Kari Lehtinen

Novell Identity Manager: Identiteetin- ja pääsynhallinta

Opinnäytetyö
Syksy 2009
Tekniikan yksikkö, Seinäjoki
Tietotekniikan koulutusohjelma
Ohjelmistotekniikan suuntautumisvaihtoehto

Seinäjoen ammattikorkeakoulu
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

OPINNÄYTETYÖN TIIVISTELMÄ

Koulutusyksikkö: Seinäjoen ammattikorkeakoulu
Koulutusohjelma: Tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto: Ohjelmistotekniikan suuntautumisvaihtoehto

Tekijä: Kari Lehtinen

Työn nimi: Novell Identity Manager: Identiteetin- ja pääsynhallinta

Ohjaaja: Petteri Mäkelä

Vuosi: 2009 Sivumäärä: 47 Liitteiden lukumäärä: 0

Identiteetin- ja pääsynhallinta voidaan käsittää monella eri tavalla. Tässä opinnäytetyössä identiteetin- ja pääsynhallinnalla tarkoitetaan eri tietojärjestelmien, kuten Microsoft Active Directoryn liittämistä osana keskitettyä identiteetin- ja pääsynhallintaa. Työssä kerrotaan identiteetin- ja pääsynhallinnasta yleisellä tasolla sekä perehdytään tarkemmin Novell Identity Manager -ohjelmistoon ja sen ominaisuuksiin. Opinnäytetyössä käsitellään Novell Identity Manager 3.5 versiota.

Opinnäytetyössä hahmotetaan Identity Managerin toimintaa käytännössä ja näytetään miten Identity Manager toimii muun muassa Microsoft Active Directory hakemistopalvelun kanssa pienessä muutaman käyttäjän ympäristössä. Tarkoituksena on arvioida ohjelmiston toimivuutta normaaleissa ylläpitotehtävissä, kuten käyttäjien ja ryhmien lisäämisessä, poistossa ja tietojen muokkaamisessa.

Opinnäytetyön kohderyhmänä ovat lähinnä sellaiset yritykset ja yhteisöt, jotka ovat harkitsemassa keskitettyä identiteetin- ja pääsynhallintaa osana omaa tietojärjestelmäinfrastruktuuriaan tai haluavat siitä lisätietoa. Vaikka opinnäytetyössä käsitellään asioita lähinnä Novell Identity Managerin näkökulmasta, niin pätee sama idea myös muihin markkinoilla oleviin vastaaviin ohjelmistoihin.

Asiasanat: Pääsynvalvonta, Novell Identity Manager

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology
Degree programme: Information Technology
Specialisation: Software Production

Author: Kari Lehtinen

Title of the thesis: Novell Identity Manager: identity and access management

Supervisor: Petteri Mäkelä

Year: 2009 Number of pages: 47 Number of appendices: 0

Identity and Access Management can be understood in different ways. In this thesis identity and access management means connecting different information systems together by using centralized identity and access management software. This thesis tells about identity and access management in general. Identity and access management software Novell Identity Manager and its features will be examined more precisely. Version 3.5 of Identity Manager is used in this thesis.

This thesis covers also Novell Identity Manager in practice and how it works, for example, with Microsoft Active Directory in a small few user environment. The main object is to evaluate software functionality with basic administration tasks such as creating, deleting or modifying users and groups.

The main target group of this thesis is those companies and communities which consider using centralized identity and access management system as a part of their information system infrastructure or those who just want to learn about identity and access management. Although, these things are discussed from the perspective of Identity Manager, the same idea applies to other corresponding software on the market as well.

Keywords: access control, Novell Identity Manager

SISÄLLYS

KÄYTETYT TERMIT JA LYHENTEET

IDM	Novell Identity Manager.
AD	Microsoft Active Directory.
LDAP	Leight Weight Access Protocol

KUVIO- JA TAULUKKOLUETTELO

1 JOHDANTO

Nykyään erilaisten tietojärjestelmien käyttö lisääntyy jatkuvasti yrityksissä ja pienissä ja keskisuurissa yrityksissä voi olla yhtäaikaisesti kymmeniä eri tietojärjestelmiä käytössä. Mitä enemmän yrityksessä on tietojärjestelmiä, sitä vaikeammaksi niiden hallinta tulee, lisäksi tietoturvaongelmien määrä kasvaa. Näitä ongelmia pyritään hallitsemaan identiteetin- ja pääsynhallinnan ratkaisuilla. Tässä opinnäytetyössä käsitellään identiteetin- ja pääsynhallintaa Novell Identity Managerin avulla. Opinnäytetyössä käytetään Novell Identity Managerista 3.5 versiota.

1.1 Työn tavoite

Opinnäytetyön tavoitteena ja tarkoituksena on antaa lisätietoa identiteetin- ja pääsynhallinnasta. Opinnäytetyön käytännön osuudessa tavoitteena on näyttää, miten keskitetty identiteetin- ja pääsynhallinta toimii käytännössä Novell Identity Managerin avulla. Käytännön osuudella pyritään hahmottamaan identiteetin- ja pääsynhallinnan käyttöä niille henkilöille, yrityksille ja yhteisöille, jotka ovat suunnittelemassa keskitetyn identiteetin- ja pääsynhallinnan käyttöönottoa nykyisiin tietojärjestelmiinsä. Käytännön osuudessa keskitytään pääosin Active Directoryn liittämiseen Identitity Managerin kanssa, koska se on hyvin suosittu hakemistopalvelu yrityksissä.

1.2 Työn rakenne

Toisen luvun tarkoituksena on vastata muun muassa seuraaviin kysymyksiin: mitä tarkoitetaan Identiteetin- ja pääsynhallinnalla ja mitä hyötyä on identiteetin- ja pääsynhallinnasta. Luvussa perehdytään yleisellä tasolla identiteetin- ja pääsynhallintaan.

Kolmannen luvun tarkoituksena on antaa yleinen kuva Novell Identity Manager -ohjelmiston toiminnasta ja siihen liittyvistä komponenteista. Johtuen ohjelmiston monipuolisuudesta, käydään läpi tärkeimmät ominaisuudet.

Neljännen luvun tarkoituksena on luoda ympäristö, joka vastaa täysin oikeaa yritysmaailmassa toimivaa ympäristöä. Ympäristössä tulee olemaan 3 erilaista toisistaan riippumatonta palvelinohjelmistoa. Toisessa palvelimessa on Microsoft Windows Server 2003, joka toimii Domain Controllerina ja sisältää Active Directory käyttäjähakemiston. Toisessa palvelimessa on Novell eDirectory -käyttäjähakemisto. Palvelimen käyttöjärjestelmänä käytetään Linuxia. Ympäristön tarkoituksena on hahmottaa miten käyttäjät, ryhmät ja mahdollisesti käyttäjäoikeudet siirtyvät näiden järjestelmien välillä. Tarkoituksena on käyttää Windows Server 2003 -palvelimessa olevaa Active Directoryä ensisijaisena tiedonlähteenä. Jos esimerkiksi Active Directoryyn lisätään uusi käyttäjä, niin se lisätään Novell IDM:n toimesta myös muihin järjestelmiin.

2 YLEISTÄ IDENTITEETIN- JA PÄÄSYNHALLINNASTA

2.1 Mitä tarkoittaa identiteetin- ja pääsynhallinta?

Identiteetinhallinta on käsitteenä hyvinkin laaja. Nykyisin jatkuva tietojärjestelmien lisääntyminen yrityksissä korostaa identiteetin- ja pääsynhallinnan tarvetta, varsinkin suurissa organisaatioissa. Suuret IT-ympäristöt asettavat haasteita tehokkaan ja tietoturvallisen identiteetin- ja pääsynhallinnan ratkaisemiseen. Näiden ongelmien ratkaiseminen varsinkin suurissa organisaatioissa ovat lähes välttämättömiä. (Rinnemaa 2006.)

Ilman identiteetin- ja pääsynhallintaohjelmistojen käyttöä käyttäjien tiedot pitää lisätä ja poistaa käsin jokaiseen käytettävään järjestelmään. Erillisen identiteetti- ja pääsynhallintaohjelmiston käyttö mahdollistaa tämän prosessin tekemisen automaattisesti. Tämä parantaa erityisesti tietoturvaa. Identiteetin- ja pääsynhallinnan tarkoituksena on varmistaa, että vain tietyt henkilöt voivat päästä käsiksi tiettyihin järjestelmiin ja resursseihin. Identiteetinhallintaohjelmiston käyttö mahdollistaa keskitetyn ja läpinäkyvän hallinnan eri järjestelmien välillä. Koska tieto liikkuu järjestelmien välillä yhden sovelluksen kautta, on virheiden ja väärinkäytöksien jäljittäminen ja seuraaminen huomattavasti helpompaa. Keskitetty identiteetin- ja pääsynhallinta mahdollistaa erilaisten ja toisistaan riippumattomien sovelluksien käyttämisen yrityksen infrastruktuurissa. (Internet2 2007.)

Tiedon synkronoinnin lisäksi useimmat identiteetin- ja pääsynhallintaohjelmistot mahdollistavat erilaisten roolipohjaisten työnkulkujen määrittämisen. Tällöin erilaisia prosesseja, kuten käyttäjän lisääminen järjestelmään, voidaan siirtää yrityksen atk-ylläpidolta itse järjestelmien käyttäjille. Esimerkiksi tieto uudesta työntekijästä menee esimiehelle, joka tiedot tarkastettuaan hyväksyy uuden työntekijän ja näin uusi työntekijä lisätään automaattisesti haluttuihin järjestelmiin. (InformationWeek 2004.)

2.2 Identiteetin- ja pääsynhallinnan käyttökohteet

Identiteetin- ja pääsynhallintaohjelmistojen käytöstä hyötyvät erityisesti keskikokoiset ja suuret yritykset, joissa on useita kriittisiä ohjelmistoja käytössä. Tutkimusyritys Gartnerin mukaan esimerkiksi 10 000 henkilön yrityksessä identiteettihallintaohjelmiston käyttö 12 eri ohjelmiston välillä voi säästää jopa 2,5 miljoonaa euroa vuodessa, mikä aiheutuu muun muassa käyttäjien hallinnoinnista ja helpdesk-palveluista. Erityisesti isoissa yrityksissä on hyötyä esimerkiksi Novell Identity Managerin roolipohjaisen järjestelymoduulin käytöstä, joka mahdollistaa erilaisten tehtävien siirtämisen ja automatisoinnin atk-ylläpidolta itse käyttäjille. Pienemmille yrityksille keskitetystä identiteetin- ja pääsynhallinnasta on hyötyä esimerkiksi erilaisten salasanakäytäntöjen pakottamisesta, joka parantaa tietoturvaa. (InformationWeek 2004.)

Yrityksien lisäksi identiteetin- ja pääsynhallintaohjelmistojen käytöstä on hyötyä muun muassa julkisella sektorilla. InformationWeekin artikkelissa (2004) Bostonin lastensairaalan tietoturva-asiantuntija Scott Lenzi sanoo, että ennen sairaalassa uusien lääkäreiden tai harjoittelijoiden lisääminen kaikkiin järjestelmiin saattoi viedä 8–21 päivää. Sairaalassa työskenteli 30 ylläpitäjää, joiden aika kului käyttäjätilien hallinnoinnissa. Identiteettihallintaohjelmiston käyttöönoton jälkeen uuden käyttätilin lisääminen järjestelmään onnistuu kymmenessä minuutissa. (InformationWeek 2004.)

Identiteetin- ja pääsynhallintaohjelmistosta on hyötyä myös silloin, kun halutaan liittää jokin ohjelmisto osaksi yrityksen infrastruktuuria, jota ei mahdollista suoraa integrointia esimerkiksi Microsoft Active Directoryn tai muun vastaavan hakemistopalvelun kanssa. Myös sellaiset omaa tietokantaa käyttävät ohjelmistot, jotka sisältävät jo olemassa olevan käyttäjähallinnan, voidaan liittää toimivaksi osana yrityksen infrastruktuuria. (InformationWeek 2004.)

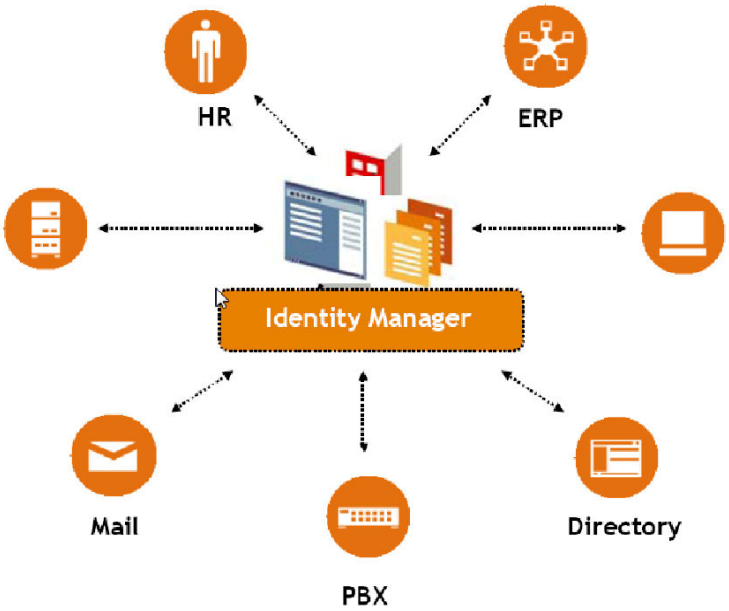
2.3 Kaupallisia identiteetinhallintaohjelmistoja

Nykypäivänä identiteetinhallintajärjestelmien kysynnän kasvaessa markkinoilla on useita tähän tarkoitukseen soveltuvia järjestelmiä. Markkinoilla on muun muassa seuraavia kaupallisia identiteetin- ja pääsynhallintaohjelmistoja

- BMC Identity Management Suite
- CA Identity Manager
- IBM Tivoli Identity Manager
- Oracle Identity Manager
- Sun Java System Identity Manager
- Microsoft Identity and Access Management Series
- Novell Identity Manager.

