ldap@helsinki.fi
Hakemiston attribuuttilistaus, *http://www.helsinki.fi/atk/luvat/skeema.html*
Rekisteriseloste, *http://www.helsinki.fi/atk/luvat/kh-seloste.html*