Mikko Nieminen

Turva- ja Find-Me-tulostuksen suunnittelu ja käyttöönotto

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

26.3.2015

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Mikko Nieminen Turva- ja Find-Me-tulostuksen suunnittelu ja käyttöönotto 50 sivua + 2 liitettä 26.3.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Tietotekniikkapäällikkö Mikael Lampe Yliopettaja Janne Salonen

Insinöörityö kertoo turvatulostusratkaisun suunnittelusta ja asennuksesta asiakas- ja henkilökuntaympäristöön. Työssä tulostusjärjestelmä integroidaan osaksi monitahoista tietoteknistä toimintaympäristöä, joka koostuu lukuisista eri palvelimista ja järjestelmistä. Tavoitetilan saavuttamiseksi työssä hyödynnetään tulostusjärjestelmän lisäksi myös esimerkiksi välityspalvelinta sekä SQL Server -integraatiopalveluita. Insinöörityö tehtiin Helsingin kaupunginkirjastolle.

Työ etenee järjestyksessä käymällä läpi ensin työssä käytetyt tärkeimmät teknologiat. Tämän jälkeen esitellään loogisella tasolla nykyinen toimintaympäristö, johon järjestelmä asennetaan sekä lopuksi kuvataan palvelun tuottamiseen liittyvien järjestelmien asetukset niiltä osin, kun ne liittyvät tulostuspalveluun.

Insinöörityötä tehtäessä havaittiin, että testissä käytetty Papercut-tulostuksenhallintaohjelmisto ei vastannut ominaisuuksiltaan kaikkiin kaupunginkirjaston tarpeisiin. Puutteita löydettiin mm. selainkäyttöliittymän muokattavuudessa. Ongelma ratkaistiin hyödyntämällä palvelun julkaisemisessa käytetyn Citrix Netscaler -palvelimen kehittyneitä sisällönmuokkausominaisuuksia. Testeissä löydettiin myös keino toteuttaa henkilökunnan kertakirjautuminen järjestelmään hyödyntämällä sovelletusti WebAuth-protokollaa ja Kerberos-tunnistusta. Järjestelmän toimintaa analysoitaessa havaittiin myös järjestelmän tietoturvaan liittyvä puute PIN-koodin salauksessa, jonka tuotteen valmistaja ratkaisi tukipalvelupyynnön perusteella. Tulosten ja havaintojen perusteella toteutettiin Helsingin kaupunginkirjastolle tulostuksenhallintajärjestelmä asiakas- ja henkilökuntaympäristöön.

Avainsanat	Tulostus, Papercut, SSIS, Netscaler

Author(s) Title Number of Pages Date	Mikko Nieminen Design and implementation of a secure Find-Me printing system 50 pages + 2 appendices 26 March 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Networks
Instructor(s)	Mikael Lampe, IT Manager Janne Salonen, Principal Lecturer

The purpose of this thesis was to build a self-service printing system test environment for Helsinki City Library. The printing system was integrated into a complicated IT-environment consisting of many IT-services and servers. To achieve the goals for the project it was necessary to use many techniques and technologies already available at the customer's operating environment such as proxy servers and SSIS packages.

This study is based on performing practical test on the Papercut printing system. The study also covers other IT technologies such as SQL Server Integration Services and Citrix Netscaler virtual appliance.

It was found that the Papercut printing system itself could not fulfill all the requirements for a printing system set by Helsinki City Library. These requirements included the customization of the printing system's website layout and integration into the library's other IT systems. These missing features were resolved with Citrix Netscaler and SQL Server Integration services. It was also found that a request for a single sign-on into administrative interface for staff members can be solved with WebAuth technology.

This study was successful in building an effective printing management system for staff members and customers at Helsinki City Library.

Keywords	Printing, Papercut, SSIS, Netscaler

Sisällys

Lyhenteet

AD	Active Directory, Aktiivihakemisto. LDAP-protokollaan perustuva Microsoftin keskitetty käyttäjä- ja asetushakemisto.
BYOD	Bring Your Own Device. Työskentelytapa, jossa työntekijä voi työnantajan luvalla käyttää omia IT-laitteitaan työn tekemiseen.
CS	Content Switching Server. Netscaler-palvelimen Content Switching -virtuaali-isäntäpalvelin.
HTTP	Hypertext Transfer Protocol. Web-sivustojen tiedonsiirrossa käytetty protokolla
HTML	Hypertext Markup Language. Web-sisällön kuvauskieli.
LB	Load Balancing. Netscaler palvelimen kuormanjako-virtuaali-isäntäpalvelin.
OSI	Osi-malli. Lyhenne sanoista Open Systems Interconnection Reference Model. Malli kuvaa tiedosiirrossa käytetyn protokollapinon seitsemässä kerroksessa.
SNIP	Netscaler Subnet IP. IP-osoite, jota Netscaler käyttää lähdeosoitteena muodostettaessa tcp/ip yhteyksiä taustapalveluihin.
SSL	Secure Sockets Layer. Salatuissa http-yhteyksissä käytetty protokolla.
SSIS	SQL Server Integration Services. SQL Server -integraatiopalvelin.
SSO	Single Sign-On. Kertakirjautuminen.
SQL	Structured Query Language. Kieli, jolla voidaan suorittaa kyselyjä relaatiotietokantoihin.
VIP	Netscaler Virtual IP. Netscalerin IP-osoite, johon asiakasohjelma muodostaa yhteyden.

XML	Extensible Markup Language. Rakenteellinen tiedon kuvauskieli.

1 Johdanto

Turvatulostus tarjoaa yrityksille mahdollisuuden tulostaa arkaluonteista tietoa yhteisissä tiloissa oleville keskitetyille tulostimille. Järjestelmien perusajatuksena on, että tulosteet odottavat keskitetyllä tulostuspalvelimella jonossa ja ne saadaan tulostimesta vasta, kun tulostaja on kirjautunut tulostinlaitteelle omalla käyttäjätunnuksellaan. Valtaosa tulostuksenhallintajärjestelmistä nojaa johonkin olemassa olevan käyttäjähakemiston, kuten Microsoft Aktiivihakemiston varaan. Tällöin tulosteen vapauttamiseksi käyttäjän on tiedettävä oma käyttäjätunnus ja salasana käyttäjähakemistossa kuten Microsoftin Aktiivihakemistossa. Vaihtoehtoisesti järjestelmät tarjoavat mahdollisuuden käyttää tunnistuksessa lähiluettavia tunnisteita, jotka on linkitetty käyttäjätunnukseen.

Turvatulostusratkaisut tarjoavat usein myös mahdollisuuden erilaisiin lisämahdollisuuksiin, kuten Find-Me -tulostukseen, jossa tuloste voidaan noutaa miltä tahansa järjestelmän piirissä olevalta tulostinlaitteelta. Lisäksi järjestelmät tarjoavat esimerkiksi mahdollisuuden seurata ja rajoittaa tulostusmääriä.

Uusimpana trendinä on viime aikoina ollut myös mahdollisuus niin sanottuun sähköpostitulostukseen. Tämä on joustava tapa tulostaa tiedostoja silloin, kun tulostajan tietokone ei ole yrityksen omassa keskitetyssä hallinnassa tai halutaan tulostaa tiedostoja mobiililaitteilta kuten älypuhelimista. Monet tulostinvalmistajat ovat kehittäneet omia palvelujaan mahdollistamaan ns. pilvitulostuksen. Monet näistä ratkaisuista on suunnattu kuluttajamarkkinoille tai ne on rajattu toimimaan vain valmistajan omissa laitteissa, eivätkä ne siksi sovellu ympäristöön, jossa käytetään usean eri valmistajan tulostin- ja monitoimilaitteita.

Tässä insinöörityössä sovelletaan eri tunnistusteknologioita mahdollistamaan erilaisten asiakastyyppien kirjautuminen järjestelmään niin keskitetyssä hallinnassa olevilta työasemilta kuin myös yrityksen ulkopuolisilta laitteilta. Palvelun web-käyttöliittymää muokataan sen puutteiden ja lisätoiminnallisuuksien saamiseksi erillisellä reverse proxy -palvelimella, sekä yhdistetään käyttäjä- ja toimikorttitietoja useista eri tietolähteistä.

2 Teknologioiden kuvaus

2.1 Yleiset teknologiat ja standardit

Aktiivihakemisto

Aktiivihakemisto eli Active Directory on Windowsin käyttäjä- ja asetustietokanta, jonka avulla hallitaan Windows-toimialueen käyttäjiä sekä käyttäjien ja työasemien asetuksia ryhmäkäytäntöjen avulla.

DMZ

Demilitarized Zone eli demilitarisoitu alue on aliverkko, johon tyypillisesti sijoitetaan yrityksen web-palvelimet, jotka tarjoavat palveluita Internetiin. (Demilitarisoitu alue (tietotekniikka) 2015).

DNS

Verkkoon kytketyt laitteet kommunikoivat keskenään ip-osoitteiden avulla. Jotta osoitteiden muistaminen olisi helpompaa, voidaan numeeristen ip-osoitteiden tilalle käyttää helposti muistettavia verkkonimiä. DNS-protokollan avulla tcp/ip -tekniikkaa hyödyntävät ohjelmistot ja käyttöjärjestelmät voivat selvittää verkkotunnusta vastaavan ip-osoitteen. (DNS 2014).

HTTP-protokolla

HTTP-protokolla on yleisesti internetliikenteessä käytetty standardi tiedonsiirtoprotokolla. Standardi on määritelty RFC-dokumenteissa 1945 (versio 1.0) sekä 2616 (versio 1.1). Protokolla määrittelee, kuinka asiakas ja palvelin keskustelevat keskenään, mutta ei ota kantaa tietosisältöön. HTTP-protokollan avulla voidaankin siis siirtää mitä tahansa sisältöä. Yleisimmin http-protokollaa käytetään Internetsivustojen kuvauskielen HTML:n siirtämiseen

Protokolla määrittelee metodit, joita asiakassovellus voi käyttää sisällön pyytämiseen sekä vastauskoodit pyyntöihin. Nämä tiedot sisältyvät http-pyynnön otsikkoon.

Otsikkoon sisältyy myös joukko muita parametri=arvokenttiä. Otsikoita voidaan myös luoda itse, mikäli niille on tarvetta. HTTP-protokolla sijoittuu OSI-mallissa kerrokselle 7 eli on sovellusprotokolla. (Hypertext Transfer Protocol 2015).

HTML-kuvauskieli

HTML on avoimeen standardiin perustuva web-sivustojen kuvauskieli. HTML:n avulla voidaan paitsi määrittää sivuston asiasisältöä, kuten tekstiä niin myös tekstin rakennetta ja tyyliä. HTML-sivuston esittämisestä vastaa Web-selain, joka tulkitsee HTML-kuvauksen ja muuntaa sen käyttäjälle näkyväksi web-sivuksi.

TCP/IP

TCP/IP-protokollasta puhuttaessa tarkoitetaan OSI-mallin kerroksille 3(ip) ja 4(tcp) sijoittuvia protokollia, jotka huolehtivat tiedon siirrosta ja siirron luotettavuudesta. Kumpaakin käytetään usein palomuurien pääsylistojen määrittelyissä.

Virtuaalijono

Tulostinjono vastaanottaa tulostustyön. Jono ei ole määritetty mihinkään tulostinlaitteeseen, vaan sinne saapuvat työt ohjataan fyysisiin tulostimiin kohdennettuihin tulostinjonoihin. Virtuaalijono mahdollistaa mm. Find-Me-tulostuksen.

EMF-formaatti

Enhanced Metafile on Windowsin oletustulostusformaatti. Se on tulostimen mallista riippumaton, ja siksi se voidaan tulostaa hyvinkin erilaisilla tulostimilla. EMF-tuloste on aina ennen tulostimelle lähettämistä konvertoitava tulostimen ymmärtämään muotoon käyttäen tulostimen ajuria. Tällöin suurin työkuorma kohdistuu tulostuspalvelimeen (Print processors and data types).

RAW -formaatti

RAW-tulostusformaatti on suoraan tulostimen ohjaimen avulla muodostettu tiedosto, joka voidaan lähettää sellaisenaan tulostimelle. Tulostus- eli spool-tiedoston luonti tapahtuu suoraan tulostavassa työasemassa eikä sitä ole tarpeen muuttaa

tulostuspalvelimella erikseen tulostimen ymmärtämään muotoon. RAW-formaatin käyttäminen kuormittaa tulostavan työaseman prosessoria toisin kuin EMF-formaatin käyttäminen, jossa suurin työkuorma kohdistuu tulostuspalvelimelle (Print processors and data types).

WebAUTH

WebAuth on Stanfordin yliopiston kehittämä protokolla, jonka avulla käyttäjä voidaan tunnistaa selain-pohjaisiin järjestelmiin suorakirjautumisena. Järjestelmässä WebKDC-palvelin suorittaa käyttäjän tunnistuksen paikallisesti tuetulla tunnistusmenetelmällä ja välittää tämän jälkeen käyttäjän autentikointitiedon resurssipalvelimelle salatussa muodostta hyödyntämällä selaimen otsikkotietoja sekä evästeitä. (Schemers ym. 2014).

2.2 Netscaler Application Delivery Controller

Netscaler ADC on fyysinen laitteisto tai virtuaalilaite, joka tarjoaa mm. OSI-mallin tason 4 kuormanjakopalveluita, reverse proxy -toiminnallisuutta, verkkoliikenteen optimointia sekä VPN-palveluita.

Content Switching

Content Switching on Netscaler ADC:n ominaisuus, jonka avulla laitteelle saapuva http, sql tai nimipalvelupyyntö voidaan ohjata sääntöpohjaisesti eri taustajärjestelmiin. Tekniikan avulla voidaan mm. esittää eri taustajärjestelmien sisältöä käyttäjälle saman url-osoitteen takaa. Toiminto tarjoaa myös tavan konsolidoida ip-osoitteita siten, että useampi eri järjestelmä voi käyttää yhtä julkista ip-osoitetta.

Content Rewrite

Content Rewrite on ominaisuus, jonka avulla Netscaler ADC voi muokata mm. laitteen läpi kulkevan http-liikenteen otsikkotietoja sekä http-protokollan välittämää sisältöä. Ominaisuus ei rajoitu ainoastaan http-protokollan käsittelyyn, mutta sen muut käyttömahdollisuudet ovat tämän insinöörityön ulkopuolella.

Traffic Management Load balancing server

Traffic Management Load Balancing server (LB-server) on virtuaali-isäntäpalvelin, jota voidaan käyttää jakamaan kuormaa yhden tai useamman samaa web-palvelua, sovellusta tai resurssia tarjoavan sovelluspalvelimen välillä. LB-palvelin tarjoaa kuormanjako-ominaisuuden lisäksi mahdollisuuden optimoida verkkoliikennettä, muokata liikenteen sisältöä sekä tarjota vikasietoisuutta taustajärjestelmän vikatilanteissa. (Load Balancing).