3 NOVELL IDENTITY MANAGER

Novell Identity Manager on identeetin- ja pääsynhallintaohjelmisto, joka mahdollistaa tiedon siirron ja hallinnoinnin erilaisten järjestelmien välillä keskitetyn tietovarastonsa kautta. (kuva 1). Identity Managerin tietovarastoa kutsutaan nimellä Identity Vault. Identity Manager tarjoaa kaksisuuntaisen rajapinnan ohjelmistojen ja Identity Vaultin välille. Identity Vault koostuu metahakemistomoottorista, joka asetettujen sääntöjen perusteella havaitsee muutokset yhdistettyihin järjestelmiin. Identity Manager mahdollistaa periaatteessa minkä tahansa kytketyn järjestelmän toimimisen koko järjestelmäinfrastruktuurin auktoritatiivisena lähteenä. Esimerkiksi auktoritatiivinen lähde voidaan määritellään toimimaan niin, että tehdyillä muutoksilla vain Microsoft Active Directory -hakemistopalvelussa on merkitystä. Jos muutoksia, kuten käyttäjän poistaminen, yritetään tehdä jossain muussa liitetyssä järjestelmässä, Identity Manager kumoaa nämä muutokset ja palauttaa vanhat arvot tähän järjestelmään. Tieto Identity Managerin ja liitetyn järjestelmän välillä kulkee aina XML-dokumenttien avulla, joka sisältää tiedon siitä, miten objektit ja niiden attribuutin sijoitetaan Identity Managerissa ja kohdejärjestelmässä. (Novell 2008a, 1-2–1-4.)



Kuvio 1. Yleiskuvaus Novell Identity Managerista. (Novell Inc. 2008a, 1-3.)

3.1 Novell eDirectory

Novell eDirectory on skaalautuva hakemistopalvelu, kuten Microsoft Active Directory. Novell eDirectoryn tietovarasto koostuu lukuisista erilaisista objekteista, joita voivat olla esimerkiksi käyttäjät, palvelimet, tulostimet sekä sovellukset. eDirectory pystyy käsittelemään ja hallinnoimaan miljoonia eri objekteja. Novell eDirectory tukee useita käyttöjärjestelmiä kuten: IBM AIX, Linux, Netware, Solaris, Windows ja HP-UX. Novell eDirectory julkaistiin ensimmäisen kerran Linuxille vuonna 2000. eDirectory tukee natiivisti LDAP 3 -protokollaa sekä mahdollistaa TLS/SSL-salauksen. (Novell 2008b, 19.)

eDirectory järjestää eri objektit puurakenteeksi (kuvio 2), jolloin niiden ylläpidettävyys helpottuu. Ylimmäisenä on aina puun nimi, jonka alle eri objektit kerätään. Yleisen mallin mukaisesti ylimmän tason jälkeen seuraavat organisaatiot ja taas niiden alle eri organisaatioyksiköt. Organisaatioyksikkö voi olla yrityksessä jokin tietty osasto kuten hallinto, talous tai myynti. Esimerkiksi myyntiorganisaatioyksikköön voidaan lisätä myyntiyksikössä olevat henkilöt, tietokoneet ja muut laitteet, näin ollen eri objekteja voidaan ryhmitellä selkeisiin kokonaisuuksiin. (Novell 2008b, 20–23.)

Kuvio 2. Yksinkertainen eDirectoryn puurakenne

Kuvion 2 puurakenteessa on kolme eri tasoa. Kuvassa ylimmäisenä on puun nimi, joka on nimetty esimerkissä nimellä "Puu". Seuraavaksi tulee organisaatio-objekti nimeltä "Organisaatio", jonka alle on yksi organisaatioyksikkö nimeltään "Organisaatioyksikkö". Organisaatioyksikön sisällä on listattu ryhmät, käyttäjät ja laiteobjektit.

3.2 Tuetut käyttöjärjestelmät

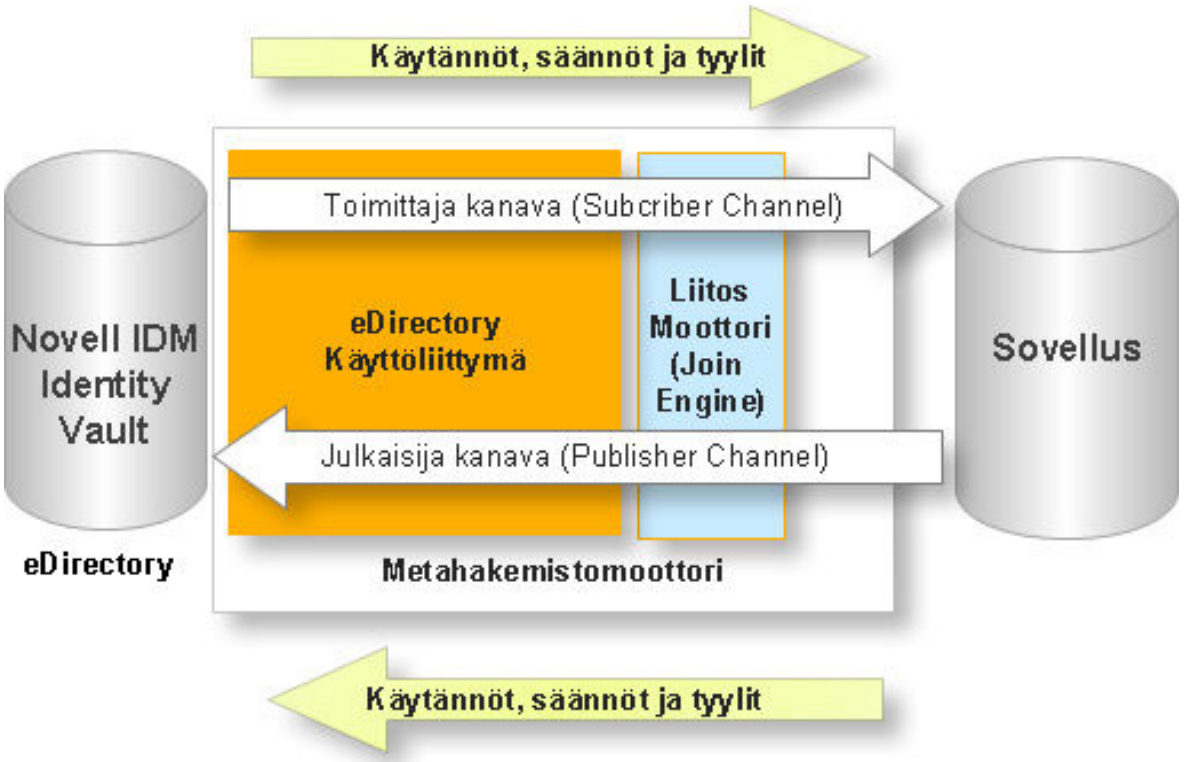
Novell Identity Manager tukee useita eri käyttöjärjestelmiä.

Novell Identity Manager 3.5 toimii ainakin seuraavissa käyttöjärjestelmissä

- NetWare 6.5 (viimeisin Support Pack asennettuna)
- Novell Open Enterprise Server 1.0 (viimeisin Support Pack asennettuna)
- Novell Open Enterprise Server 2.0
- Novell Open Enterprise Server SP1 (32-bittiä)
- Windows Server 2000 (Viimeisin Service Pack asennettuna)
- Windows Server 2003 SP1
- Linux Red Hat 3.0 - 5.0 (32/64 bittiä)
- Suse Linux Enterprise Server 9 ja 10 (32/64 bittiä)
- Solaris 9 ja 10
- AIX 5.2 ja 5.3. (Novell 2007b, 30.)

3.3 Arkkitehtuuri

Identity Manager mahdollistaa datan synkronoinnin Identity Vaultin ja siihen liitettyjen järjestelmien välillä. Liitetyt järjestelmät voivat olla ohjelmia, hakemistoja tai tietokantoja. Metahakemistomoottori käyttää sääntöprosessoria ja tiedonmuunnosmoottoria, kun tieto liikkuu järjestelmien välillä. Kuviossa 3 on kuvattu Identity Managerin yleisarkkitehtuuri. (Novell 2008c, 38.)

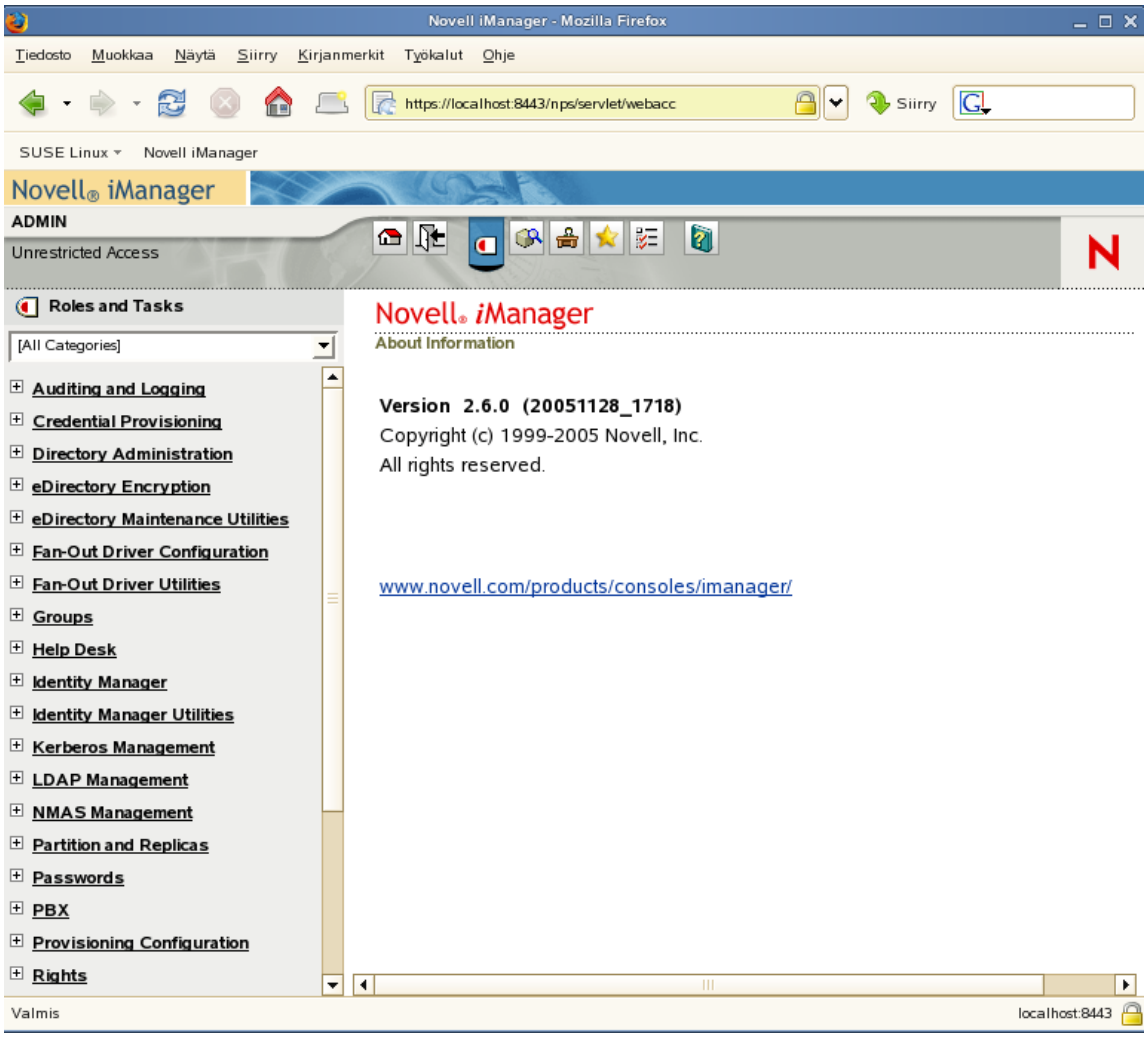


Kuvio 3. Identity Managerin arkkitehtuurikuvaus

Kuvion 3 mukainen arkkitehtuurikuvaksessa kuvataan miten tieto liikkuu Identity Vaultin ja liitetyn järjestelmän eli sovelluksen välillä. Toimittajakanavassa tieto liikkuu aina Identity Vaultista sovellukseen päin ja julkaisijakanavassa toisinpäin. Kanavissa liikkuvaa tietoa voidaan käsitellä monilla eri tavoilla, jotka perustuvat luotuihin käytäntöihin, sääntöihin ja tyyleihin. (Novell 2008c, 39–40.)

3.4 Novell iManager

Novell iManager (kuvio 4) on www-pohjainen sovellus pääosin Novell eDirectoryn hallinnointiin. iManagerin toiminnot perustuvat erilaisiin liitännäisiin, joita kutsutaan myös rooleiksi. Erikseen asennettavien roolien avulla voidaan hallita myös muita Novellin tuotteita, kuten Identity Manageria. (Novell 2009a, 11.)



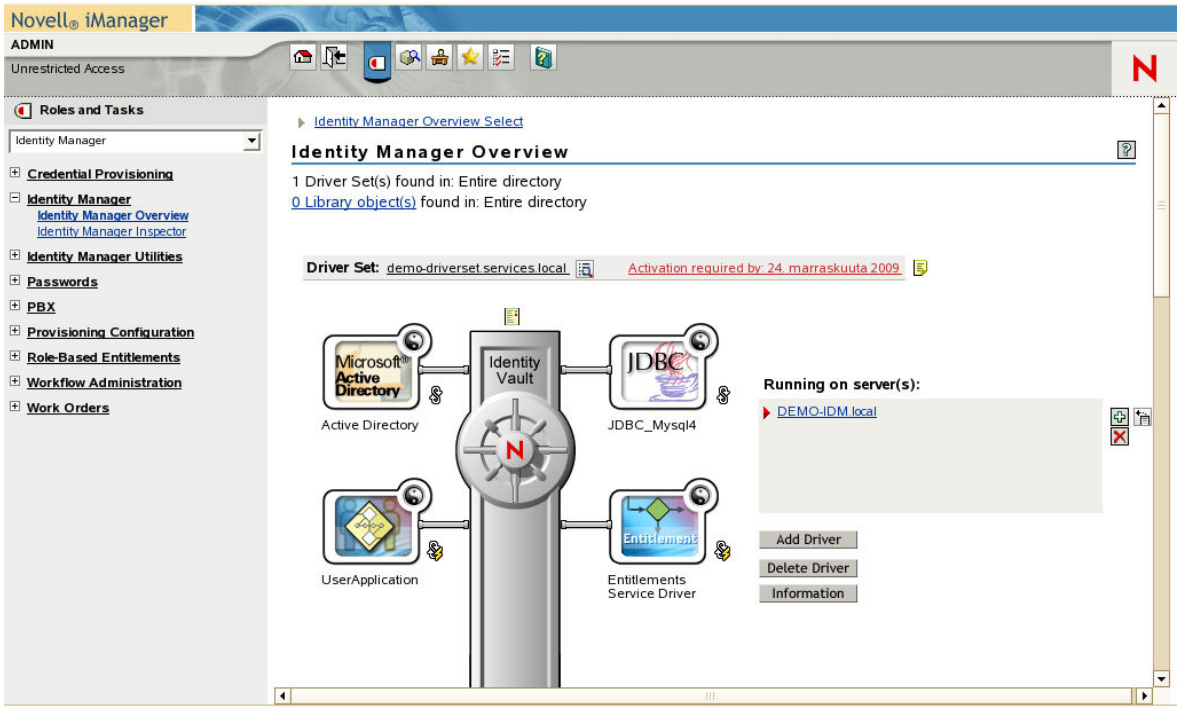
Kuvio 4. Novell iManagerin päänäkymä www-selaimessa.

Kuviossa 4 vasemmalla näkyvät linkit ovat eri rooleja iManagerissa, joiden avulla eri toimintoja voidaan hallita. Esimerkiksi valitsemalla listasta "Identity Manager" -rooli voidaan tarkastella ja hallita asennettuja ajureita Identity Managerissa. Tämän avulla nähdään myös ajureiden tila. Kuviossa 5 on kuvankaappaus Identity Managerin ajurinäkymästä iManagerissa.

Oletuksena mukana tulevat muun muassa seuraavat roolit

- hakemiston hallinnointi (engl. Directory Administration).
- osiot ja replikointi (engl. Partitions and Replicas)
- atk-tuki (engl. Help Desk)
- skeemat (engl. Schema)
- käyttöoikeudet (engl. Rights)

- käyttäjät (engl. Users)
- ryhmät (engl. Groups). (Novell 2009a, 11.)



Kuvio 5. Identity Managerin asennetut ajurit iManagerissa.

Kuviossa 5 on keskellä kuvattu Identity Vault, johon eri ajurit liittyvät. Ajurikuvakkeiden oikeassa yläkulmassa olevia pyöreä ikoni kuvastaa ajurin sen hetkistä tilaa eli onko ajuri on päällä vai ei.

3.5 Identity Manager Designer

Novell Identity Manager Designer on Java-pohjainen suunnittelu- ja hallinnointityökalu Identity Manageria varten. Designer pohjautuu vapaan lähdekoodin Eclipse -kehitystyökaluun. Designer mahdollistaa Identity Managerin ympäristö -toteutuksen suunnittelun, konfiguroinnin sekä testaamisen. Testaaminen mahdollistaa tehtyjen muutoksien simuloinnin työasemalla ennen muutoksien julkaisemista Identity Manageriin. Designerilla voidaan myös tuoda olemassa oleva projekti Identity Managerista ja jatkaa sen käsittelyä Designerissa. Koska Novell Designer

on kirjoitettu Javalla, niin se toimii Windows- sekä Linux-käyttöjärjestelmissä. (Novell 2007c, 6-2; Novell 2008a, 6-5.)

3.6 Novell Identity managerin tärkeimmät komponentit

Novell Identity Manager koostuu useista eri komponenteista. Tässä kappaleessa kuvataan Identity Managerin yleisimmät komponentit, joita ovat:

- Identity Vault
- liitetyt järjestelmät
- metahakemistomoottori
- Driver shim
- julkaisija- ja toimittajakanavat
- säännöt ja suodattimet.

3.6.1 Identity Vault

Identity Vault toimii Identity Managerin tietovarastona. Periaatteessa Novell Identity Manager tarkoittaa samaa asiaa kuin Identity Vault. Identity Vault perustuu eDirectoryyn johon kaikki objektit tallennetaan. Identity Vault on oikestaan vain oma nimitys Identity Managerin tietokannalle eli eDirectorylle. (Novell 2008a, 1-22.)

3.6.2 Liitetyt järjestelmät

Liitetyt järjestelmät ovat niitä järjestelmiä, jotka on liitetty toimimaan Identity Managerin kautta. Järjestelmän liitetään omilla ajureillaan, jotka sisältävät tiedot siitä, miten tieto liikkuu Identity Managerin ja liitetyn järjestelmän välillä. (Novell 2008a, 1-23.)

Novell Identity Manageria voidaan käyttää muun muassa seuraavien järjestelmien kanssa:

- Microsoft Active Directory

- Novell eDirectory
- Exchange 5.5
- Novell GroupWise
- JDBC-tietokanta
- Linux/Unix
- Lotus Notes
- PeopleSoft 3.7 ja 5.7.
- SAP HR. (Novell 2009b.)

Identity Manager sisältää ajurin myös CSV-tiedostoille, joten tavallista tekstitiedostoa voidaan käyttää muiden järjestelmien tapaan (Novell 2008d, 14).

3.6.3 Metahakemistomoottori

Metahakemistomoottori voidaan jakaa kahteen eri komponenttiin: eDirectoryn liittymään sekä liitosmoottoriin. eDirectoryn liittymä on osa metahakemistomoottoria, joka tunnistaa tapahtumat Identity Managerissa. Liittymän tehtävänä on varmistaa, että tieto siirtyy Identity Manageriin. Tapahtumia varten liittymässä on välimuisti (engl. event cache), joka pitää huolen siitä, että kaikki tapahtumat siirtyvät Identity Manageriin, vaikka yhteys liitetyn järjestelmän ja Identity Managerin välillä katkeaisi. Liitosmoottori muokkaa kutsuja Identity Manageriin lisättyjen sääntöjen perusteella. Säännöt luodaan erillisen graafisen käyttöliittymän avulla, joko Designer -ohjelmassa tai iManager-ohjelmalla. Säännöt ovat erillisiä XML-dokumentteja, joten graafinen käyttöliittymä helpottaa niiden luomista ja muokkaamista tavallisen tekstieditorin sijaan. Tekstieditoriakin voidaan halutessa käyttää. (Novell 2008c, 40.)

Liitosmoottorin tehtävät:

- Käsittelee siirrettävän tiedon muutokset
- Käsittelee siirrettävään tietoon liittyvät säännöt
- Prosessoi XSLT-muunnokset. (Novell 2008c, 40.)

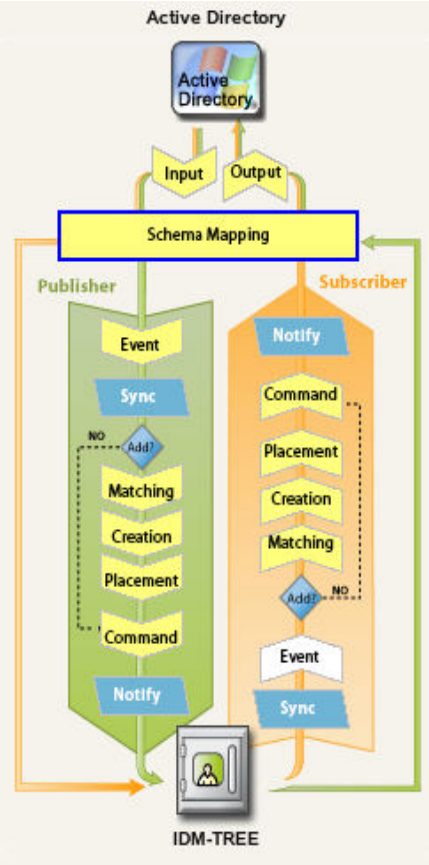
3.6.4 Driver shim

Driver shim on kirjoitettu Javalla, C:llä tai C++:lla. Jotta haluttu järjestelmä saadaan keskustelemaan Identity Managerin kanssa, niin pitää sille olla erillinen ajurinsa. Ajuri koostuu XML-dokumentista, joka sisältää kuvauksen siitä, miten tieto Identity Managerin ja liitetyn järjestelmän välillä siirretään. Dokumentti sisältää muun muassa tiedot siitä miten pyynnöt, haut ja tulokset käsitellään järjestelmien välillä. Kun Identity Vault havaitsee tapahtuman, niin se luo uuden XML-dokumentin tehdyn kyselyn perusteella ja lähettää sen julkaisijakanavaan. Driver shim tukee muun muassa seuraavia tapahtumia eri objekteille: lisääminen, muokkaus, poistaminen, uudelleen nimeäminen, siirtäminen ja salasanan muokkaus. (Novell 2008c, 41.)

Kun kohdejärjestelmä sijaitsee eri palvelimessa kuin Identity Manager, pitää tätä varten asentaa erillinen Remote Loader -ohjelmisto. Remote Loader välittää tiedon Identity Managerin ja kohdejärjestelmän välillä. (Novell 2008a, 1-25.)

3.6.5 Julkaisija- ja toimittajakanavat

Tieto Identity Managerin ja liitetyn järjestelmän välillä kulkee kahdessa eri kanavassa (kuvio 6). Näitä kanavia kutsutaan julkaisija- ja toimittajakanaviksi. Molemmat kanavat ovat yhdensuuntaisia eli julkaisijakanavassa tieto liikkuu liitetystä järjestelmästä Identity Vaultiin ja toimittajakanavassa Identity Vaultista liitettyyn järjestelmään. Kummassakin kanavassa on omat sääntönsä ja suodattimensa tiedon käsittelyä varten. Tästä on kerrottu tarkemmin kohdassa 4.5. (Novell 2008c, 43,45.)



Kuvio 6. Toimittaja- ja julkaisijakanavat

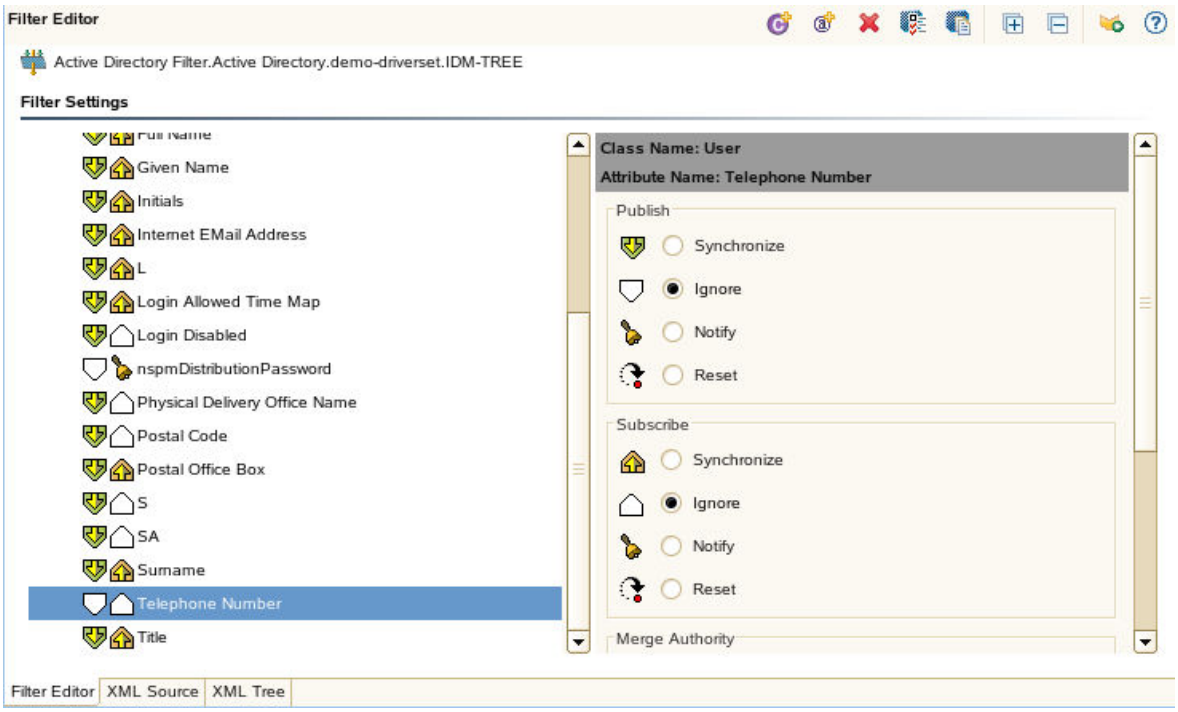
Kuvio 6 on kuvankaappaus Active Directory -ajurin toimittaja- ja julkaisijakanavista Designer-ohjelmassa. Kuviossa näkyy molempien kanavien säännöt sekä suodattimet. Tästä on kerrottu lisää kohdassa 3.8.