2.3 Papercut MF -tulostusjärjestelmä

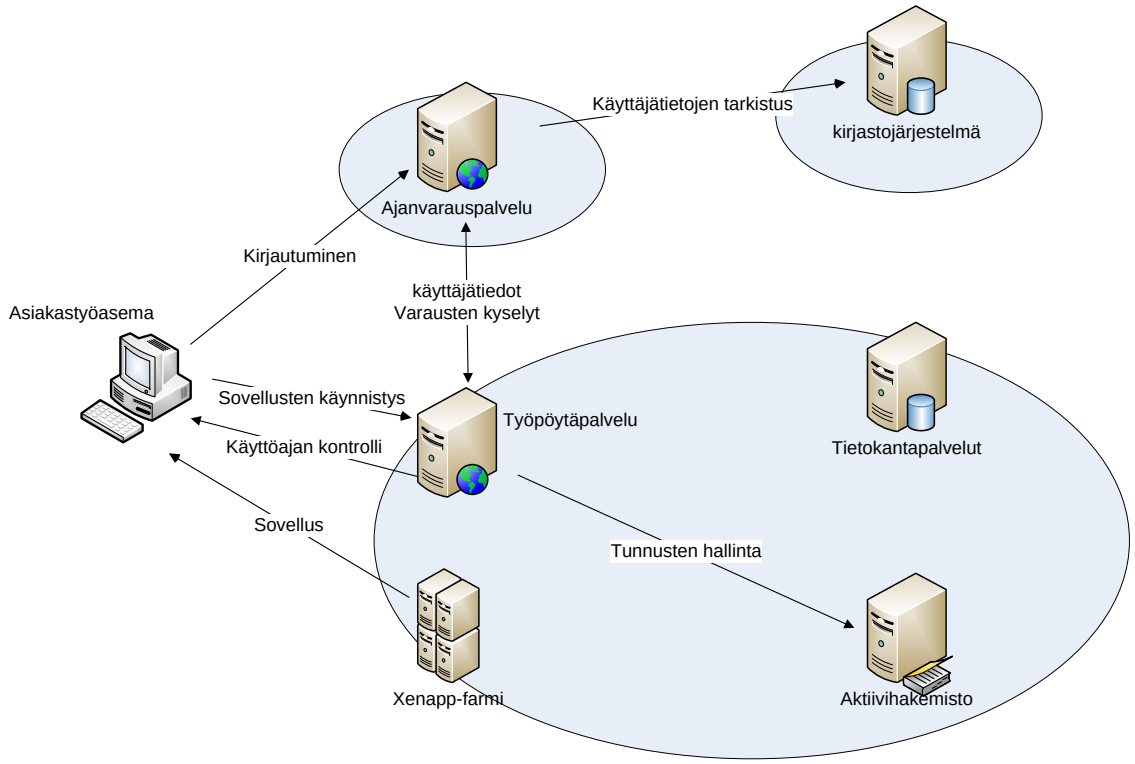
Papercut MF on turvatulostusjärjestelmä, joka on mahdollista integroida useaan käyttäjähakemistoon. Järjestelmä on riippumaton tulostimen valmistajasta ja mallista ja hyödyntää kunkin valmistajan omia tulostinajureita. Tämä mahdollistaa sovelluksen käytön heterogeenisissä ympäristöissä, joissa on käytössä erimerkkisiä tulostimia ja monitoimilaitteita. Järjestelmä koostuu sovelluspalvelimesta (Application server) sekä mahdollisista toissijaisista tulostuspalvelimista (Secondary server). Järjestelmän tukee pilvitulostusta sähköpostin sekä Google Cloud Print -ominaisuuden kautta. Tulosteiden vapauttamiseen voidaan käyttää joko monitoimilaitteiden omaa käyttöliittymää tai erillistä Windows-työasemaan asennettavaa Print Release Station -sovellusta.

3 Testiympäristö ja järjestelmän toiminnan testaus

Helsingin kaupunginkirjasto on osa Helsingin kaupunkikonsernia. Konsernissa monien tietoteknisten ratkaisujen hallinnointi on keskitetty yhteiselle IT-osastolle, joka vastaa mm. henkilökunnan tietoverkosta sekä aktiivihakemistosta. Kohdeyritys itse vastaa mm. asiakkaille tarjottavista palveluista kokonaisuudessaan sekä henkilökunnan käyttäjätietojen ylläpidosta aktiivihakemistossa. Lisäksi yritys ylläpitää henkilökunnan työajanseurantajärjestelmää.

ASKO-asiakastyöasema on kirjaston ylläpitämä työasemapalvelu, joka koostuu lukuisista eri järjestelmistä. ASKO tarjoaa asiakkaille mahdollisuuden käyttää Microsoft Office -ohjelmia, selata Internetiä Google Chrome- ja Internet Explorer -selaimilla sekä käyttää joitakin muita varusohjelmia. Järjestelmä rakentuu Citrix Xenapp -tuotteen

ympärille, josta käyttäjien sovellukset suoritetaan. Itse kirjastoissa on Thin Client -tyyppiset asiakaspäätteet. Järjestelmään kirjaudutaan kirjastojärjestelmän käyttäjätunnuksella sekä PIN-koodilla. Tällä ratkaisulla on haluttu varmistaa, että asiakkaat voivat asioida kirjaston eri palveluissa käyttäen yhtä käyttäjätunnusta. Työasemia voidaan varata etukäteen varaus.lib.hel.fi-palvelussa, josta asiakas voi varata työaseman käyttöönsä itselleen sopivasta kirjastosta.



Kuva 1. Asiakastyöasemaympäristön tärkeimmät komponentit

Kuvassa 1 on esitetty asiakastyöasemajärjestelmän tärkeimmät komponentit sekä yhteydet järjestelmien välillä. Käyttäjän tiedot tarkistetaan ajanvarausjärjestelmän avulla kirjastojärjestelmästä, jonka jälkeen ne välitetään selainpohjaisesta työpöytäkäyttöliittymästä vastaavalle työpöytäpalvelimelle. Käyttäjä voi käynnistää tarjolla olevan sovelluksen selaimen työpöytäliittymästä, jonka jälkeen hänet yhdistetään Citrix XenApp -palvelimelle, josta käyttäjälle esitetään näkymä sovelluksesta.

Toimintaympäristössä rajoitetaan tietoliikennettä eri verkkoalueiden välillä. Tämä tulee ottaa huomioon järjestelmää suunniteltaessa, jotta voidaan hyödyntää mahdollisimman

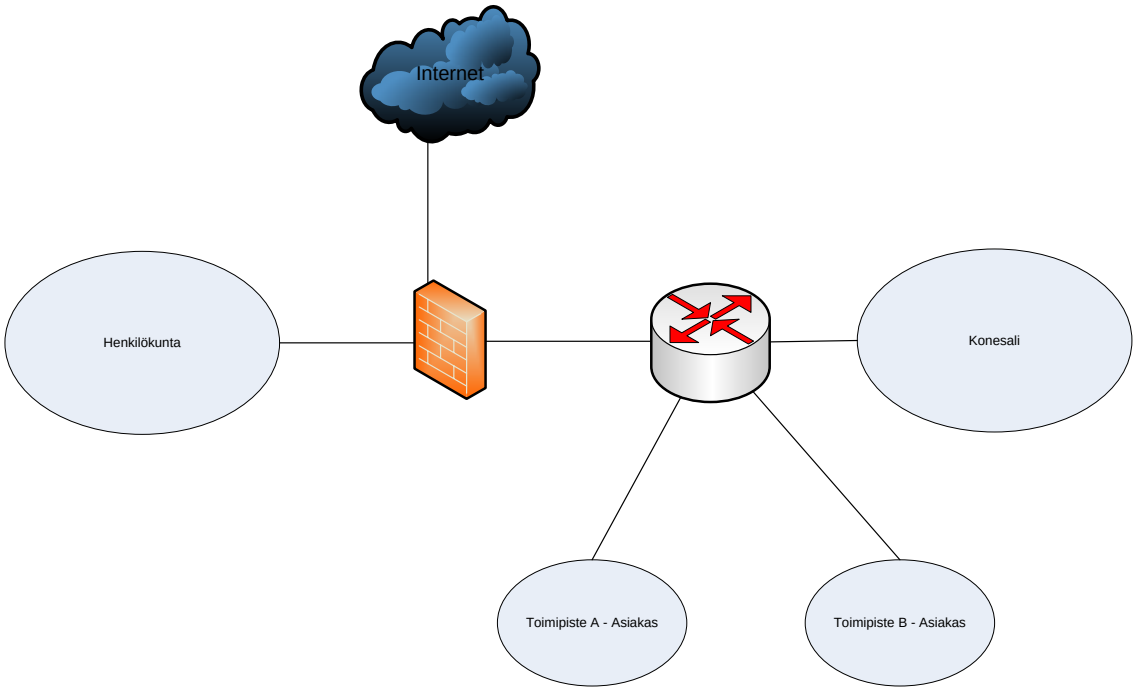
paljon jo olemassa olevia palomuurisäännöstöjä sekä tarvittaessa pyytää palomuuriavauksia verkonhallinnassa vastaavalta taholta.

Tulostusjärjestelmän ominaisuuksien testausta, optimointia ja vianselvitystä varten rakennettiin erillinen testiympäristö tulostusjärjestelmästä, joka vastaa tärkeimmiltä osiltaan suunniteltua tuotantojärjestelmää. Työssä hyödynnettiin olemassa olevaa testiympäristöä verkon, aktiivihakemiston ja tietokantapalveluiden osalta.

Järjestelmän ominaisuuksia testatessa huomattiin, että järjestelmän oletusarvoja pitää muuttaa soveltuvin osin. Esimerkiksi Papercut-palvelimen käyttämät tcp-portit muutettiin käyttämään standardeja http- ja https-portteja. Nämä muutokset on kuvattu tarkemmin dokumentin myöhemmissä vaiheissa.

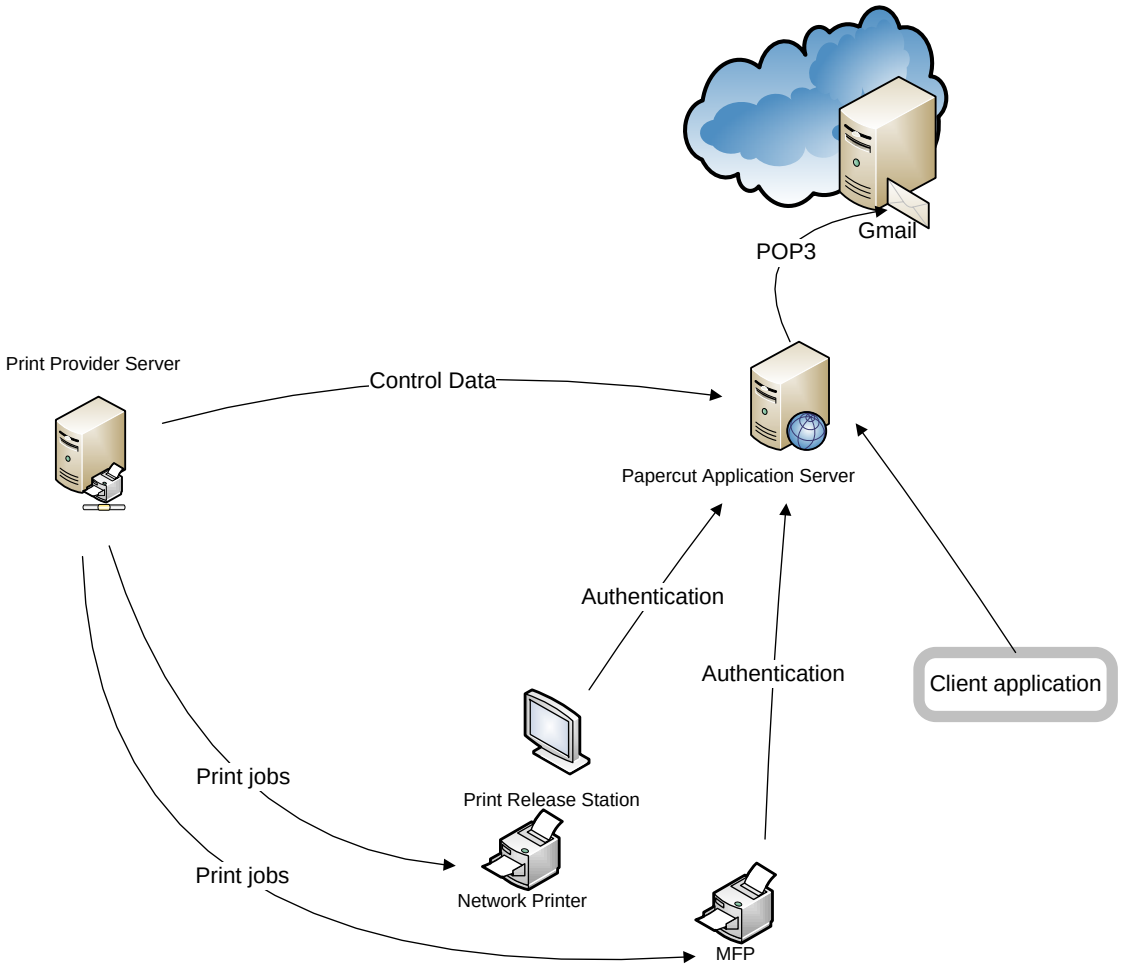
3.1 Palvelinympäristö ja verkkoyhteydet

Kaupunginkirjastolla on käytössään kaksi toisistaan eristettyä verkkoa, joista toinen on tarkoitettu henkilökunnan ja toinen asiakastietokoneiden käyttöön. Tämän lisäksi on käytössä DMZ-alue, jolla sijaitsevat julkiseen Internet-verkkoon palveluja tarjoavat web-palvelimet. Verkon perusasettelu on esitetty kuvassa 2.



Kuva 2. Looginen verkkorakenne

Testissä käytettiin kahta erillistä Papercut-tulostuspalvelinta, joista asiakasympäristön palvelimeen asennettiin sekä Application Server että Print Provider Server -rooli. Henkilökunnan tulostinpalvelimelle asennettiin Print Provider Server -rooli. Näin toimien voitiin minimoida virtualisointiympäristön resurssien käyttöä, koska tarvittavat tietoliikennetestit ja selvitykset voitiin suorittaa kuvassa olevalla kokoonpanolla. Henkilökunnan tulostuspalvelimelle asennetut tulostinjonot asetettiin yrityksen käytäntöjen mukaisesti käyttämään LPR-tulostusta, joka toimii TCP-portin 515 kautta.



Kuva 3. Tulostusjärjestelmän tietoliikenneyhteydet

Kuvassa 3 on esitetty Papercut-tulostusjärjestelmän tietoliikenneyhteydet järjestelmän eri komponenttien välillä. Kuvan mukaisesti tcp/ip -yhteyden avaavana osapuolena ei toimi sähköpostitulosteiden tarkistusta lukuun ottamatta sovelluspalvelin vaan järjestelmän alikomponentit sekä siihen liitetyt muut toimijat. Tämä huomioitiin järjestelmän suunnittelussa tietoliikenneyhteyksien osalta. Toimintaa tarkasteltiin myös Wireshark-sovelluksella.

Sähköpostitulostuksen testauksen yhteydessä havaittiin, että palvelimen lähettämät sähköpostiviestit sisältävät palvelimen url-osoitteen isäntänimen lisäksi palvelimen käyttämän tcp-portin 9191, vaikka palvelimen asetuksissa oli erikseen asetettu päälle myös porttien 80 (http) sekä 443 (https) käyttö. Tästä syystä sovelluspalvelimen varsinainen tcp-portti muutettiin käyttämään portteja 80 ja 443 alla olevan konfiguraatioesimerkin mukaisesti. Sähköpostitulostusta käsitellään tarkemmin kappaleessa 3.2.3.

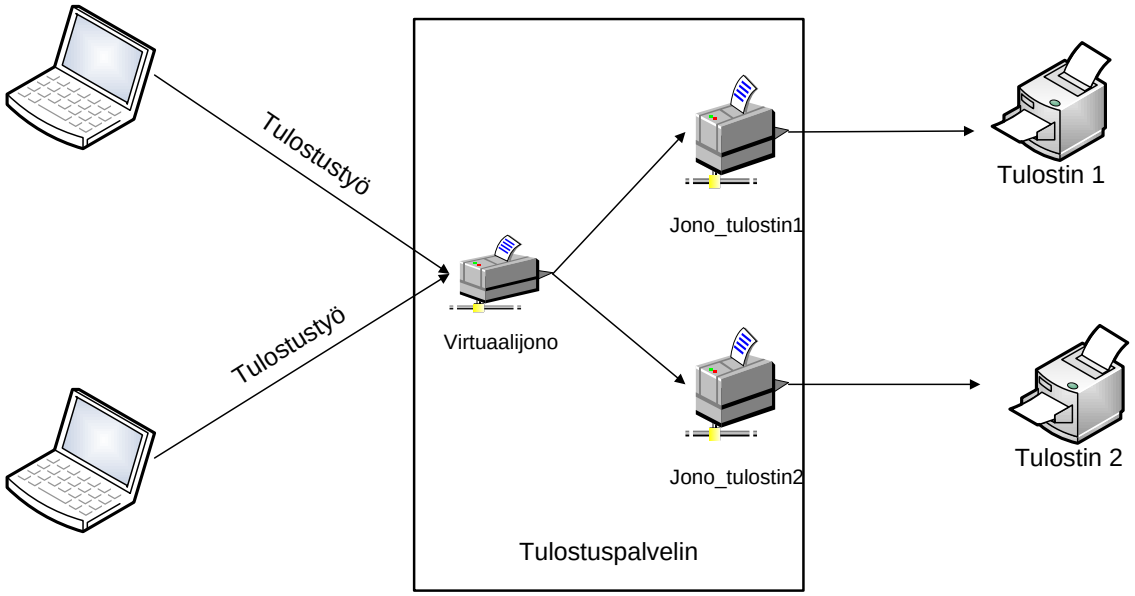
```
### Server Port (Default: 9191 and SSL: 9192) ###
# IMPORTANT: Use these options only if directed by support.
#server.port=9191
#server.ssl.port=9192
server.port=80
server.ssl.port=443
#server.force-host-header=print.debug.lib.hel.fi
```

Muutoksen jälkeen järjestelmän palvelinten välistä liikennettä seurattiin Wireshark-sovelluksella. Verkkokaappausten perusteella todettiin, että palvelinten välille ei muodostunut yhteyttä. Tämän todettiin johtuvan siitä, että tulostuspalvelin pyrki ottamaan yhteyttä järjestelmän oletusporttiin 9191. Sovelluksen dokumentaation perusteella muutettiin tulostuspalvelimen print-provider.conf-asetustiedostoa siten, että ApplicationServerPort-avaimen arvoksi vaihdettiin 80.

```
# Define the TCP port associated with the application server.
#   Default: 9191
#   Examples:  8080
#
ApplicationServerPort=80
```

3.2 Tulostimet ja tulostusjonot

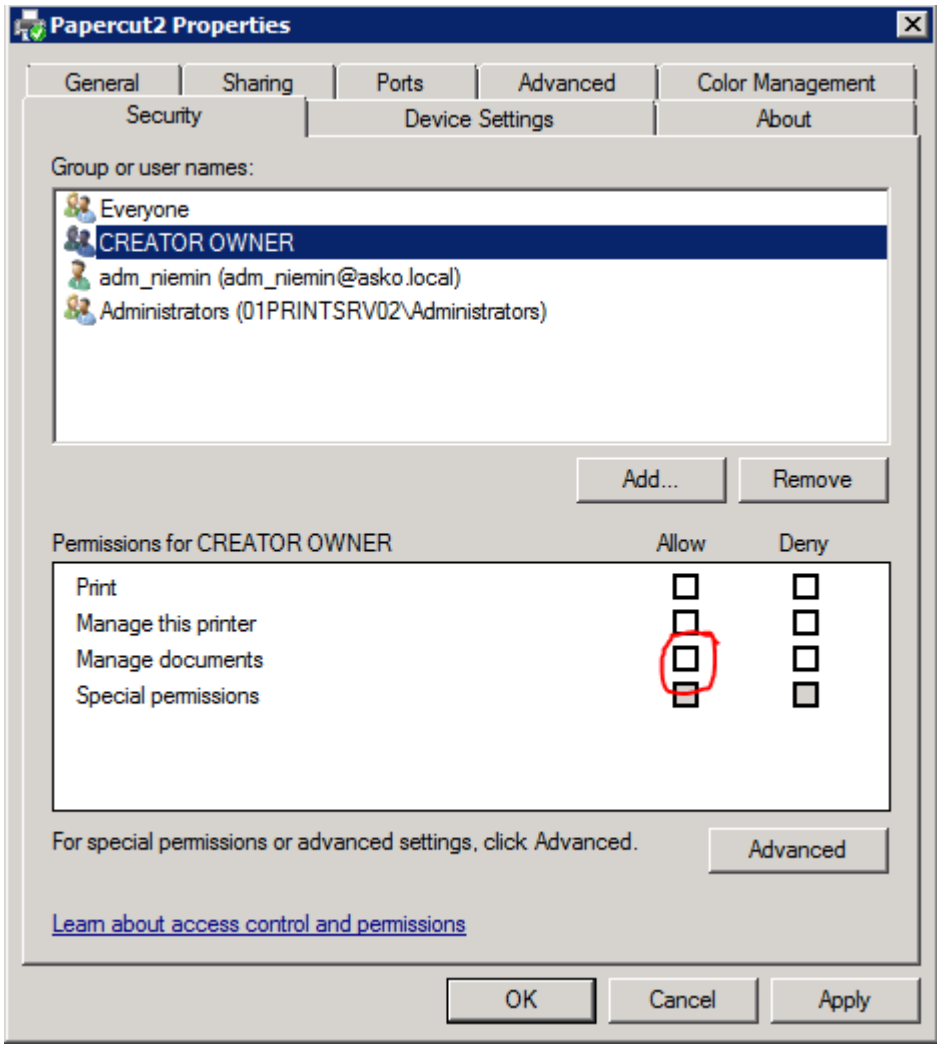
Papercut MF -tulostusjärjestelmän Find-Me Print -ominaisuus perustuu siihen, että työt tulostetaan virtuaalijonoihin, joista työt ohjataan erillisiin tulostinlaitekohtaisiin tulostusjonoihin käyttäjän sijainnin perusteella. Tällöin käyttäjän ei tarvitse erikseen valita tulostettaessa, mille tulostimelle työnsä haluaa. Tämän toiminnallisuuden lisäksi haluttiin muokata tulosteen oletusasetuksia siten, että tulosteet muutetaan mustavalkoisiksi sekä kaksipuoleisiksi. Kuitenkin käyttäjälle oli annettava mahdollisuus valita halutessaan sekä väri- että yksipuolinen tulostus. Tulostustöiden muunnos sekä valintamahdollisuus toteutettiin tulostusjärjestelmän tarjoamalla Advanced Print Scripting -ominaisuudella, jonka avulla voidaan ohjelmoida käyttäjälle esitettäviä valintoja sekä viestejä käyttäen Javascript-ohjelmointikieltä. Monipuolisten valintojen esittämisestä käyttäjälle vastaa Papercut client -sovellus (PC-client.exe), joka asennettiin kaikkiin Citrix Xenapp -palvelimiin.



Kuva 4. Tulostus virtuaalijonoon

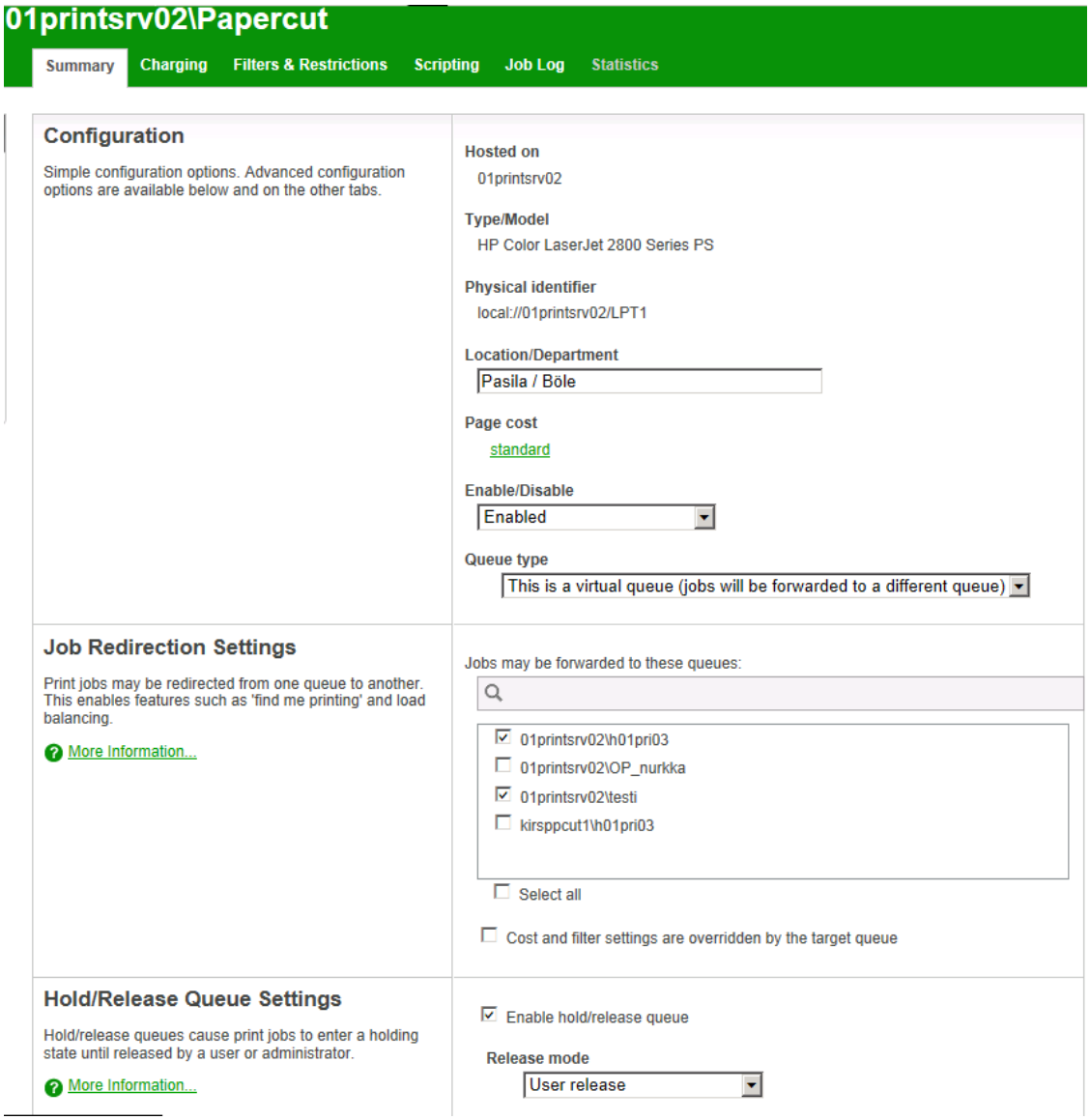
Kuvassa 4 on esitetty järjestelmän tulostamisen toimintalogiikka. Loppukäyttäjät tulostavat työt virtuaalijonoon, johon tulostetyö jää odottamaan. Käyttäjän kirjautuessa tulostimelle tai monitoimilaitteelle työ siirretään virtuaalijonosta sen tulostimen jonoon, johon käyttäjä on kirjautunut. Tämän jälkeen työ lähetetään jonosta tulostimelle, ja käyttäjä saa tulosteensa.

Tulostamisen yhteydessä asiakkaille esitetään vallintaikkuna, josta asiakas voi valita haluaako tulosteensa mustavalkoisen vai värillisenä. Tämän lisäksi asiakas voi valita yksi- tai kaksipuoleisen tulosteen. Tämä valintaikkuna toiminnallisuuksineen toteutettiin Advanced Print Script -ominaisuudella. Toiminnallisuuden toteuttava Javascript-koodi sekä valintaikkuna on esitetty liitteessä 1. Tulostusta testattaessa ilmeni, että tulostusjärjestelmä ei kyennyt muuttamaan dokumentin tulostusasetuksia väriasetusten ja kaksipuolisuuden suhteen. Ratkaisu tähän löydettiin valmistajan dokumenteista. Dokumenttien perusteella ilmeni, että tulostustyön tulee olla RAW-formaatissa, kun se oletuksena oli Windowsista tulostettaessa EMF-formaatissa. Tämä muutettiin poistamalla virtuaalitulostimen asetuksista valinta ”enable advanced printing features”.



Kuva 5. Tulostimen käyttöoikeuksien muokkaus

Valmistajan dokumentaation mukaisesti virtuaalijonojen käyttöoikeuksia muokattiin kuva 5 esittämällä tavalla, jotta käyttäjät eivät voi itse poistaa omia tulostustöitään virtuaalijonosta. Tällä toimenpiteellä estetään järjestelmän oman toimintalogiikan sekaantuminen sekä varmistetaan raportoinnin oikeellisuus. Kuvassa esitetään asetusten muokkaus tulostinjonokohtaisesti. Sama asetus voidaan myös tehdä palvelimen tasolla keskitetysti, jolloin asetus tulee voimaan kaikille uusille tulostusjonoille, kun ne luodaan.