3.7 Säännöt ja suodattimet

Julkaisija- ja toimittajakanavat sisältävät erilaisia sääntöjä ja suodattimia kanavissa läpikulkevaa tiedonkäsittelyä varten. Säännöillä ja suodattimilla määritellään miten tietoa käsitellään sen mennessä kanavan läpi. Säännöt ja suodattimet ovat aina ajurikohtaisia. Muutokset voidaan tehdä joko Designer-ohjelmassa tai iManagerissa. (Novell 2008a, 4-2.)

3.7.1 Suodattimet

Suodattimilla voidaan määritellä, mitä tietoa halutaan julkaisija- ja toimittajakanavissa kuljettaa. Esimerkiksi Active Directory ajurissa voidaan estää käyttäjien puhelinnumero-attribuutin siirtyminen Identity Vaultiin. Kuviossa 7 on määritelty Active Directoryn ajuri suodattamaan käyttäjä-objektin puhelinnumero-attribuutti molemmissa kanavissa. (Novell 2008a, 4-3.)



Kuvio 7. Active Directory -ajurin suodattimien muokkaaminen Designerissa

Suodattimien avulla voidaan määritellä myös Identity Manageriin liitettyjen järjestelmien autoratiivinen lähde. Oletuksena tieto liikkuu järjestelmien välillä molempiin suuntiin. Esimerkiksi jos Identity Manageriin on liitetty Active Directory sekä tietokantasovellus ja halutaan Active Directoryn toimivan autoratiivisena lähteenä voidaan asettaa objektit kulkemaan Active Directory ajurissa vain julkaisijakanavaa pitkin ja tietokanta-ajurissa toimittaja-kanavaa pitkin. Näin ollen muutokset virtaavat Active Directorystä Identity Vaultiin ja sieltä taas tietokanta sovellukseen, mutta eivät toisinpäin. Tämän ansiosta tietokanta sovelluksessa tehdyillä muutoksilla ei

ole vaikutusta vaan ainoastaan Active Directorystä käsin voidaan hallita eri objekteja. Tästä hyötyä siinä, että muut järjestelmät eivät sotke toisiaan ja esimerkiksi käyttäjien hallinta on keskitettyä. (Novell 2008a, 4-2–4-5, 4–7.)

3.7.2 Kanavien säännöt

Suodattimien lisäksi kummassakin kanavassa voidaan määritellä joukko haluttuja sääntöjä kanavissa kulkevaa tietoa varten. Kummassakin kanavassa on useita sääntöketjuja, jotka suoritetaan kanavassa aina samassa järjestyksessä. (Novell 2008a, 4-13.)

Julkaisija- ja toimittajakanavissa voidaan määritellä seuraavia sääntöketjuja:

- skeeman kartoitussäännöt
- Tapahtumien muutossäännöt
- tarkistussäännöt
- luontisäännöt
- sijoitussäännöt
- komentojen muunnossäännöt (Novell 2008a, 4-13).

Sääntöjen avulla voidaan muun muassa lisätä halutuilla säännöillä yksilöllisiä tietoja ja luoda oletussalasanoja uusille käyttäjä-objekteille perustuen esimerkiksi käyttäjän nimeen. Säännöt luodaan omalla graafisella sääntöeditorilla, jotka rakennetaan erilaisilla loogisilla lausekkeilla Boolen operaattoreita hyväksi käyttäen. (Novell 2008a, 4-12.)

Skeeman kartoitussäännöt. Skeeman kartoitussääntöihin lisätään tiedot attribuuteista Identity Vaultin ja liitetyn järjestelmän välillä. Säännöt sisältävät kaksi skeemaa, toinen Identity Vaultille ja toinen liitetylle järjestelmälle. Skeeman kartoitussäänöillä kerrotaan Identity Managerille miten samaa tietoa sisältävä attribuutti on nimetty Identity Managerissa ja liitetyssä järjestelmässä. Taulukossa 1 on kuvattu "User"-objektin skeemakartoitus Active Directory -ajurille. (Novell 2008a, 4-18.)

Taulukko 1 User-objektin skeemakartoitus Active Directory ajurille

Selite	**Kentän nimi eDirectoryssä**	**Kentän nimi Active Directoryssä**
Järjestelmä	*Identity Vault*	*Active Directory*
Luokka	User	user
Käyttäjätunnus	DirXML-ADAliasName	sAMAccountName
Toimiston sijainti	L	physicalDeliveryOfficeName
Toimiston sijainti	Physical Delivery Office Name	l
Salasana	nspmDistributionPassword	nspmDistributionPassword

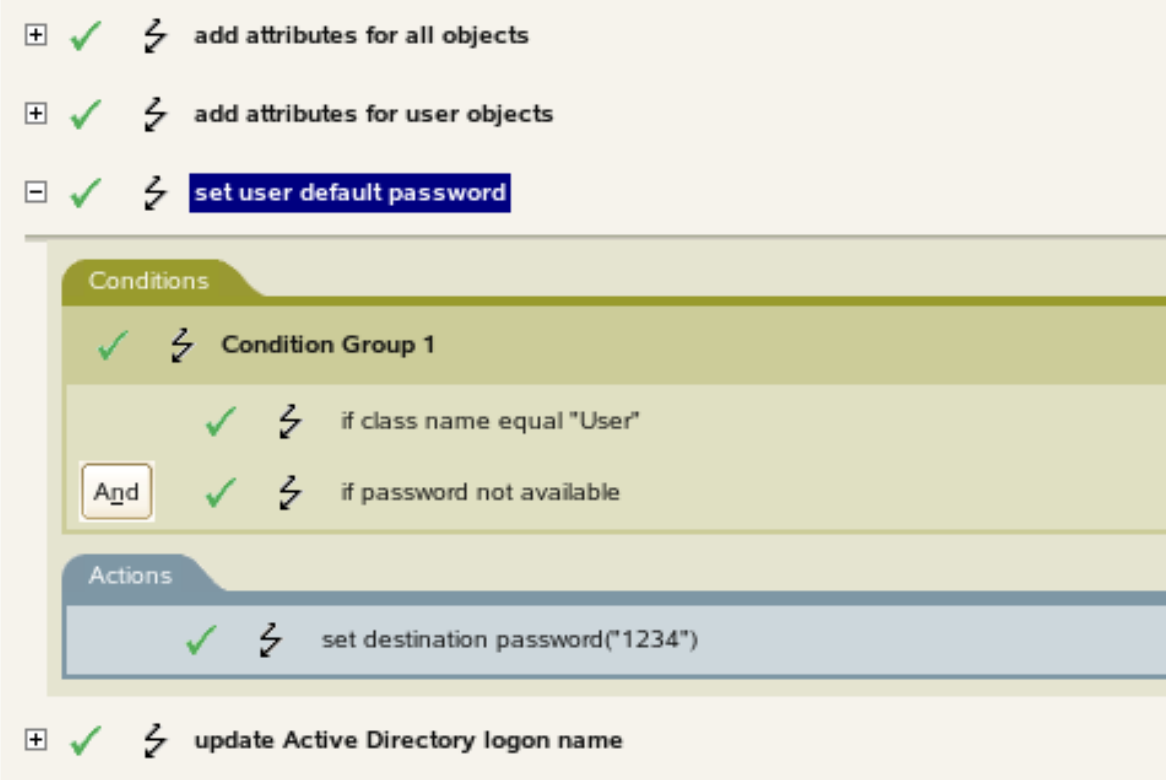
Tapahtumien muutossäännöt. Tapahtumien muutossääntöihin voidaan määritellä sääntöjä, joilla muutetaan Identity Managerin lähettämiä komentoja metahakemistomoottorille. Esimerkiksi objektin poistamiskomento voidaan muuttaa tässä vaiheessa muokkaus tai siirtokomennoiksi. (Novell 2008a, 4-17.)

Tarkistussäännöt. Tarkistussäännöllä tarkistetaan onko lisättävä objekti jo olemassa. Jotta tarkistus voidaan tehdä, niin täytyy objektilla olla jokin yksilöllinen attribuutti kuten sähköpostiosoite objektin tunnistamista varten. Tarkistussääntöjä voidaan lisätä myös useampia, koska esimerkiksi pelkän sähköpostiosoitteen tarkistaminen voi olla hyvin virhealtista. (Novell 2008a, 4-15.)

Luontisäännöt. Luontisäännöt suoritetaan silloin kun tarkistussäännöt eivät täsmää prosessoituun objektiin eli voidaan olettaa, että kyseistä objektia ei löydy. Luontisääntöjen avulla voidaan objektille määritellä erilaisia arvoja eri attribuuteille kuten oletussalasana. Kuviossa 8 on kuvankaappaus Active Directory -ajurin luontisäännöistä. Kuvassa olevan kolmannen säännön kohdalla on kaksi ehtolauseketta uuden käyttäjä-objektin oletusalasanan luomiselle, joka esimerkissä asetetaan merkkijonoksi "1234". Salasana "1234" asetetaan, mikäli luokan nimi on "User" ja salasana-attribuuttia ei ole. (Novell 2008a, 4-13.)

Sijoitussäännöt. Sijoitussäännöillä määritellään nimi ja sijainti uusille objekteille Identity Vaultissa. Sijoitussääntö on pakollinen julkaisijakanavassa objektien luontiin Identity Vaultissa. (Novell 2008a, 4-16.)

Komentojen muunnossäännöt. Komentojen muunnossäännöillä voidaan muuttaa alkuperäinen komento kuten objektin siirtokomento, muokkauskomennoksi (Novell 2008a, 4-17).



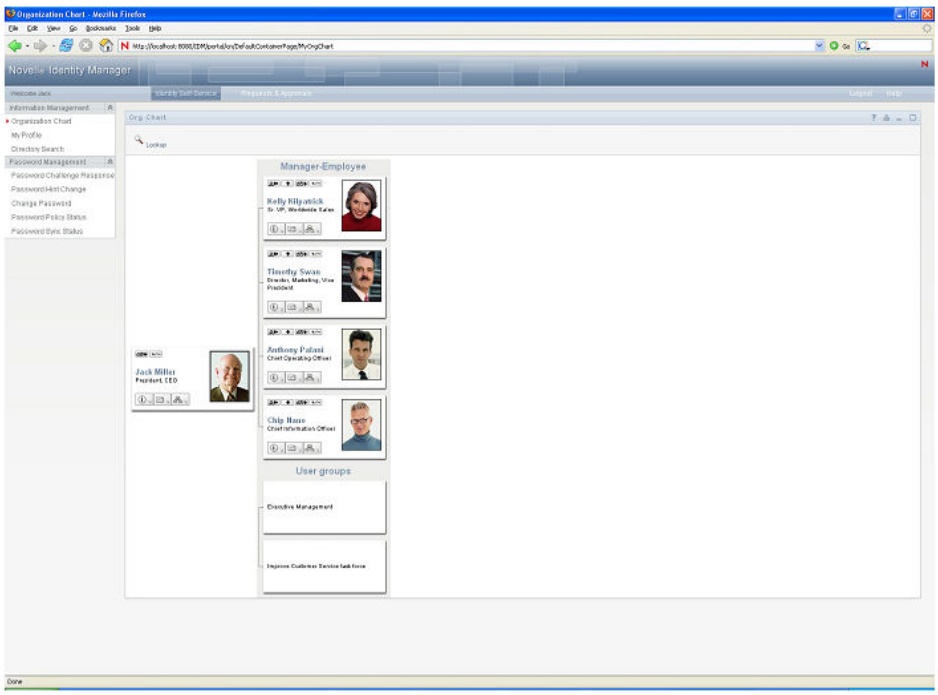
Kuvio 8. Active Directory -ajurin luomissäännöt Designerin sääntöeditorissa.

3.8 User Application

User Application on www-pohjainen loppukäyttäjäsovellus Identity Manageriin. Sovellus on toteutettu Javalla ja toimii JBOSS- tai IBM WebSphere -sovelluspalvelimien päällä. Tietokantana on oletuksena MySQL. User Application tarjoaa graafisen käyttöliittymän muun muassa erilaisille itsepalvelutoiminnoille, kuten käyttäjien omien tietojen muuttamiselle, salasanojen vaihtamiselle jne. Mikäli User Applicationia käytetään yhdessä Provisioning- ja Novell Audit -lisäosien

kanssa, voidaan sillä muun muassa siirtää normaalisti atk-ylläpidolle kuulua tehtäviä loppukäyttäjille erilaisten asiankäsittelykulkujen avulla. (Novell 2007a, 21-23.)