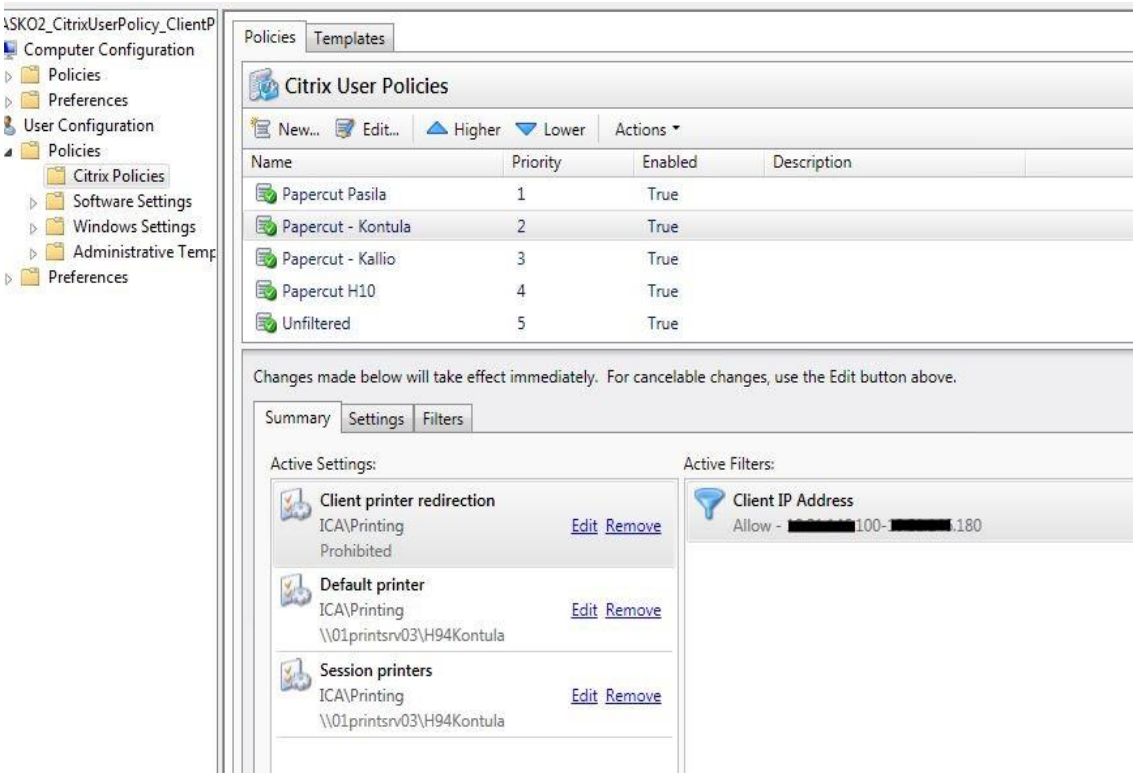


Kuva 6. Tulosteiden ohjaus virtuaalijonosta

Kuvassa 6 esitetään Papercut-sovelluksen ylläpitoliittymä, jonka avulla voidaan määrittää, mihin tulostusjonoihin tulostustyöt voidaan siirtää mistäkin virtuaalijonosta. Tällä asetuksella voidaan varmistaa esimerkiksi se, että mikäli tuloste asiakas tulostaa haluamansa dokumentin Pasilan kirjaston virtuaalitulostimelle, ei hän voi noutaa sitä kuin niiltä tulostinlaitteilta, joihin ko. virtuaalijonosta tuloste voidaan siirtää. Edellä mainitussa tapauksessa testattiin, että tuloste voidaan ohjata vain tulostimille 01printsrv02\h01pri03 ja 01printsrv02\testi.

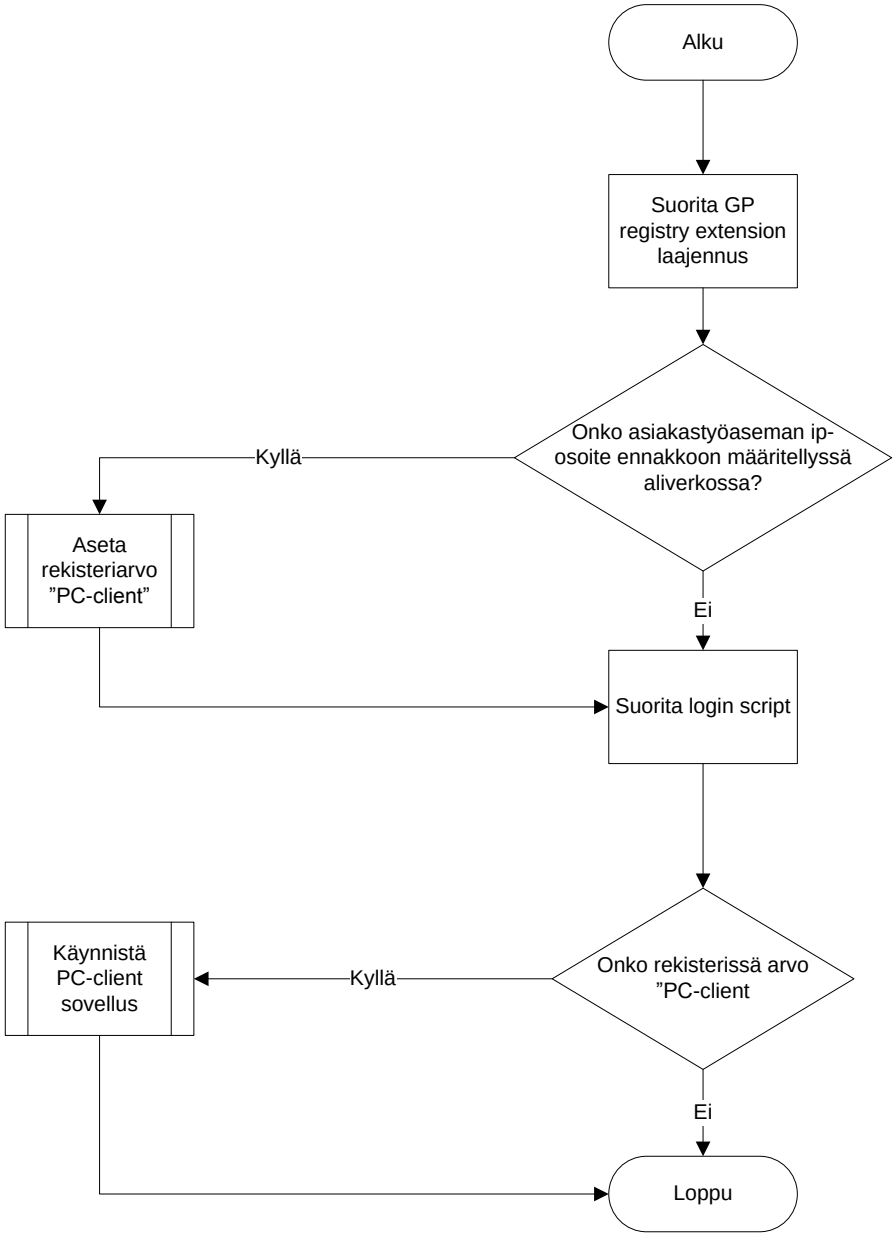
3.2.1 Oletustulostimen määritys

Asiakastyöasemilta käyttäjät käyttävät sovelluksia, kuten Microsoft Word -sovellusta keskitetyssä konesalissa sijaitsevilta Citrix Xenapp -palvelimilta. Jotta tarvittavat tulostimet voitiin asentaa vain koekäytössä mukana olleiden kirjastojen käyttäjille, asennettiin heille oletustulostin hyödyntäen Citrixin tarjoamaa ryhmäkäytäntölaajennusta. Koska jokaisella kirjastolla on erillinen oletustulostin, luotiin testissä neljä erillistä käyttäjätunnuksiin kohdistuva käytäntöä, joka suodatettiin kunkin kirjaston aliverkon perusteella (kuva 7).



Kuva 7. Oletustulostimen asennus aliverkon perusteella

Oletustulostimen asennuksen lisäksi käyttäjien päätepalveluistunnoissa oli tarve käynnistää Papercut-järjestelmän asiakasohjelmisto (pc-client.exe), jonka avulla käyttäjille voidaan esittää erilaisia tulostamiseen liittyviä ilmoituksia. Sovelluksen tuli käynnistyä vain niillä käyttäjillä, jotka olivat kirjautuneet järjestelmään testikirjastoista. Ongelma ratkaistiin hyödyntäen ryhmäkäytäntöjen rekisterilaajennuksia sekä asetusten kohdennusta etätyöpöytäsession ip-osoitteen perusteella sekä käynnistyskomentojonolla.

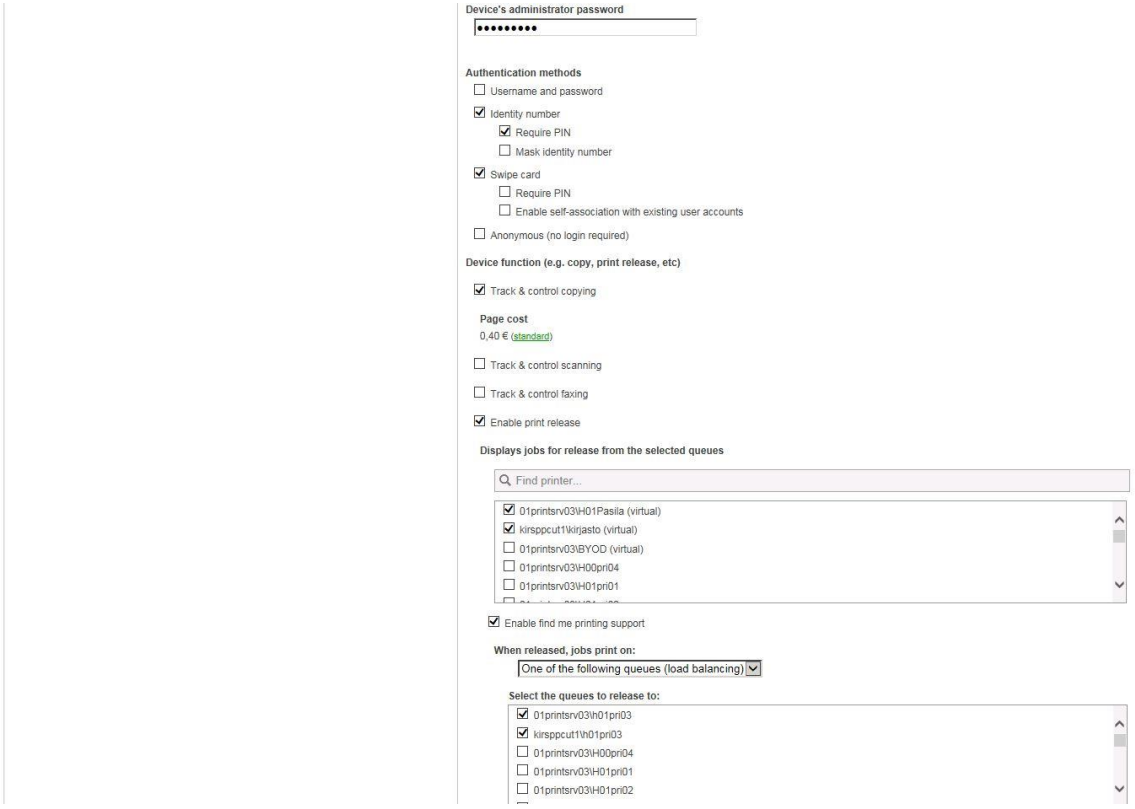


Kuva 8. PC-client-sovelluksen käynnistys työaseman ip-osoitteen perusteella

Kuvassa 8 on kaavio PC-client-sovelluksen käynnistämisestä automaattisesti käyttäjän etätyöpöytäistuntoon. Käyttäjän kirjautuessa palvelimelle suoritetaan automaattisesti ryhmäkäytännöt. Ryhmäkäytännöissä on määritetty, että mikäli istuntoon yhdistyvä työasema on ennalta määritellyssä aliverkossa (testikirjastot), asetetaan käyttäjän HKCU-rekisterihaaraan ennalta määritettyyn sijaintiin rekisteriarvo ”PC-client”. Arvon tiedoksi asetetaan pc-client.exe-sovelluksen täydellinen tiedostopolku. Tämän jälkeen ryhmäkäytäntö suorittaa käynnistyskomentojonon, joka tutkii, löytyykö ”PC-client”-arvo rekisteristä. Mikäli arvo löytyy, lukee sovellus arvoon asetetun tiedon ja pyrkii käynnistämään sen mukaisen sovelluksen.

3.2.2 Monitoimilaitteet

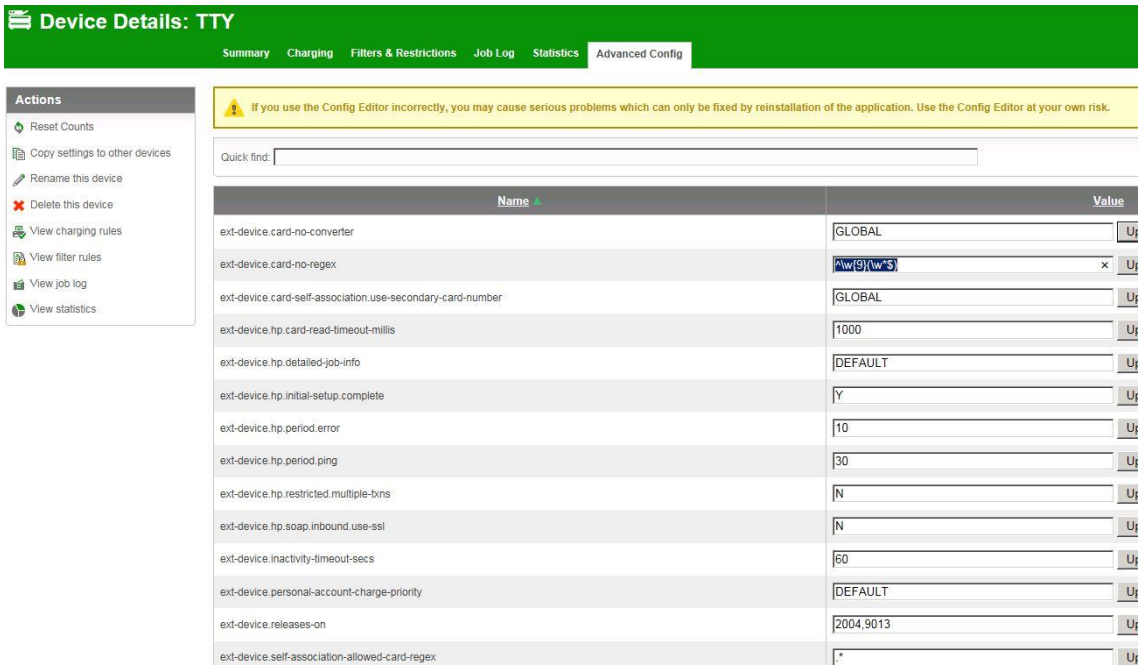
Monitoimilaitteilla voidaan tulostamisen lisäksi mm. kopioida ja skannata asiakirjoja. Järjestelmän perustestauksen yhteydessä haluttiin myös kokeilla monitoimilaitteiden liittämistä järjestelmään sekä niiden käytön helppoutta. Testeissä hyödynnettiin HP MFP 500 -sarjan monitoimilaitetta, johon hankittiin lisävarusteeksi toimikortin lukulaite. Laitteeseen asennettiin sen omaa web-käyttöliittymää hyödyntäen Papercutin toimittama lisäsovellus, joka kytki sen osaksi järjestelmää. Monitoimilaitteet näkyvät järjestelmän ylläpitoliittymässä omalla välilehdellään, jossa niiden asetuksia voidaan muokata. Jotta laite toimisi Papercut-järjestelmän kanssa, oli tulostuksenhallintajärjestelmän ylläpitoliittymässä asetettava laitteen ylläpitäjän käyttäjätunnus sekä salasana. Papercut käyttää ylläpitäjän tunnuksia laitteen asetusten muokkaukseen verkon kautta.



Kuva 9. Monitoimilaitteen asetussivu

Kuvassa 9 on esitetty monitoimilaitteen asetussivu. Kirjautuminen laitteelle mahdollistettiin syöttämällä ID-numero manuaalisesti tai erillisellä lähiluettavalla kortilla. Syötettäessä kortin numero käsin vaadittiin käyttäjää syöttämään myös PIN-koodi. Lähiluettavaa korttia käytettäessä PIN-koodia ei vaadittu. Monitoimilaitteelle otettiin

kuvan 9 mukaisesti käyttöön myös tulosteiden ohjausmahdollisuus laitteelle. Laite asetettiin näyttämään kirjautuneen käyttäjän tulostustyöt asiakas- sekä henkilökuntapalvelimen virtuaalitulostinjonoista sekä vapauttamaan tuloste testiympäristön kahteen eri tulostusjonoon sen mukaisesti, onko tuloste henkilökunnan vai asiakkaiden virtuaalijonossa.



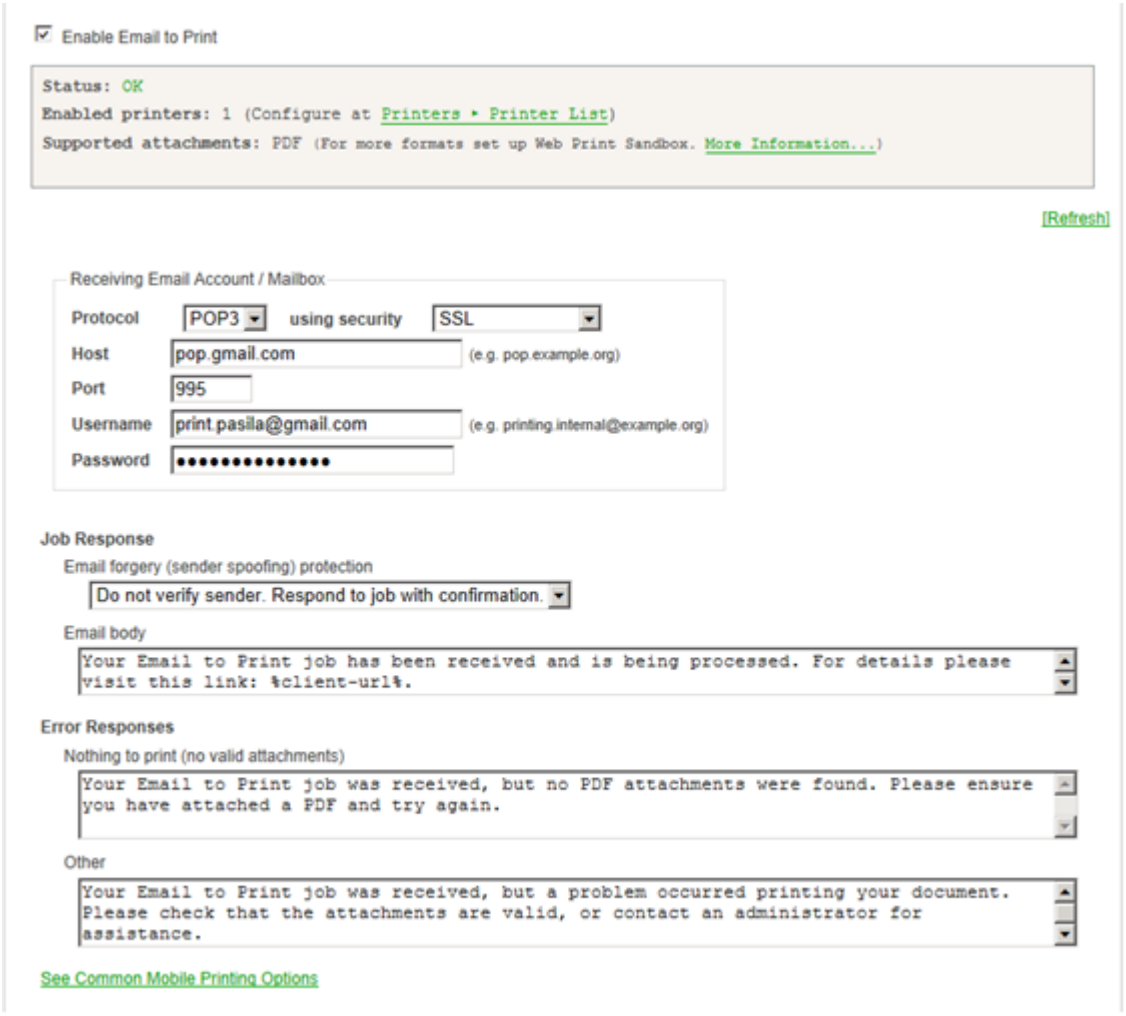
Kuva 10. Regex-lausekkeen hyödyntäminen id-numeron tarkistuksessa

Kun monitoimilaitteelle kirjautumista testattiin erilaisilla lähiluettavilla korteilla, havaittiin, että kortinlukija esittää kortin tunnisteen toisessa muodossa kuin mitä se on toimikorttitietokannassa. Useampaa korttia ja korttistandardia testattaessa havaittiin, että kaikille korteille yhteinen ominaisuus oli, että lukija lisäsi jokaisen kortin alkuun yhdeksän merkkiä ennen kortin varsinaista tunnistetta. Ongelma saatiin ratkaistua käyttämällä Papercutin ylläpitoliittymän tarjoamaa mahdollisuutta muodostaa kortin numero regex-lausekkeella lukijan välittämästä tiedosta. Kuvan 10 mukaisesti monitoimilaitteen asetuksiin määritettiin, että kortin numeron tarkastamisessa käytetään kortin numeroa siten, että yhdeksän ensimmäistä merkkiä jätetään huomioimatta. Testien jälkeen muodostettu regex-lauseke oli: ^\w{9}(\w*$). lauseke muodostaa ensimmäisen yhdeksän merkin jälkeen erillisen ryhmän lopuista merkeistä. Järjestelmä kykenee tämän jälkeen hyödyntämään regex-lausekkeen ryhmää kortinnumeron tarkistuksessa.

3.2.3 Mobiilitulostus

Papercut-järjestelmä tarjoaa mahdollisuuden mobiilitulostukseen käyttäen sähköpostia tai Google Cloud Print -integraatioita. Testiympäristössä käyttöön otettiin sähköpostitulostus. Sähköpostitulostusta käytetään lähettämällä pdf-liitetiedostoja järjestelmää varten luotuun sähköpostiosoitteeseen. Järjestelmä noutaa sähköpostilaatikkoon saapuneet liitetiedostot ja konvertoi ne tulostettavaksi spool-tiedostoksi.

Sähköpostitulostusta varten palvelimelle luotiin erillinen virtuaalitulostusjono ”BYOD”. Tulostin määritettiin käyttämään olemassa olevaa LPT1-porttia. Portilla ei ole merkitystä toiminnan kannalta, koska virtuaalitulostimen voidaan ajatella toimivan eräänlaisena välivarastona tulostustiedostoille, josta ne siirretään toiseen tulostusjonoon varsinaista tulostusta varten.

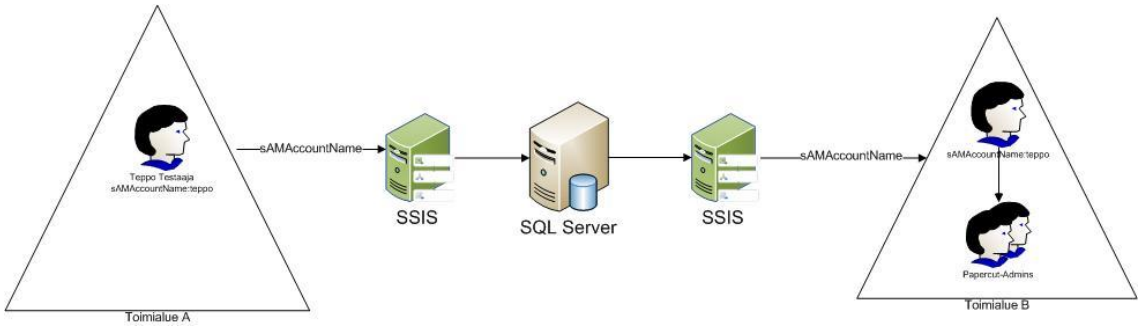


Kuva 11. Sähköpostitulostuksen käyttöönotto

Järjestelmän testejä varten perustettiin oma gmail-sähköpostitili ”print.pasila@gmail.com”. Sähköpostitilin sekä tulostusjonon luonnin jälkeen sähköpostitulostus otettiin käyttöön kuvan 11 esittämällä tavalla. Papercut-palvelin tarkastaa postilaatikon sisällön oletusarvoisesti 30 sekunnin välein. Mikäli postilaatikkoon on saapunut viesti, jossa on pdf-liitetiedosto, lataa Papercut-palvelin sähköpostin POP3-protokollan avulla omaa käsittelyään varten. Liitetiedoston lataamisen jälkeen järjestelmä muuntaa pdf-liitetiedoston normaaliksi tulostetiedostoksi sekä analysoi sen ominaisuudet kuten sivumäärän. Tämän jälkeen tuloste jää odottamaan tulosteen vapautusta BYOD-virtuaalijonoon, josta käyttäjä voi vapauttaa sen tulostettavaksi kirjautumalla Print Release -työasemalle.

3.3 Käyttäjätunnukset ja kirjautuminen

Papercut-järjestelmä ylläpitää tietoa järjestelmän käyttäjistä omassa tietokannassaan. Tiedot voidaan synkronoida automaattisesti olemassa olevista hakemistopalveluista, kuten Aktiivihakemistosta tai muusta LDAP-tietokannasta tai ne voidaan tuoda manuaalisesti eräajona tai ohjelmallisesti rajapinnan kautta. Kirjastolla on rekisteröityjä työasemakäyttäjiä yli 300 000 kappaletta. Näistä käyttäjistä vain osa käyttää tulostuspalvelua, joten kaikkien käyttäjien automaattinen synkronointi ei ole asianmukaista. Tämän lisäksi ylläpitohenkilöiden käyttäjätunnukset synkronoidaan järjestelmään asiakasympäristön Aktiivihakemistosta. Papercut-järjestelmä konfiguroitiin ylimääräisen kuormituksen välttämiseksi siten, että asiakkaan tiedot synkronoidaan olemassa olevasta aktiivihakemistosta ensimmäisen tulostuskerran yhteydessä. Tästä käytetään järjestelmässä termiä ”create users on demand”. Lisäksi ylläpitotunnukset synkronoidaan järjestelmään automaattisesti kerran vuorokaudessa.



Kuva 12. Käyttäjätunnusten automaattinen ylläpito

Tunnusten kopiointiin käytetyn prosessin toiminta on esitetty kuvassa 12. Henkilökunnan käyttäjätiedot sijaitsevat aktiivihakemistossa, joka ei ole käytettävissä asiakasverkossa olevista järjestelmistä. Kirjautumisessa haluttiin kuitenkin hyödyntää lähiverkon käyttäjätunnusta ja mahdollistuu suorakirjautuminen asiakaspalvelutehtävissä työskenteleville henkilöille. Toteutustavaksi valittiin WebAuth-protokolla, jolla lähiverkon käyttäjätunnus välitetään taustajärjestelmälle (Papercut) http-otsikkotietona. http-otsikon mukana välitettävä tunnus tulee olla järjestelmään valmiiksi luotuna. Ylläpitotunnusten automaattisen kirjautumisen ja synkronoinnin mahdollistamiseksi luotiin henkilökunnan lähiverkkotunnuksista kopio asiakasjärjestelmän Aktiivihakemistoon käyttäen tunnuksen käyttäjänimi-kentässä (sAMAccountName) samaa tunnusta kuin henkilökunnan aktiivihakemistossa. Nämä tunnukset synkronoidaan Papercut-järjestelmään automaattisesti kerran

vuorokaudessa. Käyttäjätunnusten kopiointiprosessi automatisoitiin ylläpidon helpottamiseksi käyttäen tunnusten kopioinnissa SQL Server Integration Services (SSIS) -alustaa. Kopiointiprosessin yhteydessä käyttäjätunnukset lisätään erilliseen aktiivihakemiston käyttäjätyhmään, jolle on luvitettu pääsyoikeus Papercut-järjestelmän ylläpitoasetuksiin.

Asiakkaiden useimmin käyttämä tulostusjärjestelmän käyttöliittymä on tulosteiden vapautustyöasema. Vapautustyöasemalle kirjaudutaan samalla käyttäjätunnuksella kuin asiakastyöasemille. Kirjautumisessa asiakkaan on mahdollista käyttää kirjastokortin numeroa ja siihen liitettyä pin-koodia tai vaihtoehtoisesti sähköpostiosoitetta ja pin-koodia. Jälkimmäisessä tapauksessa sähköpostiosoite on alias kirjastokortin numerolle ja näin ollen siis pin-koodi on molemmissa sama. Asiakastyöasemien lisäksi käyttäjien on mahdollista tulostaa omilta laitteilta. Tällöin kirjautumisessa käytetään itse luotua käyttäjätunnusta ja salasanaa. Asiakastyöasemakäyttäjien käyttäjätunnusten tiedot sijaitsevat erillisessä työasemien ajanvarausjärjestelmässä. Asiakastyöaseman taustajärjestelmänä toimivan aktiivihakemiston käyttäjätunnusta asiakkaat eivät tiedä, vaan asiakkaille luodaan aktiivihakemiston käyttäjätunnus automaattisesti.

Ylläpitäjien käyttöliittymä sekä omilta laitteilta tulostavien asiakkaiden käyttöliittymä toimivat selaimella. Asiakkaat käyttävät kirjautumisessa itse luomaansa käyttäjätunnusta sekä salasanaa.