User Application toimii myös niin sanottuna yrityksen sisäisenä puhelinluettelona, koska sen avulla voidaan selata ja hallita Identity Vaultissa sijaitsevia käyttäjiä, joten tiedot Identity Manageriin liitetyistä järjestelmistä löytyvät keskitetysti yhdestä paikasta. Koska käyttäjätasot noudattavat normaalia yrityshierarkiaa, voidaan sovelluksen avulla nähdä yrityksen työntekijähierarkia. Kuvassa 9 on esimerkki User Appicationin yrityshierarkianäkymästä. (Novell 2007a, 21.)



Kuvio 9 Yrityshierarkianäkymä User Application -ohjelmassa.

User Applicationilla on seuraavat edut:

- Siirtää päivittäisiä ylläpitotehtäviä järjestelmän käyttäjille.
- Mahdollistaa käyttäjien omien tietojen muokkaamisen
- Lista sovelluksista joihin käyttäjällä on käyttäoikeus.
- Tuo läpinäkyvyyttä järjestelmien käyttöön.
- Automatisoi tehtäviä automaattisten hyväksyntäkiertojen avulla. (Novell 2007a, 21-22.)

4 NOVELL IDENTITY MANAGER KÄYTÄNNÖSSÄ

Tässä luvussa kerrotaan käytännön kautta Identity Managerin käytöstä ja ominaisuuksista. Luvussa käydään läpi Active Directoryn sekä User Application loppukäyttäjäsovelluksen liittäminen Identity Manageriin.

4.1 Tavoite

Käytännön osuuden tavoitteena on rakentaa ympäristö, jonka avulla hahmotetaan Novell Identity Managerilla tehtävää keskitettyä identiteetinhallintaa. Ympäristö koostuu kahdesta palvelimesta, joista toinen on Linux-palvelin ja toinen Windows Server 2003 -palvelin. Palvelimet asennetaan VMware-virtuaalikoneiksi, joten muuta laitteistoa käytettävän työaseman lisäksi ei käytetä.

Linux-palvelimeen asennetaan Novell Identity Manager 3.5 ja sen käyttämät komponentit kuten Novell eDirectory, Designer sekä iManager. Linux-palvelimeen asennetaan myös User Application, jonka avulla voidaan testata Active Directoryyn lisättyjen käyttäjien toimivuus. User Application voisi sijaita myös toisella palvelimella, koska monen yhtäaikaisen järjestelmän virtualisointi samassa työasemassa vie paljon resursseja, on päätetty asentaa User Application samaan palvelimeen Identity Managerin kanssa.

Toisena palvelimena toimii Windows Server 2003 Standard SP2, johon asennetaan Microsoft Active Directory -hakemistopalvelu Windows Domain -kirjautumista varten. Active Directoryn on tarkoitus toimia ympäristöön liitettävien järjestelmien auktoritatiivisena lähteenä, eli Active Directoryn kautta hallitaan ympäristön käyttäjät ja ryhmät.

4.2 Kohderyhmä ja tarkoitus

Kohderyhmänä ovat kaikki ne, jotka haluavat käytännön esimerkin keskitetyn identiteetin hallinnan toiminnasta Novell Identity Managerin avulla. Käytännön toteutus antaa myös yleisen kuvan keskitetyn identiteetin hallinnan toiminnasta. Windows Server 2003:n sisältämä Active Directory -hakemistopalvelu on käytössä suuressa osaa yrityksiä ja yhteisöjä, joissa käytetään Windows domain-kirjautumista.

4.3 Mitä tarkoittaa virtualisointi?

Virtualisointi mahdollistaa usean yhtäaikaisen käyttöjärjestelmän ajamisen samassa fyysisessä järjestelmässä. Virtualisoinnin avulla voidaan ajaa esimerkiksi Windows käyttöjärjestelmän päällä eri Linux versioita. Fyysistä järjestelmää kutsutaan Host- eli isäntä-järjestelmiksi ja virtualisoituja järjestelmiä Guest- eli vierasjärjestelmiksi. Virtualisoinnissa jokainen vierasjärjestelmä on oma itsenäinen järjestelmänsä, joten virtualisoidut järjestelmät eivät voi sotkea toisiaan tai isäntä järjestelmää vaikka yksi tai useampi virtualisoitu järjestelmä kaatuisi. (VMware [viitattu 4.7.2009].)

Virtualisoinnin tehokkuus perustuu siihen, että virtualisointiohjelmisto, kuten tässä opinnäytetyön käytännön ympäristössä käytetty VMWare jakaa fyysisen järjestelmän resurssit kuten prosessorin, keskusmuistin ja kiintolevyn kapasiteetin tasaisesti kaikille virtuaalikoneille käytettäväksi. VMWaren lisäksi muita virtualisointiohjelmistoja on esimerkiksi Citrixin Xen, Microsoftin Virtual PC sekä Sun Microsystemsin VirtualBox. (VMware [viitattu 4.7.2009].)

4.4 Laitteisto ja ohjelmistot

Ympäristö asennetaan tavalliseen työasemaan. Työasema asetetaan VMWaressa samaan verkkoon, jotta saadaan verkkoyhteys käytössä oleviin virtuaalikoneisiin. Työasemalla ip-osoitteeksi asetetaan 192.168.148.2. Työasema toimii samalla

myös yhdyskäytävänä, joka mahdollistaa Internet-yhteyden jakamisen virtuaalikoneille.

Työaseman järjestelmätiedot

- Intel E6750 Prosessori (2 ydintä)
- 6 GT keskusmuistia
- Windows Vista Premium, 64-bittinen.
- VMware Workstation versio 6.5.2.

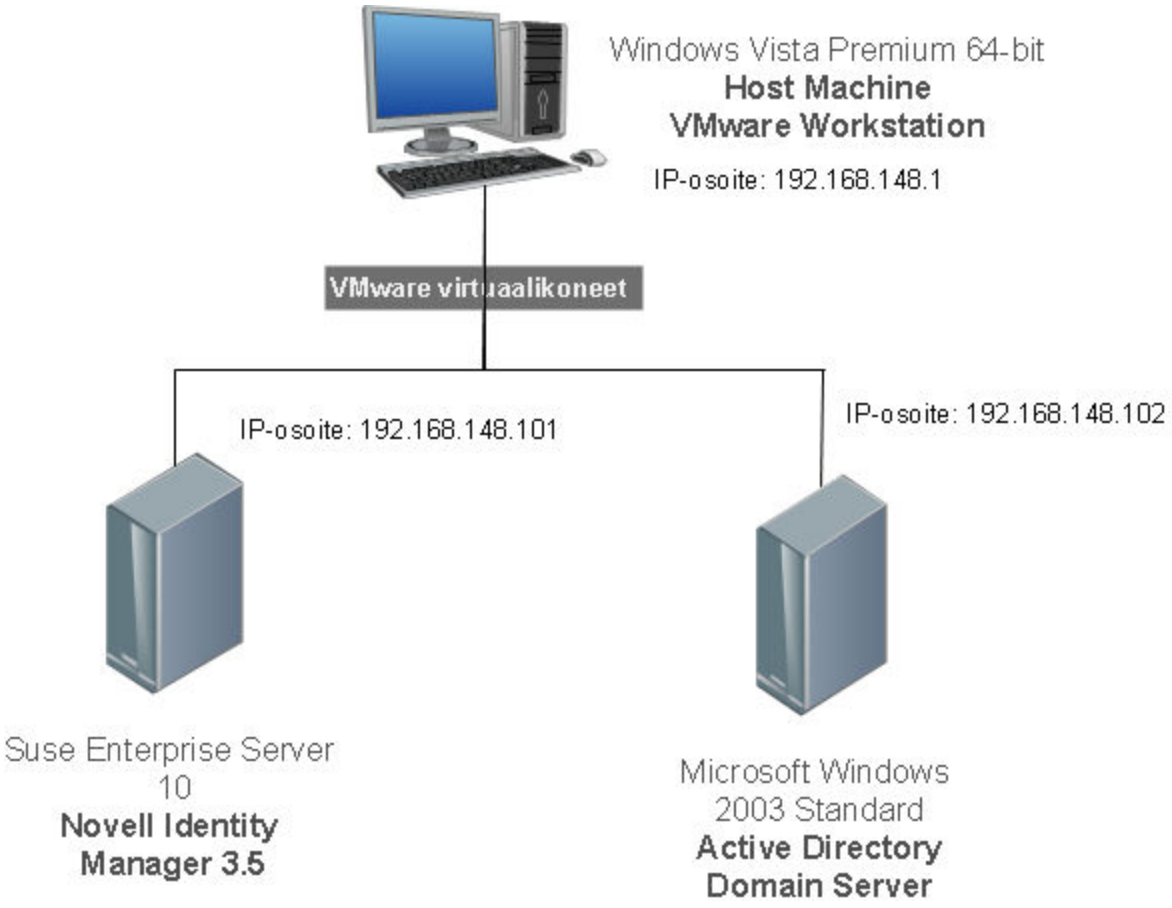
4.5 Vaiheet

Ympäristössä ei keskitytä itse käyttöjärjestelmien tai sovelluksien asennukseen, vaan käyttöjärjestelmät on asennettu valmiiksi, kuitenkin Novell IDM:n konfiguroinnin vaiheita tarkastellaan hieman tarkemmin. Projekti voidaan jakaa neljään eri vaiheeseen

1. Suunnitteluvaihe
2. Asennusvaihe
3. Määrittelyvaihe
4. Testaaminen

4.6 Suunnittelu

Ympäristön kaksi palvelinta asennetaan VMWare–virtuaalikoneiksi. Kumpaankin virtuaalikoneeseen varataan keskusmuistia 512 MT sekä kiintolevytilaa 8 GT. Palvelimet konfiguroidaan samaan verkkoon ja työryhmään nimeltä DEMOWORKGROUP. Novell Identity Manager 3.5 palvelimen nimeksi tulee DEMO-IDM, Windows Server 2003 Standard -palvelimen nimeksi DEMO-AD (kuvio 10).



Kuvio 10. Ympäristön arkkitehtuuri.

4.6.1 Identity Manager -palvelin

Novell Identity Manager palvelimen käyttöjärjestelmänä on Suse Enterprise Linux 10. Palvelimelle varataan keskusmuistia 512 megatavua ja nimeksi asetetaan DEMO-IDM sekä ip-osoitteeksi 192.168.148.101.

Palvelimeen asennettavat ohjelmistot:

- Identity Manager 3.5 sekä asennuskomponentit:
  - metahakemistomoottori
  - eDirectory -ajuri
  - Identity Manager liitännäiset iManageria varten
- User Application sekä tarvittavat asennuskomponentit:
  - JBOSS–sovelluspalvelin
  - MySQL 5 -tietokantapalvelin

4.6.2 Active Directory palvelin

Active Directory palvelin asennetaan Windows Server 2003 Standard SP2 -käyttöjärjestelmään. Palvelimelle varataan keskusmuistia 512 megatavua. Palvelimen nimeksi asetetaan DEMO-AD sekä ip-osoitteeksi 192.168.148.102.

Active Directory palvelimeen asennetaan ohjelmistot:

- Active Directory
- Remote loader

4.6.3 Ajureiden sääntömäärittelyt

Tavoitteena on saada säännöt toimimaan siten, että muutokset mihin hyvänsä järjestelmään päivittyvät Identity Vaultiin ja sitä kautta muihin järjestelmiin. Salasanakäytäntö luodaan siten, että mikäli uudelle käyttäjäobjektille ei ole salasanaa määritelty, niin sille luodaan uusi salasana "demo". Mikäli käyttäjä kuuluu johonkin ryhmään, niin siirtosääntöihin lisätään sääntö, että käyttäjä lisätään Identity Vaultissa kyseisen ryhmän jäseneksi.

4.6.4 Käyttäjätunnuksien nimeäminen

Käyttäjätunnuksiin käytetään yhtenäistä nimeämistapaa. Kolmi-merkkinen käyttäjätunnus koostuu käyttäjä etunimen kahdesta ensimmäisestä ja sukunimen ensimmäisestä kirjaimesta. Esimerkiksi henkilön Kari Lehtinen käyttäjätunnus on tällöin "kal". Koska oletuksena Active Directoryssä ei sallita alle 7 merkin pituista salasanaa, Active Directoryn salasanakäytäntöä muutetaan siten, että hyväksytään 4 merkkiä pitkät salasanat. (Novell 2007c, intro-13.)

4.6.5 Käyttäjät ja ryhmät

Ympäristössä luodaan myös yksi organisaatioyksikkö DEMO, johon palvelimen käyttäjät ja ryhmät lisätään. Active Directoryyn luodaan käyttäjäryhmä Accounting. Ryhmään luodaan kolme kuvitteellista käyttäjää.

Identity Managerissa ryhmille ja käyttäjille luodaan omat organisaatioyksiköt, jotta ryhmä- ja käyttäjäobjektien hallinta helpottuisi. Ylimmäiseksi organisaatioyksiköksi lisätään Vault. Ryhmät sijoitetaan "Group"-organisaatioyksikköön. Käyttäjiä varten luodaan "Users"-organisaatioyksikkö, jonka alle aktiivisia käyttäjiä varten luodaan organisaatio nimeltään "active" ja ei-aktiivisia käyttäjiä varten "Inactive"-organisaatioyksikkö.

4.7 Asentaminen

Tässä kappaleessa kuvataan ympäristön palvelimien asennusvaiheet. Ympäristöön asennetaan kaksi palvelinta: DEMO-AD ja DEMO-IDM.

4.7.1 DEMO-AD-palvelin

DEMO-AD–palvelimeen asennetaan järjestyksessä seuraavat roolit ja ohjelmistot:

- Active Directory
- DNS-palvelin
- DHCP-palvelin
- Identity Manager Remote Loader -ohjelmisto.

Roolien asentaminen. Ensimmäiseksi palvelimeen asennetaan Active Directory hakemistopalvelu. Active Directoryn asennuksen yhteydessä asennetaan myös vaadittavat DNS-palvelin sekä DHCP-palvelin, vaikka näitä ei sinällään vaadita ympäristön toiminnan kannalta.

Remote Loader asennus. Jotta Active Directorya voidaan käyttää Identity Managerin kanssa, pitää sitä varten asentaa erillinen Remote Loader -ohjelmisto. Remote Loader saadaan asennettua Identity Managerin asennusmedialta kun asennuksessa valitaan vain asennettavaksi paketit "Novell Identity Manager Connected System" ja "Utilities". *(*Novell 2007c, WB 7-2–WB 7-3.)

Salasanojen synkronointi. Active Directoryn käyttäjille määritettyjen salasanojen synkronointi Identity Vaultiin saadaan aktivoitua, kun Active Directoryyn otetaan erillinen salasanojen suodatustoiminto käyttöön. Suodatustoiminto määritetään Remote Loader -ohjelmiston mukana tulevalla Identity Manager PassSync -ohjelmalla. Ohjelmalle annetaan domainin- ja Active Directory -palvelimen nimi. *(*Novell 2007c, WB 8-12.)

4.7.2 DEMO-IDM -palvelin

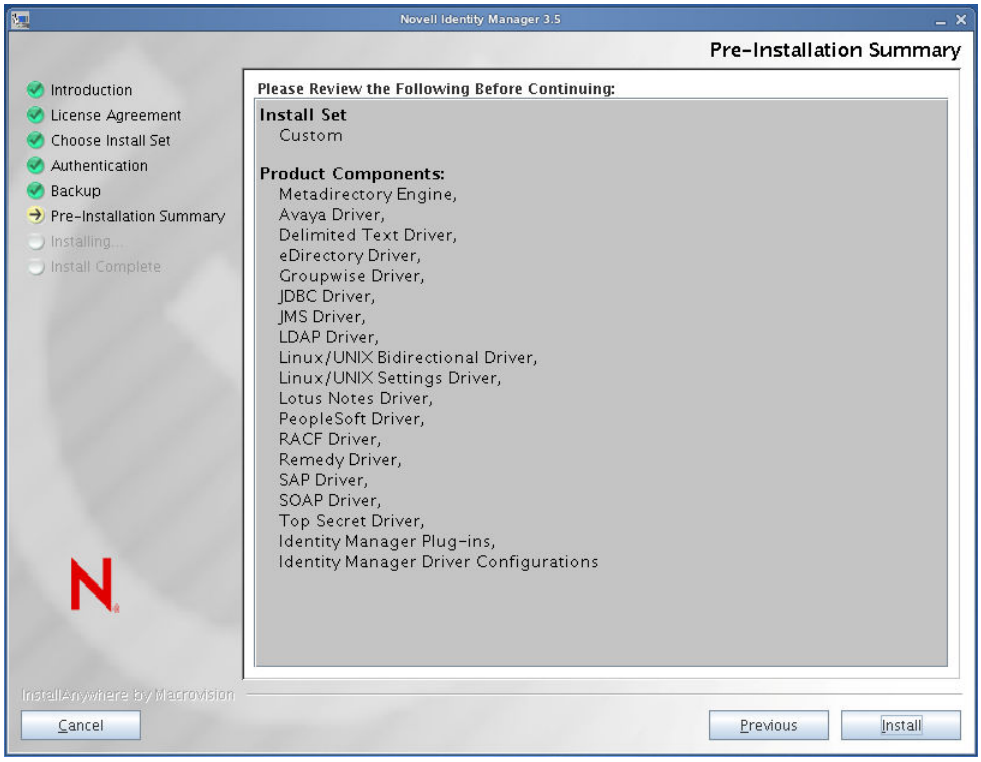
DEMO-IDM-palvelimeen asennetaan järjestyksessä seuraavat ohjelmistot

- Novell eDirectory 8.8
- Novell Identity Manager 3.5
- JBOSS sovelluspalvelin ja MySQL tietokantapalvelin.
- User Application.

Novell eDirectoryn asennus. Asennus aloitetaan asentamalla Suse Linux Enterprise 10 palvelimelle Novell eDirectory ohjelmisto. eDirectory on pohjana Identity Managerille, mutta ei sinällään vielä toimi Identity Managerin kanssa, vaan siihen asennetaan tarvittavat laajennukset, kuten Security Services, joka on saatavilla ilmaiseksi Novellin kotisivuilta. Tässä ympäristössä käytetään versiota 2.0.6. Security Services -laajennuksen asentamisen jälkeen pitää eDirectoryn skeemat vielä päivittää ajan tasalle. (Novell 2007c, WB 2-12–WB 2-17.)

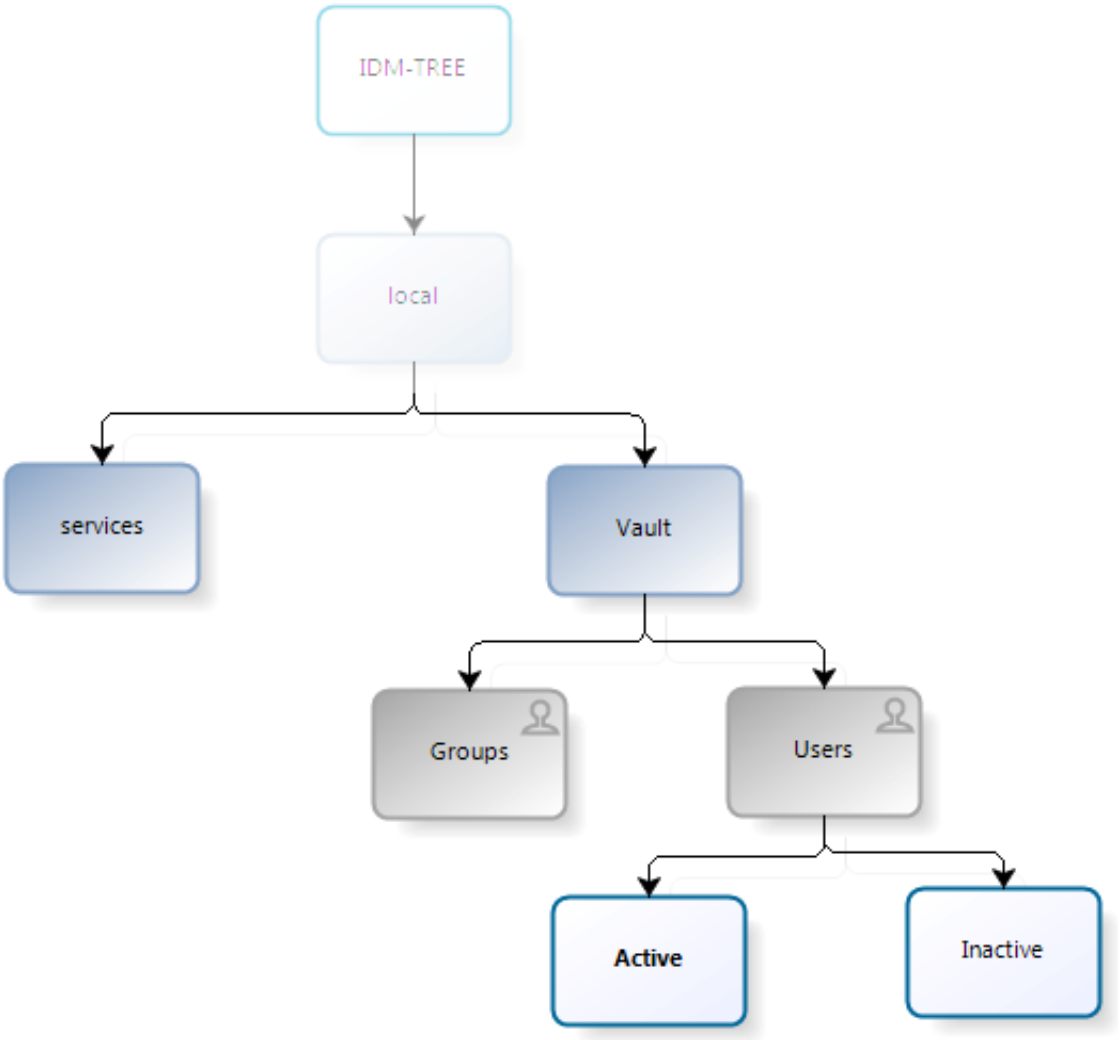
eDirectoryn määrittely. eDirectoryyn puun nimeksi annetaan "IDM-TREE". Organisaatioksi "Local", jonka alle eri organisaatioyksiköt lisätään. Puun polku on kokonaisuudessaan IDM-TREE.demo.local.

Identity Managerin asennus. Identity Managerista asennetaan 90-päivän kokeiluversio, jonka jälkeen se tulee rekisteröidä. Asennukseen valitaan metahakemistomoottori, kaikki saatavilla olevat ajurit sekä Identity Manager -lisäosat iManageria varten (kuvio 11).



Kuvio 11. Identity Managerin asennusikkuna.

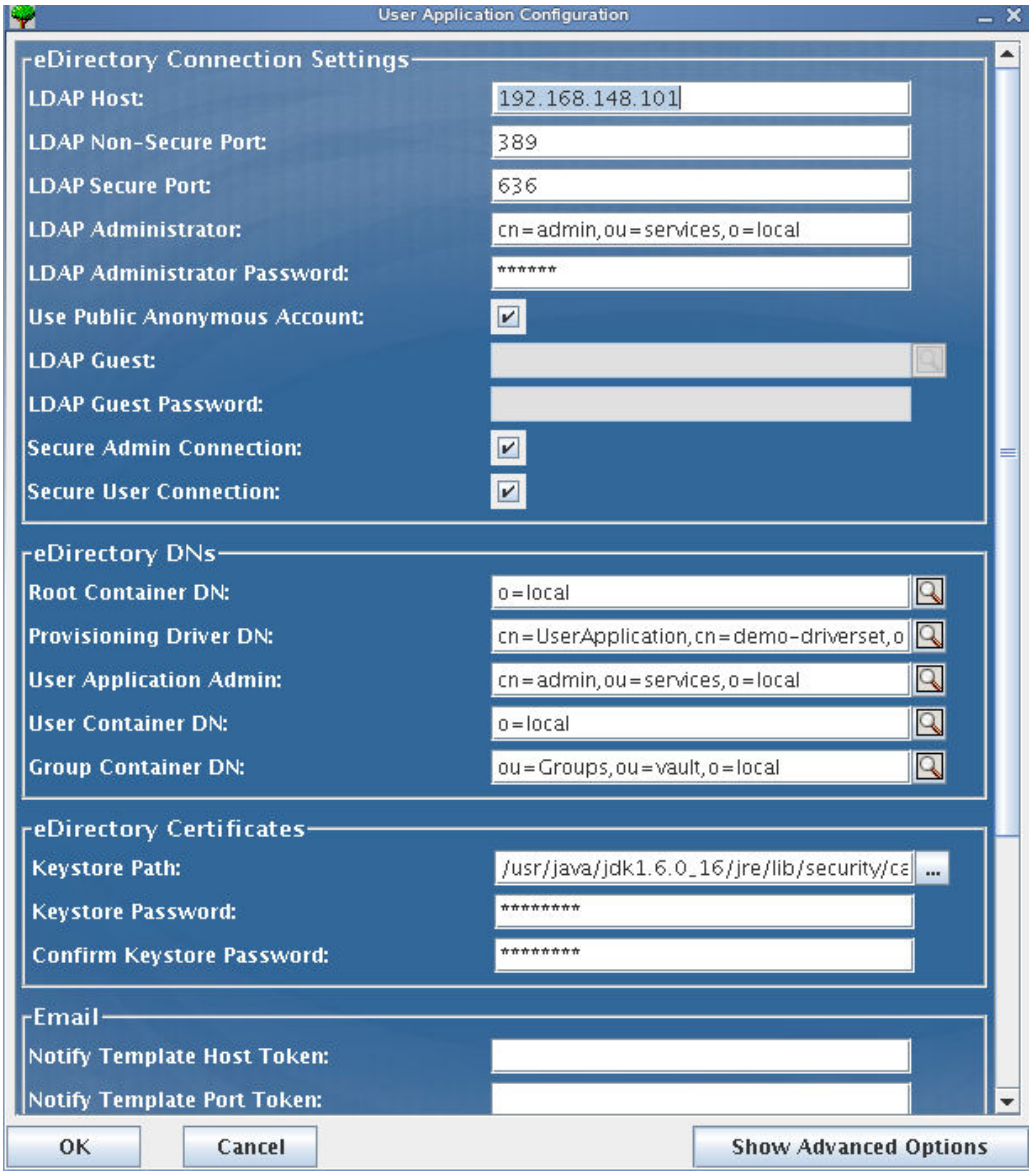
Käyttäjäryhmien ja käyttäjien sijaintien määrittely. Kun Identity Manager on asennettu, kirjaudutaan iManageriin, jossa määritellään tarvittavat organisaatioyksiköt puurakenteeseen. Organisaatioyksiköt lisätään kuvion 12 mukaisesti iManager-sovelluksen avulla. Kuvion 12 mukaisesti esimerkiksi aktiivisien käyttäjien sijainnin polku on IDM-TREE.local.Vault.Users.Active. Ryhmät sen sijaan sijoitetaan aina polkuun IDM-TREE.local.Vault.Groups.