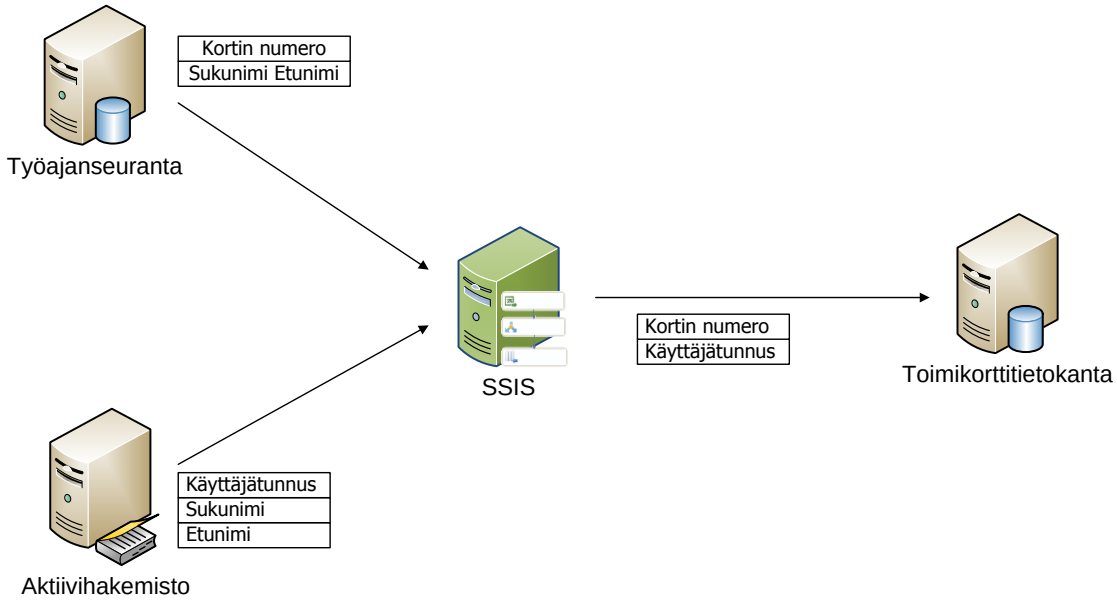
3.3.1 Toimikortin tarkistaminen ulkoisesta tietolähteestä

Papercut mahdollistaa kahden erillisen toimikortin numeron liittämisen käyttäjätunnukseen. Tällöin kirjautuminen tulostimelle voidaan suorittaa käyttäen jo valmiina olevaa kulkukorttia tai muuta toimikorttia. Monissa ympäristöissä on kuitenkin tarve käyttää useampia toimikortteja tai toimikorttien numeroita ei muusta syystä haluta tuoda Papercutin omaan tietokantaan. Tällöin järjestelmä voidaan konfiguroida tarkistamaan käyttäjän toimikortin tieto ulkoisesta tietolähteestä. Tämä tarkoittaa käytännössä sitä, että toimikortteja voi olla rajaton määrä, ja niiden lähdetiedot voivat sijaita useassa eri tietokannassa.

Kirjastolla on käytössä erilliset toimikorttitietokannat henkilöstölle ja asiakkaille. Tiedot päivittyvät usein varsinkin asiakkaiden osalta jolloin toimikorttitietojen synkronointi

Papercut-järjestelmän tietokantaan aiheuttaisi turhaa kuormitusta. Tästä syystä tulostusjärjestelmä konfiguroitiin tarkistamaan toimikorttiin liitetty käyttäjätunnus erillisestä Microsoft SQL Server -tietokannasta.

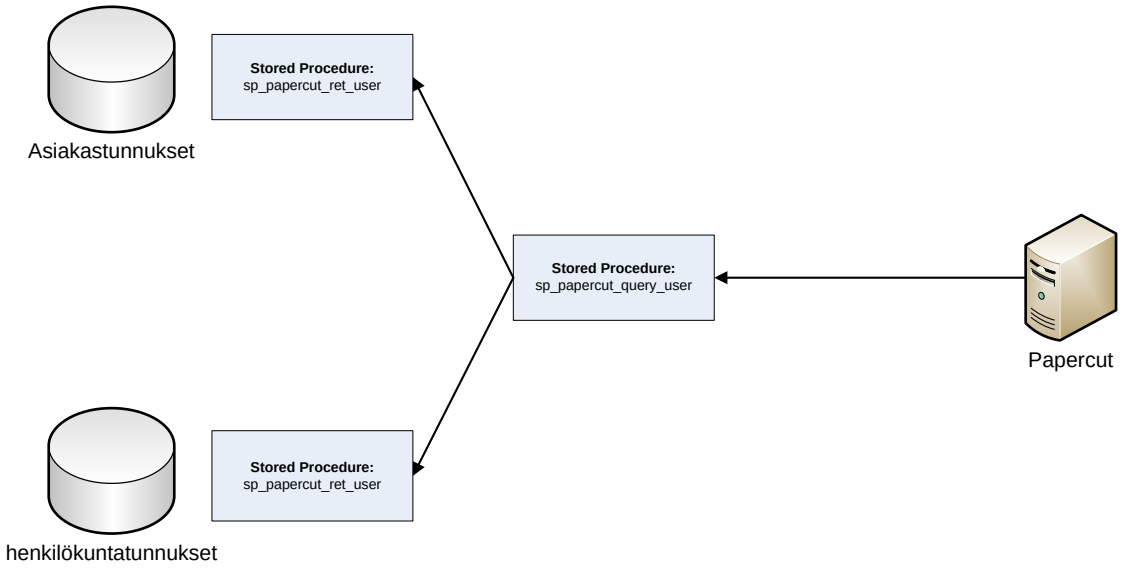
Henkilökunnan toimikorttitiedot sijaitsevat erillisessä työajanseurantajärjestelmässä. Työajanseurantajärjestelmä ei sisällä tietoa henkilön Windows-käyttäjätunnuksesta vaan tiedot yhdistetään hyödyntäen SQL Server Integration Services(SSIS) -alustaa. Kuvassa 13 on esitetty tietojen yhdistämien sekä vienti erilliseen toimikorttitietokantaan SSIS:n avulla.



Kuva 13. Toimikortti- ja käyttäjätunnustietojen yhdistäminen erilliseen tietokantaan

Papercut-järjestelmässä toimikortin numeron tarkistus ja yhdistäminen käyttäjätunnukseen hyödyntäen ulkoista tietokantaa toteutetaan erillisellä SQL-lauseella, joka määritetään järjestelmän ylläpitoliittymässä. Jotta toimikortin tarkistus voidaan pitää mahdollisimman yksinkertaisena Papercut-järjestelmän näkökulmasta, toteutettiin tarkistus hyödyntäen SQL-palvelimen Stored proseduuria. Tämä mahdollistaa uusien toimikorttitietokantojen liittämisen järjestelmään sekä toimikortin taustalla olevan tietokannan rakenteen muuttamisen tarvittaessa joustavasti ilman, että tulostusjärjestelmään konfiguroitua SQL-lausetta tarvitsee muuttaa. Hyödyntämällä Stored proseduuria voidaan myös parantaa tietokannan tietoturvaa siten, että SQL-yhteyden muodostuksessa käytetylle käyttäjätunnukselle määritetään oikeus suorittaa vain ennalta tietokantaan määritetty määritetty Stored proseduuri. Mikäli

käyttäjätunnuksen tiedot siis päätyisivät ulkopuolisen tahon käsiin, ja tämä onnistuisi kytkeytymään tietokantajärjestelmään ed. mainitulla käyttäjätunnuksella, ei sillä voida suorittaa esimerkiksi select-lausekkeita tietokantajärjestelmässä. Oikein konfiguroiduilla Stored procedureilla voidaan myös estää esimerkiksi sql injektio -tyyppisiä hyökkäyksiä (Swan 2011).



Kuva 14. Stored Proseduurin käyttö toimikortin tietojen tarkistuksessa

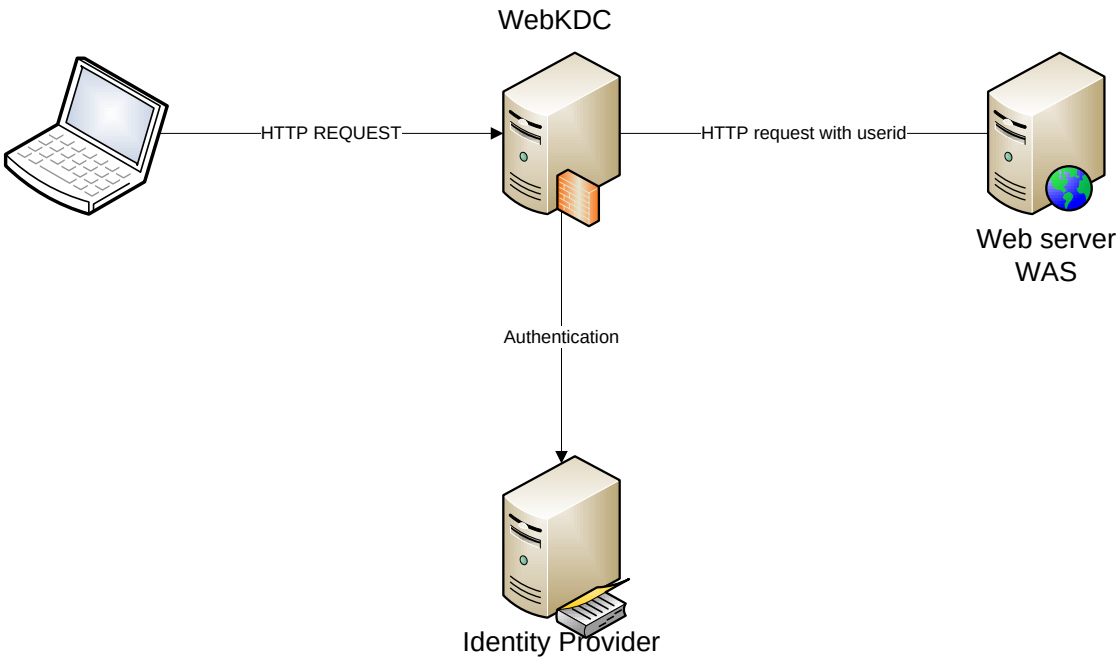
Kuvassa 14 on esitetty toimikortin tarkistuksen logiikka. Kuvan mukaisesti Papercut-järjestelmä kutsuu erillisellä tietokantapalvelimella sijaitsevaa ”sp_papercut_query_user” -proseduuria välittäen kutsun parametrina toimikortin tunnisteen. sp_papercut_query_user -proseduuri toimii välittävänä proseduurina ohjaten kyselyn edelleen toimikorttitietokannoissa sijaitseviin ”sp_papercut_ret_user”-proseduureihin. Kyselyn lopputuloksen Papercut-järjestelmälle palautetaan paluuarvona lähiverkon käyttäjätunnus, johon toimikortti on yhdistetty. Hyödyntämällä Papercut-järjestelmän ja tietokantapalvelimen välisessä SQL-kyselyssä stored proseduuria voidaan siihen vähäisellä työllä lisätä useita toimikorttitietojen lähteitä kopioimalla sp_papercut_ret_user-proseduuri kuhunkin tietokantaan ja muuttamalla sen suorittamaa kyselyä tarvittavilta osin. Tämän jälkeen viittaus uuteen kantaan lisätään sp_papercut_query_user-proseduuriin. Tämä yksinkertaistaa Papercut-järjestelmän ylläpitoa, koska se ei vaadi muutoksia olemassa olevaan konfiguraation sovelluspalvelimella vaan kaikki muutokset voidaan toteuttaa SQL-palvelimella. Proseduurien SQL-koodi on kuvattu tarkemmin 1.

3.3.2 Asiakkaat

Asiakkaiden kirjautuminen järjestelmään riippuu asiakastyypistä. Kirjaston asiakastyöasemilta tulostavat henkilöt käyttävät ainoastaan Print Release -työasemaa, jolloin heidän kirjautuminen suoritetaan toimikorttikirjautumisena. Tämä on kuvattu tarkemmin kappaleessa 3.3.1. Toinen asiakastyyppi on omilta työasemilta tulostavat käyttäjät, joita järjestelmän näkökulmasta kutsutaan järjestelmän sisäisiksi käyttäjiksi (Internal User). Sisäiset käyttäjät voivat kirjautua järjestelmään web-sivuston kautta, jossa he pääsevät tarkastelemaan ja muuttamaan omia käyttäjäasetuksiaan kuten salasanaa. Toinen käyttötapaus sisäisille käyttäjille on kirjautuminen Print Release -työasemalle. Sekä web-käytössä, että Print Release -työasemalle kirjautumisessa sisäiset käyttäjät käyttävät itse luomaansa käyttäjätunnusta sekä siihen liitettyä salasanaa.

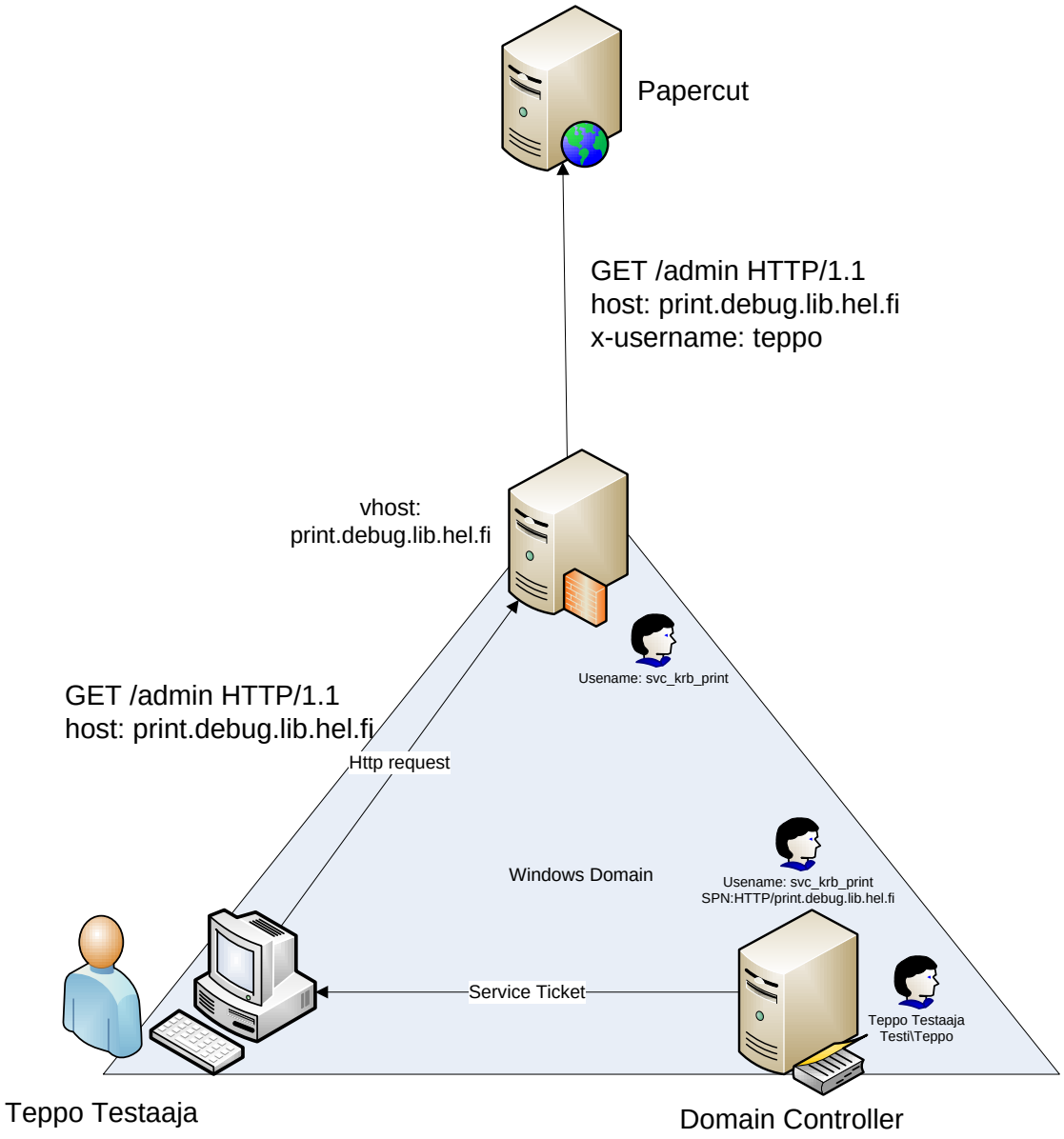
3.3.3 Ylläpitäjät

Papercut-järjestelmän ylläpitäjille toteutettiin mahdollisuus käyttää henkilökohtaista lähiverkkotunnusta järjestelmään kirjautumisessa. Verkon rakenteesta ja yrityksen käytännöistä johtuen ei kirjautumissa kuitenkaan voitu hyödyntää perinteistä Windows-käyttäjätodennusta sellaisenaan. Ratkaisuna suorakirjautumiseen otettiin käyttöön Papercut-järjestelmän tukema WebAuth-protokolla, joka on Stanfordin yliopiston kehittämä protokolla suorakirjautumiseen selainpohjaisiin järjestelmiin. WebAuth-kirjautuminen toteutettiin sovelletusti hyödyntäen WebAuth-protokollan mukaisen webKDC-palvelimen tilalla Citrix Netscaler -palvelinta.