Kuvio 12. Ympäristön puurakenne

User Application asennus. User Application asennetaan omasta asennusohjelmastaan. Ennen User Application sovelluksen asennusta tulee Identity Manageriin asentaa ajuri User Applicationia varten Designerissa tai iManagerissa. Ajurin asentamisen ja käyttöönoton jälkeen Asennusohjelman mukana asennetaan samalla myös JBOSS-sovelluspalvelin sekä MySQL 5 -tietokantapalvelin. Asennusohjelmalle kerrotaan root-käyttäjän salasana sekä haluttu tietokannan nimi, johon asennusohjelma asentaa User Applicationin käyttämät tietokantataulut. Asennusohjelmalla kerrotaan myös haluttu polku asetuksille. JBOSS sovelluspalvelin asennetaan käyttämään porttia 8081. (Novell 2007c, WB 2-12–WB 2-17.)

Kuviossa 13 on ympäristöä varten määritetyt asetukset User Applicationin käyttöönottoon.



Kuvio 13. User Applicationin asennusparametrit

Kuvio 13 sisältää esimerkin User Applicationin asennusparametreista. Asetukset sisältävät muun muassa pääkäyttäjän sijainnin Identity Managerissa (LDAP Administrator), sekä käyttäjien (User Container DN) ja ryhmien sijainnin (Group Container DN). (Novell 2007c, WB 9-13.)

Novell Designer for Identity Manager asentaminen. Designerista asennetaan versio 2.0. Designerin asennus käynnistetään omasta asennusohjelmasta, muita vaiheita Designerin käyttöönottoon ei tarvita. Designer on ladattavissa myös ilmaiseksi Novellin verkkosivuilta.

Ajureiden asentaminen ja konfigurointi Designer ohjelmassa. Ajureiden asentaminen ja määrittely on helpointa tehdä Designer-ohjelmassa, vaikka samaan lopputulokseen päästään myös käyttämällä Novell iManageria. Designerin hyöty on siinä, että muutokset voidaan tehdä ja testata ennen kuin ne julkaistaan Identity Manageriin, jonka jälkeen muutokset astuvat heti voimaan palvelimella. (Novell 2007c, WB 6-8.)

Active Directory -ajurin asentaminen. Active Directory -ajuri asennetaan valitsemalla Designerin ajurivalikosta Active Directory -ajuri. Tämän jälkeen määritellään yhteysasetukset kuten domainin nimi sekä tieto siitä suoritetaanko ajuri paikallisesti vai ei. Koska Active Directoryä ei ole asennettu samalle palvelimelle niin valitaan ajuri suoritettavaksi etänä. Taulukossa 2 on kuvattu Active Directory -ajurin olennaisimmat yhteysparametrit. Yksi olennainen parametri on asettaan ryhmien sijoittelu synkroniseksi. Tämän avulla Identityt Manager lisätä uuden käyttäjän aina sille kuuluvaan ryhmään Identity Vaultissa.

Taulukko 2. Active Directory -ajurin yhteysparametrit

Ajurin Nimi	Active Directory
Autentikaatio metodi	Negotiate
Autentikaatio Id	Administrator
Autentikaatiosalasana	demo
Autentikaatiokonteksti	DEMO-AD.demo.local
Domainin nimi	dc=demo, dc=local
Domain DNS nimi	demo.local
Ajurin päivitysväli	1 sekunti
Salasanan synkrointi	5 minuuttia
Osoite ja portti	192.168.148.102:8092
Käyttäjien sijainti eDirectoryssa	Active.Users.Vault
Käyttäjien sijainti Active Directoryssa	cn=users,dc=demo,dc=local
Tiedon kulkusuunta	Bi-Directional
Ryhmien määrittäminen	Synkroninen

Active Directory -ajurin sääntömäärittelyt. Sääntömäärittelyihin voidaan käyttää Active Directory -ajurin oletusasetuksia, joiden avulla tietojen siirtoa voidaan testata.

User Application -ajurin asentaminen. User Applicationin käyttöönottoa varten pitää asentaa Identity Manageriin oma ajuri. Asennus Designer ohjelmassa etenee Active Directory ajurin tapaan. Ajurille annetaan parametreina pääkäyttäjän tunnus, joka on tässä ympäristössä admin.services.local sekä portin numero 8081.

Salasanojen synkronoinnin käyttöönotto. Salasanojen synkronointi järjestelmien välillä saadaan käyttöön aktivoimalla "Universal Password" -toiminto Identity Managerissa. Universal Password otetaan käyttöön iManager-sovelluksen kautta. Oletuksena Identity Managerissa on salasanapolitiikka jo esikonfiguroitu, joten riittää, että salasanapolitiikka aktivoidaan halutulle käyttäjäryhmälle. Salasanapolitiikka saadaan aktivoitua iManagerissa Authentication -roolin alla olevasta Password policies -linkistä. (Novell 2007c, WB 8-5.)

4.8 Testaaminen

Tässä kappaleessa testataan toteutuksen toimivuus kohdan 4.6 mukaisen suunnitelman pohjalta. Kappaleessa tarkistellaan myös testaamisen myötä ilmenevät tulokset eli toteutuksen toimivuus käytännössä.

4.8.1 Miten testataan

Järjestelmän toiminta testataan lisäämällä DEMO-AD-palvelimen Active Directoryyn yksi käyttäjäryhmä nimeltä "Accounting". Seuraavaksi Active Directoryyn lisätään muutama käyttäjä ja tarkastellaan, päivittyvätkö lisätyt käyttäjät ja ryhmät automaattisesti myös Identity Vaultiin eli DEMO-IDM-palvelimelle.

Testaamisen vaiheet:

1. Lisätään ryhmä "Accounting" Active Directoryyn.
2. Lisätään 3 käyttäjää Active Directoryyn sekä lisätään käyttäjät "Accounting"-ryhmään.
3. Tarkastellaan iManagerin avulla ovatko käyttäjät ja ryhmät päivittyneet automaattisesti Identity Vaultiin DEMO-IDM-palvelimella.
4. Päivitetään käyttäjien tietoja Active Directoryssa ja ja tarkastellaan iManagerin avulla muutokset.
5. Kirjaudutaan yhdellä Active Directoryyn lisätyllä käyttäjällä User Applicationiin.

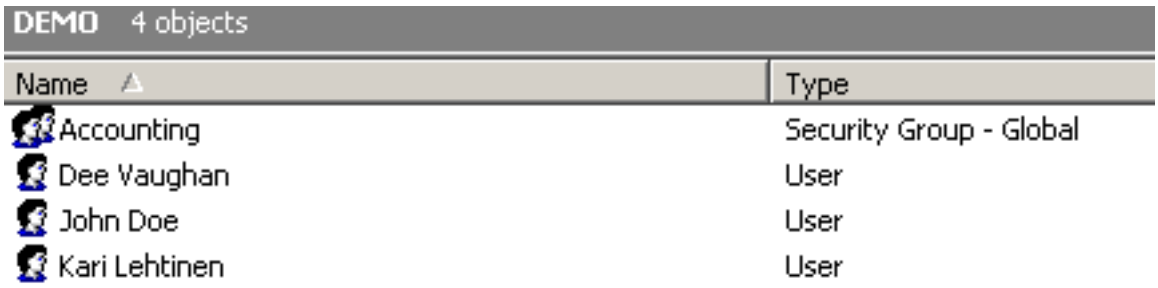
4.8.2 Käyttäjien ja ryhmien lisääminen Active Directoryyn

Ensimmäiseksi lisätään ryhmä "Accounting" DEMO-AD-palvelimen Active Directoryyn. Ryhmän lisäämisen jälkeen lisätään kuvitteelliset käyttäjät taulukon 3 mukaisesti.

Taulukko 3. Active Directoryyn lisättävät käyttäjät

Käyttäjätunnus	**Käyttäjän nimi**
jod	John Doe
dev	Dee Vaughan
kal	Kari Lehtinen

Tämän jälkeen, kun käyttäjät on lisätty Active Directoryyn, niin lisätään käyttäjät vielä "Accounting"-ryhmään.

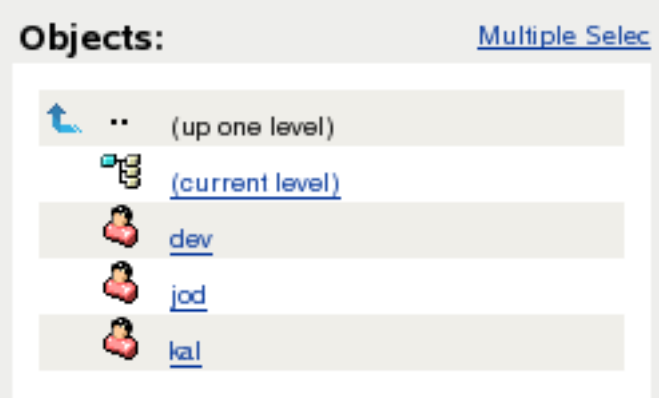


Kuvio 14. Käyttäjät ja ryhmä Active Directoryssa

Kuviossa 14 on näkymä lisätyistä käyttäjistä Active Directoryyn.

4.8.3 Lisättyjen käyttäjien ja ryhmien tarkasteleminen iManagerissa

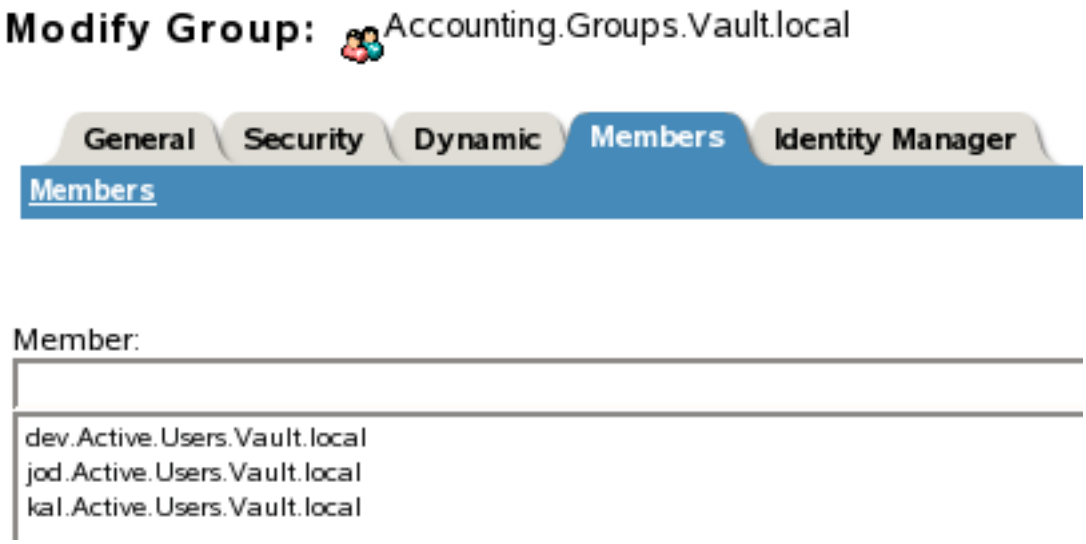
Kun halutut objektit on lisätty Active Directoryyn, voidaan niitä tarkastella DEMO-IDM-palvelimessa iManager-sovelluksen avulla. Käyttäjäobjekteja voidaan selailla iManagerin käyttöliittymästä löytyvällä "view object" -painikkeen kautta. Kuvassa 13 on kuvankaappaus Vault.Users.Active-organisaatioyksikössä olevista objekteista kohdassa 4.8.2 Active Directoryyn lisättyjen käyttäjien osalta. Tämän perusteella voidaan päätellä, että käyttäjät ovat päivittyneet halutulla tavalla Identity Manageriin. (Novell 2009a, 17.)



Kuvio 15. Käyttäjä-objektit Identity Managerissa

Kuvion 15 perusteella nähdään, että käyttäjät ovat päivittyneet oikein Identity Manageriin.

Tämän jälkeen tarkastellaan ovatko käyttäjä-objektit päivittyneet oikein "Accounting"- käyttäjäryhmään. Ryhmiä ja niiden tietoja voidaan tarkastella iManagerissa Groups -roolin avulla. Tämän avulla voidaan nähdä muun muassa ryhmään liitetyt käyttäjät eli jäsenet. Tässä tapauksessa kaikkien 3 käyttäjän pitäisi kuulua Accountiing -ryhmään. Kuvassa 14 on näkymä Accounting ryhmän jäsenistä.



Kuvio 16. Accounting-ryhmän jäsenet

Kuvan 16 mukaisesti Accounting-ryhmään lisätyt käyttäjät ovat päivittyneet oikein Identity Manageriin.