Kuva 15. WebAuth-palvelun toteutus yksinkertaistettuna

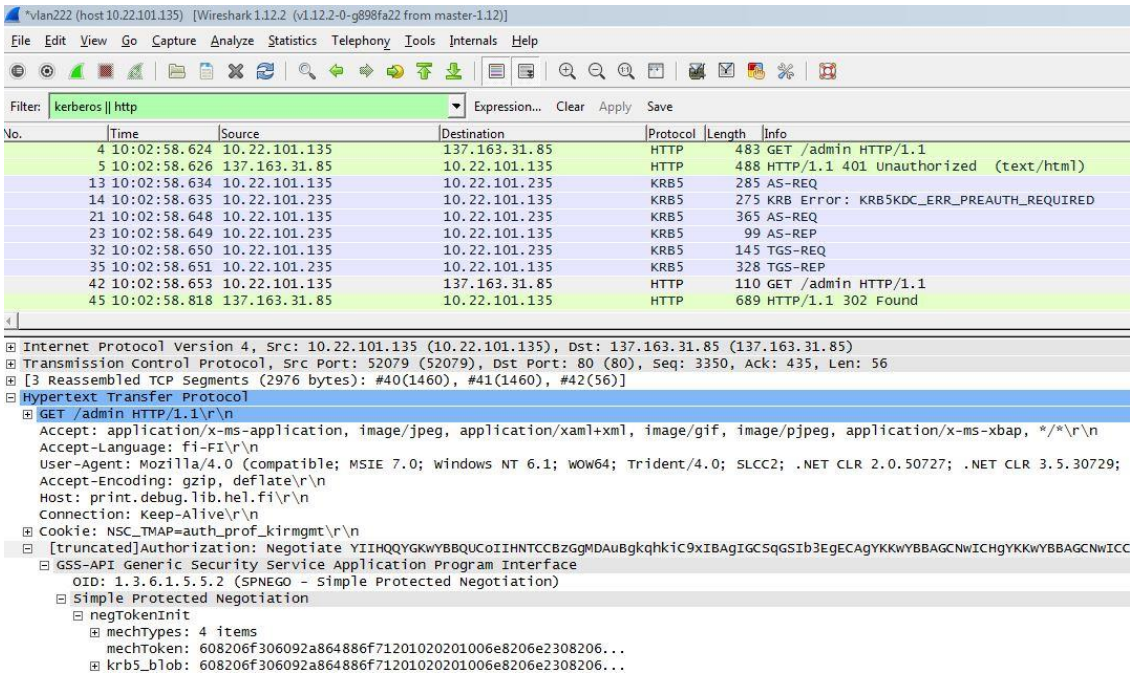
Kuvassa 15 on esitetty WebAuth-järjestelmän perusosat sekä yksinkertaistettu toimintokaavio. Järjestelmä koostuu WebAuth-protokollaa tukevasta taustajärjestelmästä, joka tuottaa varsinaisen web-palvelun sisällön. Tästä käytetään nimeä WAS. Tämän lisäksi järjestelmään kuuluu WebKDC-palvelin, jonka tehtävänä on tunnistaa käyttäjä ja välittää käyttäjätiedot WAS-palvelimelle. Käyttäjän tunnistus voidaan tehdä integroidusti hyödyntäen NTLM- ja Kerberos-autentikointia, tai käyttäjää voidaan pyytää syöttämään tunnistetiedot web-lomakkeen kautta. (Schemers & Allbery 2014)



Kuva 16. Suorakirjautuminen ylläpitoliittymään

Kuvassa 16 on esitetty toteutetun suorakirjautumisen looginen toiminta. Käyttäjän selain esittää http-sivupyynnön virtuaalipalvelimelle print.debug.lib.hel.fi. Pyyntö sisältää Kerberos-tiketin. Palvelin lukee kerberos tiketistä käyttäjänimen ja lisää sen alkuperäiseen http-pyyntöön ”x-username” -otsikkotiedon arvoksi ja välittää pyynnön Papercut-palvelimelle. Papercut-palvelin tunnistaa selaimen otsikkotiedosta käyttäjänimen ja kirjaa käyttäjän sisään järjestelmään. Toteutuksessa on hyvä huomioida, että vastoin WebAuth-protokollan määrityksiä Papercut-palvelu ei tarkista http-pyynnössä välitetyn autentikointitiedon oikeellisuutta WebKDC-palvelimelta, vaan luottaa automaattisesti kaikkiin http:n otsikkotietona välitettyyn käyttäjätunnukseen.

Tästä syystä välityspalvelimen säännöstöissä tulee huomioida, että mahdollisten tietomurtoyritysten ehkäisemiseksi käyttäjän itse lisäämä ”x-username”-otsikko poistetaan http-pyynnöstä ennen taustajärjestelmään välittämistä. Papercut-järjestelmän tunnistukseen käyttämä http-otsikko on myös vapaasti järjestelmän ylläpitäjän valittavissa.



Kuva 17. Kerberos-autentikointi virtuaali-isännälle

Kuvassa 17 on esitetty verkon pakettikaappaus kerberos-autentikoinnin vaiheista. Vaiheet käydään läpi alla:

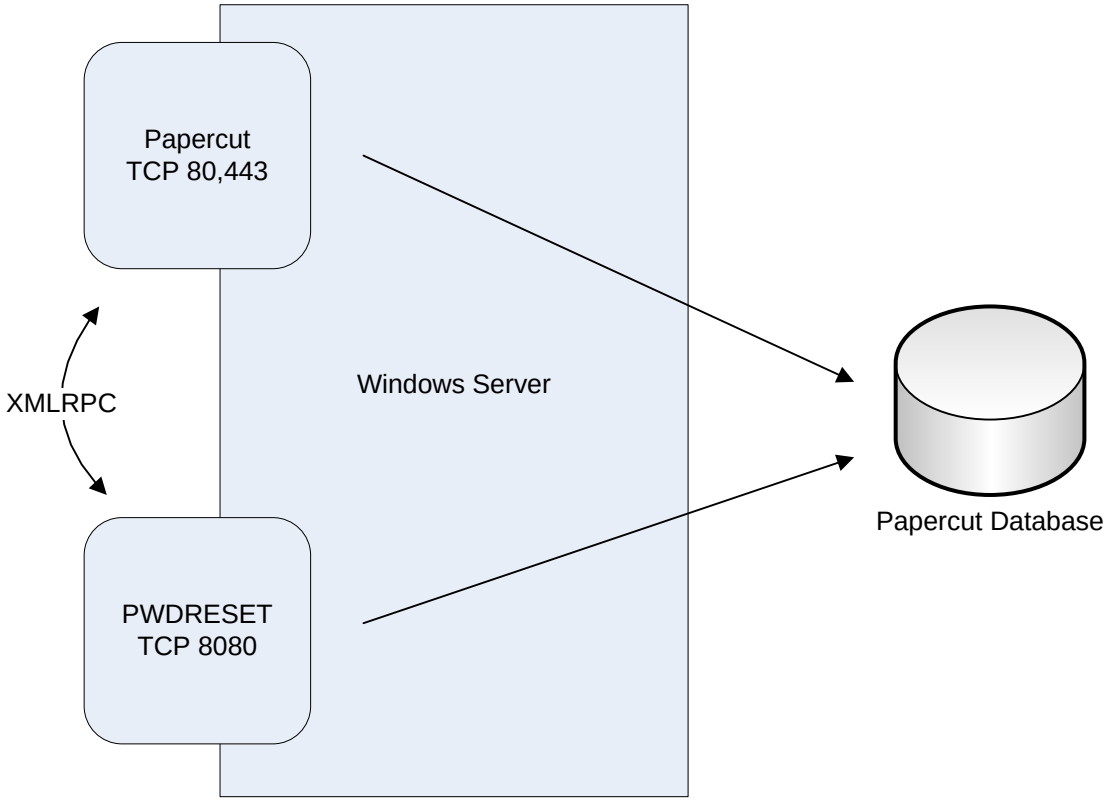
- Paketissa nro. 4 käyttäjän selain lähettää http get-pyynnön print.debug.lib.hel.fi -palvelimelle, joka on Netscaler-virtuaalipalvelin.
- Pakettissa nro. 5 palvelin vastaa käyttäjälle http:n paluukoodilla 401 - unauthorized. Tämä tarkoittaa, että käyttäjän on todennettava itsensä palvelimelle.
- Paketeissa 13-35 käyttäjä pyytää toimialueen Kerberos Key Distribution Center -palvelimelta sessio-tiketin print.debug.lib.hel.fi -palvelimelle todentamista varten.
- Paketissa nro. 42 selain lähettää alkuperäisen sivunpyynnön uudestaan print.debug.lib.hel.fi -palvelimelle sisältäen myös kerberos sessio -tiketin käyttäjän tunnistusta varten. Paketin sisältö on avattu Wireshark-ohjelmassa tarkastelua varten. Sisällöstä havaitaan, että palvelimelle lähtevä http-pyyntö sisältää nyt myös GSSAPI-määrityksen mukaisen

tokenin (Generic Security Services Application Program Interface 2014), jossa välitetään KDC-palvelimelta saatu sessio-tiketti palvelimelle.

- Paketti nro. 45: virtuaali-isäntäpalvelin on todentanut käyttäjän kerberos-tiketin perusteella, ohjannut sivupyynnön taustajärjestelmään lisättynä x-username -otsikkotiedolla ja palauttaa käyttäjälle sivuston sisällön taustajärjestelmän vastauksen perusteella.

3.3.4 Salasanan vaihtopalvelu

Papercut-sovellus ei tarjoa mahdollisuutta salasanan vaihtoon itsepalveluna. Koska kirjasto tarjoaa asiakkaille mahdollisuuden rekisteröityä järjestelmän käyttäjäksi itse valitsemallaan tunnuksella ja salasanalla, haluttiin myös toteuttaa verkkopalveluissa tyypillisesti oleva mahdollisuus vaihtaa uusi salasana unohtuneen tilalle itsepalveluperiaatteella. Tätä varten Tietotekniikkayksikön kehitystiimi, joka on erikoistunut web-sovellusten kehittämiseen, loi erillisen PHP:lla koodatun WEB-sovelluksen.



Kuva 18. PWDRESET-sovelluksen toiminta

Palvelun sovellusalustana käytetään UniServerZ-web-palvelinta. Sovellus hyödyntää Papercut-järjestelmän tarjoamaa XMLRPC-rajapintaa sekä SQL-server-tietokantakyselyjä käyttäjätunnusten salasanan vaihtamiseen. Sovellus on asennettu Papercut-palvelimelle, ja se on määritetty kuuntelemaan tcp-porttia 8080. Jotta loppukäyttäjän käyttökokemus pysyisi yhdenmukaisena sekä palvelun saatavuus helppona, konfiguroitiin palvelu saataville suojatun http-portin 443 kautta osoitteesta https://print.lib.hel.fi/resetpwd. Tämä toteutettiin hyödyntällä Netscaler-palvelimen Content Switching -ominaisuutta.

3.4 Web-käyttöliittymä

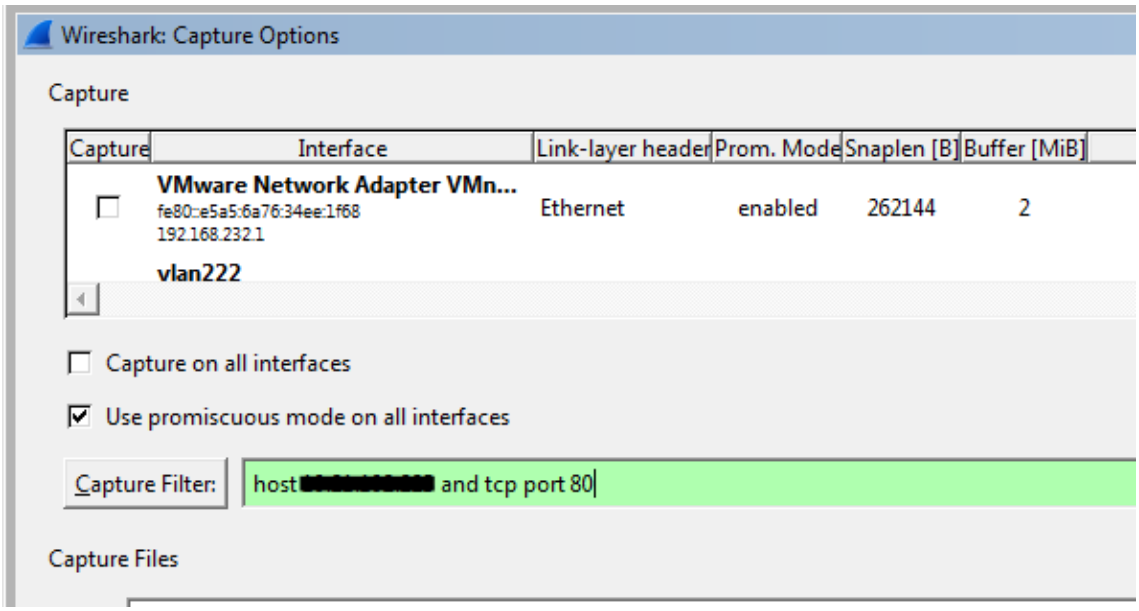
Papercut-palvelun web-käyttöliittymää käytetään rekisteröidyttäessä järjestelmän käyttäjäksi sekä yläpitotehtäviin. Web-liittymän avulla käyttäjät voivat tarkastaa käytettävissä olevan tulostussaldon sekä tulostuksenpalvelun käyttömäärän. Lisäksi käyttäjä voi vaihtaa tunnuksen salasanan. Papercut-sovellus tarjoaa rajoitetusti mahdollisuuksia käyttöliittymän muokkaamiseen varsinkin ylläpitoliittymän osalta. Tästä syystä järjestelmän ulkoasun muokkausta on tehty kahdella tasolla: sekä Papercutin tarjoamilla ratkaisuilla että Netscaler ADC:n Content Rewrite -ominaisuuksilla. Lähtökohtaisesti kaikki muutokset pyritään tekemään suoraan Papercut-järjestelmän omilla menetelmillä.