4.8.4 Käyttäjätietojen päivittäminen Active Directoryssä

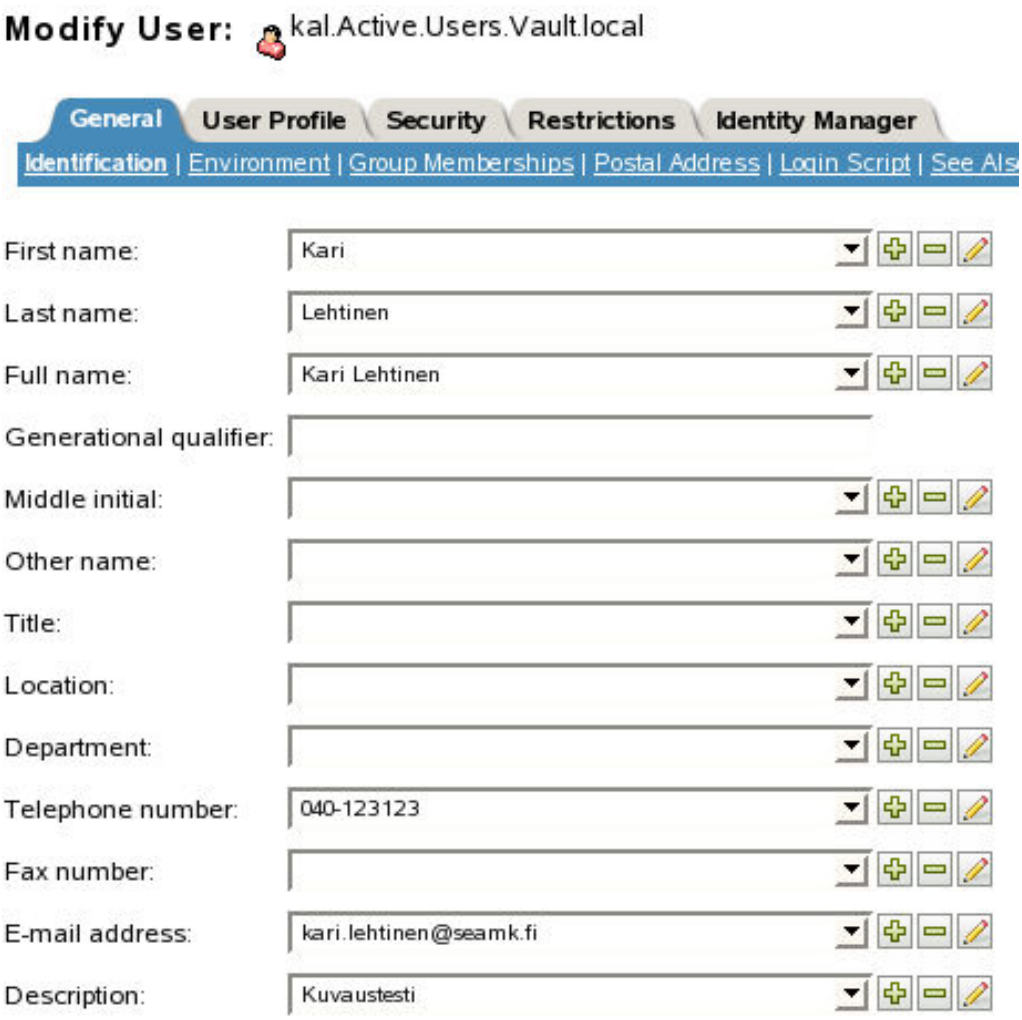
Seuraavaksi päivitetään kohdassa 4.8.2 lisätyn käyttäjän "kal" käyttäjätietoja Active Directoryssä. Käyttäjän tietoihin päivitetään tiedot taulukon 4 mukaisesti.

Taulukko 4. Käyttäjän "kal" päivitettävät tiedot Active Directoryyn

Kentän nimi	**Arvo**
Puhelinnumero (Telephone number)	040-123123
Sähköpostiosoite (E-mail)	kari.lehtinen@seamk.fi
Kuvaus (Description)	Kuvaustesti

4.8.5 Käyttäjätietojen tarkastelu iManagerissa

Kun kohdan 4.8.4 mukaiset tiedot on päivitetty Active Directoryssä, voidaan käyttäjän tietoja tarkastella iManagerissa. Käyttäjän arvoja voidaan selata "Users"-roolin avulla. Kuviossa 17 on kuvattu kohdassa 4.8.4 päivitettyjen tietojen muutoksia iManagerissa. (Novell 2009a, 49.)

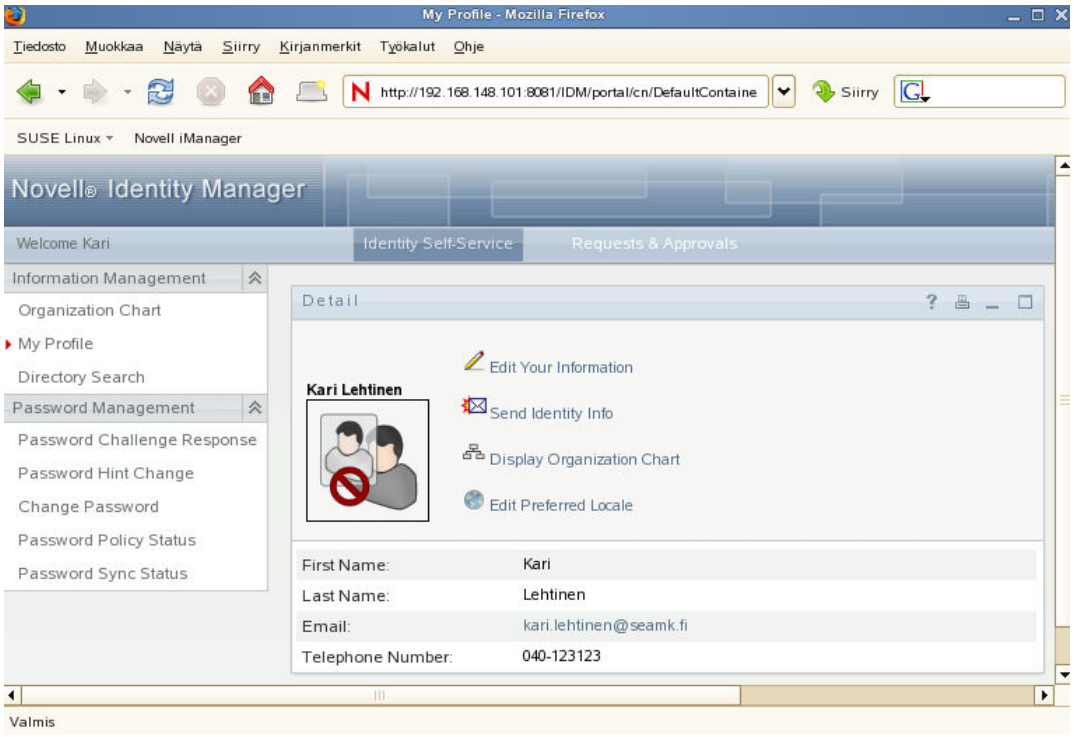


Kuvio 17. Käyttäjä-objektin tietojen tarkastelu iManagerissa.

Kuvion 17 perusteella voidaan todeta, että käyttäjän "kal" tiedot ovat päivittyneet oikein Identity Manageriin.

4.8.6 Käyttäjän kirjautuminen User Applicationiin

Seuraavaksi testataan käyttäjän "Kari Lehtinen" kirjautumista User Applicationiin. User Applicationiin kirjaudutaan tunnuksella "kal" ja määritetyllä salasanalla "demo". Kuviossa 18 tarkastellaan käyttäjän tietoja User Applicationissa.



Kuvio 18. Käyttäjän tiedot User Application -sovelluksessa.

Kuvion 18 perusteella voidaan todeta, että käyttäjän tiedot ovat päivittyneet oikein Active Directorysta ja ne on nähtävissä ja muokattavissa myös User Application sovelluksen kautta. Sovelluksen kautta nähdään käyttäjä-objektin attribuutteja kuten nimi, sähköpostiosoite ja puhelinnumero.

5 JOHTOPÄÄTÖKSET

Opinnäytetyön tavoitteena oli tutkia identiteetin- ja pääsynhallinnan tarkoitusta, hyötyjä sekä tutkia paremmin Novellin identiteetin- ja pääsynhallinnan ratkaisua Novell Identity Manageria. Keskitetty identiteetin- ja pääsynhallinta helpottaa useita ylläpitotehtäviä sekä parantaa tietoturvaa. Tänä päivänä keskitetyn identiteetin- ja pääsynhallinnan ratkaisuja on kaupallisella puolella useita. Useimmat identiteetin- ja pääsynhallinnan ratkaisut ovat periaatteeltaan samanlaisia, joten valinta eri järjestelmien perusteella ei ole kovin yksiselitteinen. Identiteetin- ja pääsynhallinnan ratkaisua harkitessa vaikuttavatkin muun muassa hinta, ympäristön vaatimukset sekä järjestelmän käyttötuki.

Novell Identity Manager on laaja identiteetin- ja pääsynhallinnan ohjelmisto, joka mahdollistaa monipuolisen keskitetyn identiteetin- ja pääsynhallinnan. Johtuen Identity Managerin suuresta koosta voi sen mahdollisuuksien kartoittaminen sekä käyttöönotto olla aluksi hankalaa. Riippuen kohdeympäristön vaatimuksista voidaan kuitenkin pienellä työllä saada toimiva ympäristö aikaan. Tämän opinnäytetyön perusteella voidaan todeta, että suurimmaksi haasteeksi Identity Managerin käyttöönotossa tulee sääntöjen- ja suodattimien määrittely.

Opinnäytetyön käytännön osuuden tavoitteet saatiin toteutettua suunnitellusti. Tavoitteena oli rakentaa pieni ympäristö, jossa Microsoft Active Directory liitetään toimimaan Novell Identity Managerin kanssa. Ympäristössä oli tavoitteena myös tutustua Novell User Applicationin toimintaan ja tarkastella ympäristön toimivuutta tämän kautta. Ennen opinnäytetyön aloittamista oli tarkoitus ottaa yhtenä järjestelmänä mukaan MySQL-tietokantaa hyödyntävä sovellus, jolla oltaisiin voitu testata Identity Managerin toimivuutta sellaisen järjestelmän kanssa johon ei ole mitään esikonfiguroituja ajurimäärityksiä. Tietokantasovellusta ei kuitenkaan saatu liitettyä, koska tietokantapalvelimessa vaadittavaa Java pohjaista Remote Loaderia ei saatu toimimaan. Remote Loaderin käynnistyksen yhteydessä ei saatu mitään virheilmoituksia, joten toimimattomuuden syytä oli hyvin vaikea selvittää.

LÄHTEET

InformationWeek. 2004. The Need for Identity Management. [Verkkosivusto]. InformationWeek. [Viitattu 22.4.2009]. Saatavana: http://www.informationweek.com/news/infrastructure/showArticle.jhtml?articleID=18312163

Internet2. 2007. Identity and Access Management. [Verkkojulkaisu]. [Viitattu 14.3.2009]. Saatavana: www.internet2.edu/pubs/200703-IS-MW.pdf

Novell, Inc. 2007a. Identity Manager User Application: Administration Guide. [Verkkojulkaisu]. [Viitattu 11.9.2009]. Saatavana: http://www.novell.com/documentation/idm35/pdfdoc/agpro/agpro.pdf

Novell, Inc. 2007b. Novell Identity Manager 3.5.1: Installation Guide. [Verkkojulkaisu]. [Viitattu 11.9.2009]. Saatavana: http://www.novell.com/documentation/idm35/pdfdoc/install/install.pdf

Novell, Inc. 2007c. Novell Identity Manager 3.5. Administration Workbook. Course 3091. Version 1. Provo: Novell, Inc.

Novell, Inc. 2008a. Novell Identity Manager 3.5. Administration Manual. Course 3091. Version 1. Volume 1. Provo: Novell, Inc.

Novell, Inc. 2008b. Novell eDirectory 8.8 SP3 Administration Guide. [Verkkojulkaisu]. [Viitattu 8.9.2009]. Saatavana: http://www.novell.com/documentation/edir88/pdfdoc/edir88/edir88.pdf

Novell, Inc. 2008c. Novell Identity Manager 3.5 - SP1 Advanced Technical Training. Novell, Inc. 2008. Provo: Novell, Inc.

Novell, Inc. 2008d. Novell Identity Manager Driver for Delimited Text. Implementation Guide. [Verkkojulkaisu]. [Viitattu 11.9.2009]. Saatavana: http://www.novell.com/documentation/idm35drivers/pdfdoc/delimited/delimited.pdf

Novell, Inc. 2009a. Novell iManager 2.7.3: Administration Guide. [Verkkosivu]. [Viitattu 11.9.2009]. Saatavana: http://www.novell.com/documentation/imanager27/

Novell, Inc. 2009b. Identity Manager Drivers: Connected Systems. [Verkkosivu]. [Viitattu 11.9.2009]. Saatavana: http://www.novell.com/products/identitymanager/drivers/

Rinnemaa, T. 2006. Identiteetinhallinta tuo uusia palasia infrakerrokseen. [Blogimerkintä]. Helsinki: Tietoviikko. [Viitattu 14.3.2009]. Saatavana: http://www.tietoviikko.fi/blogit/analyytikon_ikkuna/article133769.ece

VMware. Virtualization Basics. [Verkkosivu]. [Viitattu 4.7.2009]. Saatavana: http://www.vmware.com/technology/virtualization.html