3.4.1 Kirjautumissivun muokkaus

Tulostusjärjestelmän kirjautumissivua voidaan muokata tuotteen valmistajan tukemilla tekniikoilla vain hyvin rajallisesti. Esimerkiksi sivun ulkoasua määrittelevää css-tyylitiedostoa ei voida muokata suoraan, koska se palvelun uudelleenkäynnistyksen yhteydessä korvataan aina järjestelmän oletustyylitiedostolla. Myöskään sivun html-koodaukseen ei voida vaikuttaa suoraan sovelluspalvelimella. Ainoa muutosmahdollisuus, jonka sovelluksen valmistaja tarjoaa, on mahdollisuus lisästä logon alapuolelle ohje-teksti sekä muuttaa rekisteröintisivustolle osoittavan linkin tekstiä.

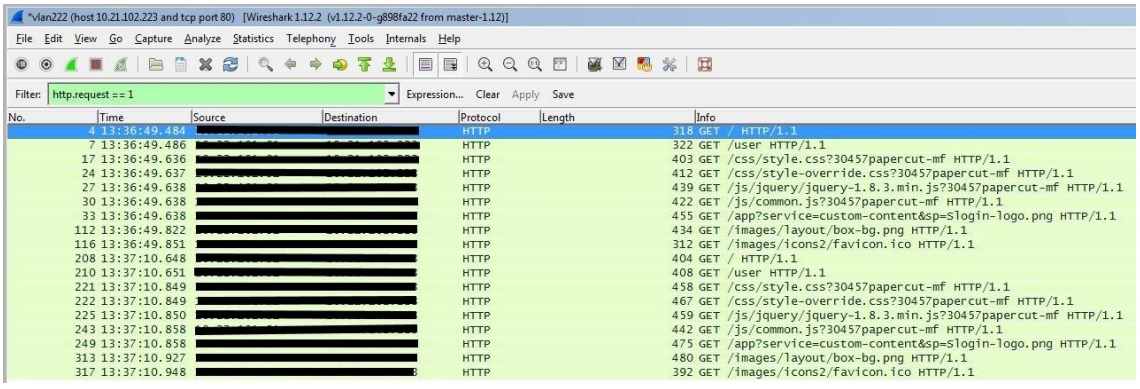
Koska kirjastolla oli tarve vaikuttaa kirjautumissivun ulkoasuun, sivuston toimintaa tutkittiin Wireshark-ohjelman avulla. Wireshark-sovellus konfiguroitiin kaappaamaan kaikki liikenne testipalvelimen tcp-porttiin 80, joka on standardi http-protokollan

käyttämä portti (kuva 19). Http-sovellukset voivat muokata sivustoja selaimen version ja valmistajan mukaan hyödyntäen selaimen lähettämiä otsikkotietoja. Koska sovelluksen toiminta haluttiin varmistaa käytettäessä sitä erilaisilla selaimilla, avattiin sovelluksen etusivu sekä Internet Explorer että Google Chrome -selaimella.



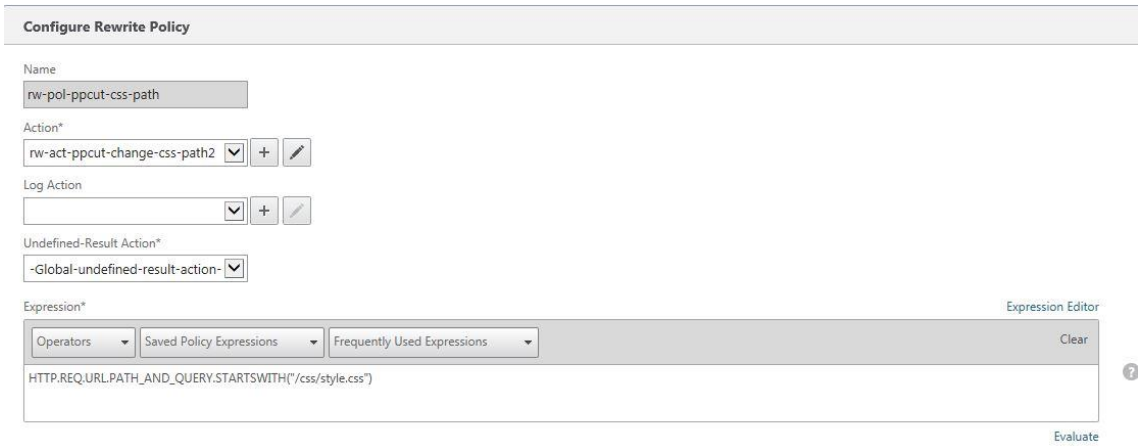
Kuva 19. Wireshark-sovelluksen konfigointi

Kun molemmat selaimet olivat suorittaneet sivupyynnöt, tarkasteltiin niiden suorittamia http-pyyntöjä. Verkkoliikenteestä haluttiin tarkastella ainoastaan selaimen lähettämiä sivupyyntöjä, jotta nähtiin, suorittavatko molemmat selaimet samat http-resurssipyynnöt. Liikenteestä suodatettiin tarkasteltavaksi pyynnöt kuvassa 20 esitetyllä tavalla hyödyntäen Wireshark-sovelluksen suodattimia.



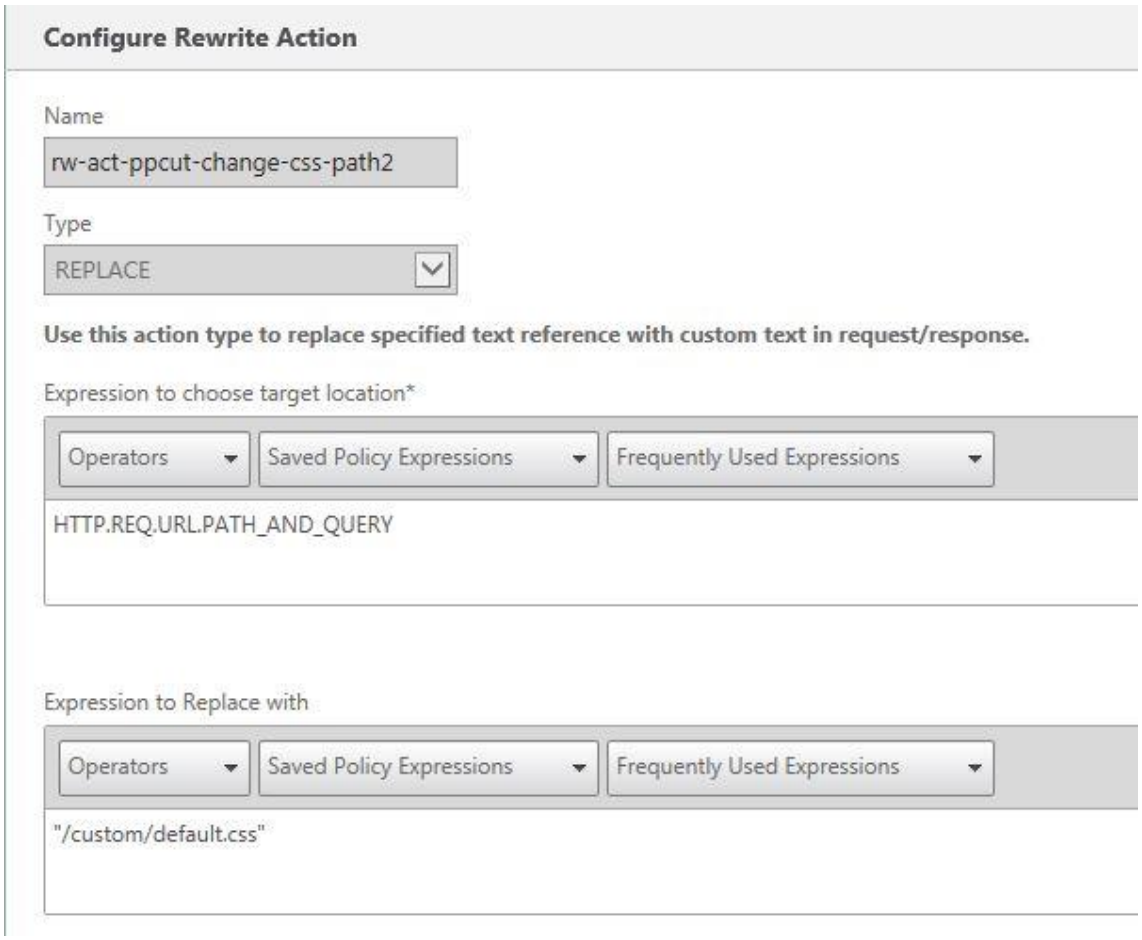
Kuva 20. http-liikenteen tarkastelu Wireshark-sovelluksella

Verkkoliikenteen tarkastelusta voitiin todeta, että sovellus käyttäytyi samalla tavalla riippumatta käytettävästä selaimesta. Verkkoliikenteestä myös todettiin, että sivuston tyylin määrittämiseen käytetään kahta css-tyylitiedostoa: "/css/style.css?30457papercut-mf" sekä ”/css/style-override.css?30457papercut-mf". Vaikka jälkimmäisestä css-tyylitiedoston ”style-override.css”-nimestä voitaisiin olettaa, että oletustyylille on olemassa tiedosto, jota käyttäjä voi muokata, ei valmistajan sivuilta kuitenkaan löydy ohjetta, millä tiedostonimellä ja mihin tämä tiedosto tulisi sijoittaa. Tämän vuoksi päätettiin toteuttaa oman tyylitiedoston toteutus hyödyntämällä Netscaler-palvelimen Content rewrite -ominaisuutta. Muutos toteutettiin siten, että alkuperäisen css-tyylitiedoston sisältö kopioitiin Internet Explorerin developer tools -työkalujen avulla erilliseen tekstitiedostoon. Tämän jälkeen tiedosto tallennettiin sovelluspalvelimelle erilliseen ”/custom/web” -hakemistoon, johon voidaan valmistajan dokumentaation mukaan viitata http-pyynnöissä polulla ”/custom/”.



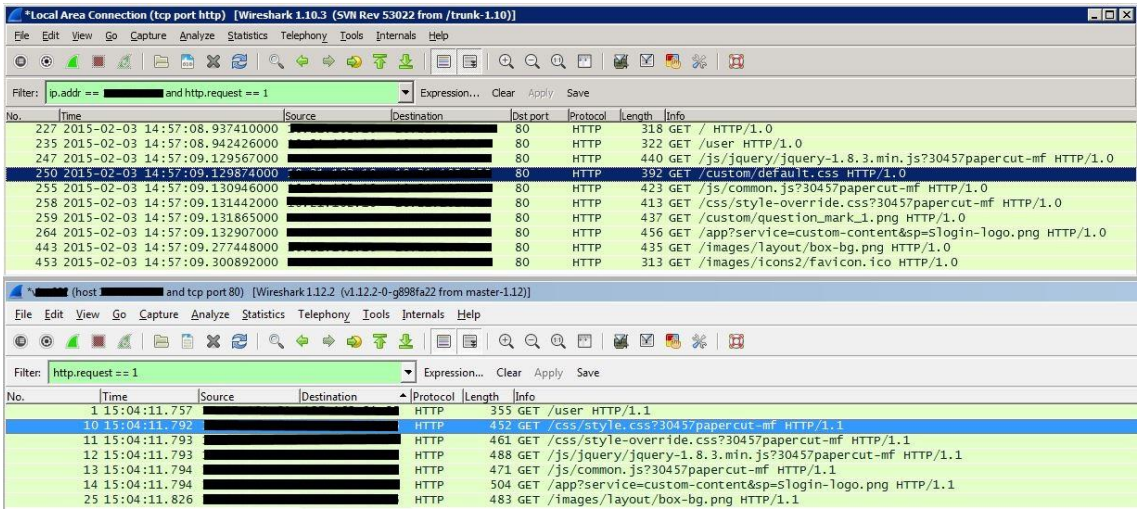
Kuva 21. Netscler Content Rewrite Policy - GET-pyynnön polun tarkistaminen

Lopuksi Netscaler-laitteeseen konfiguroitiin rewrite-sääntö (kuva 21), joka tarkastaa laitteen läpi virtaavat http-pyynnöt etsien niiden resurssipolusta tekstiä ”/css/style.css”. Mikäli pyynnön resurssipolku alkaa kyseisellä tekstillä, suorittaa Netscaler sääntöön kiinnitetyn toiminnon, jonka tehtävänä tässä tapauksessa on muuttaa http-pyynnön polku muotoon ”css/default.css” (kuva 22).



Kuva 22. Netscaler content rewrite action - http-pyynnön polun muuttaminen

Kun Netscaler -asetukset oli konfiguroitu, tarkastettiin asetusten toiminta Wireshark-ohjelmalla siten, että verkkoliikennettä tarkkailtiin sekä pyynnön suorittavalta työasemalta että palvelimelle saapuvasta liikenteestä. Kuvasta 23 on esitetty sekä palvelimelta että työasemasta tallennettu verkkoliikenne. Kuvasta voidaan havaita, että Netscaler-palvelimen konfigurointi onnistui, koska alkuperäisen http-pyynnön resurssipolku "/css/style.css?30457papercut-mf" on palvelimelle saapuessaan muuttunut muotoon ”/custom/default.css”.



Kuva 23. Content Rewrite -toiminnan tarkastaminen Wireshark-ohjelmalla

Papercut-järjestelmän kirjautumissivu on käännetty suomen kielelle vain osittain. Koska ulkoasun ja tekstien muokkaus ei onnistunut suoraan sovellukseen, päätettiin sivuton muokkaus toteuttaa Netscalerin avulla. Tämä toteutettiin luomalla kuormanjako-virtuaalipalvelimelle Content Rewrite -toiminto sekä -käytäntö.

```
add rewrite action rew_act_ppcut_replace_register_fi
replace_all "HTTP.RES.BODY(10000)" "\"Rekisteröidy\""
-pattern "New User"
```

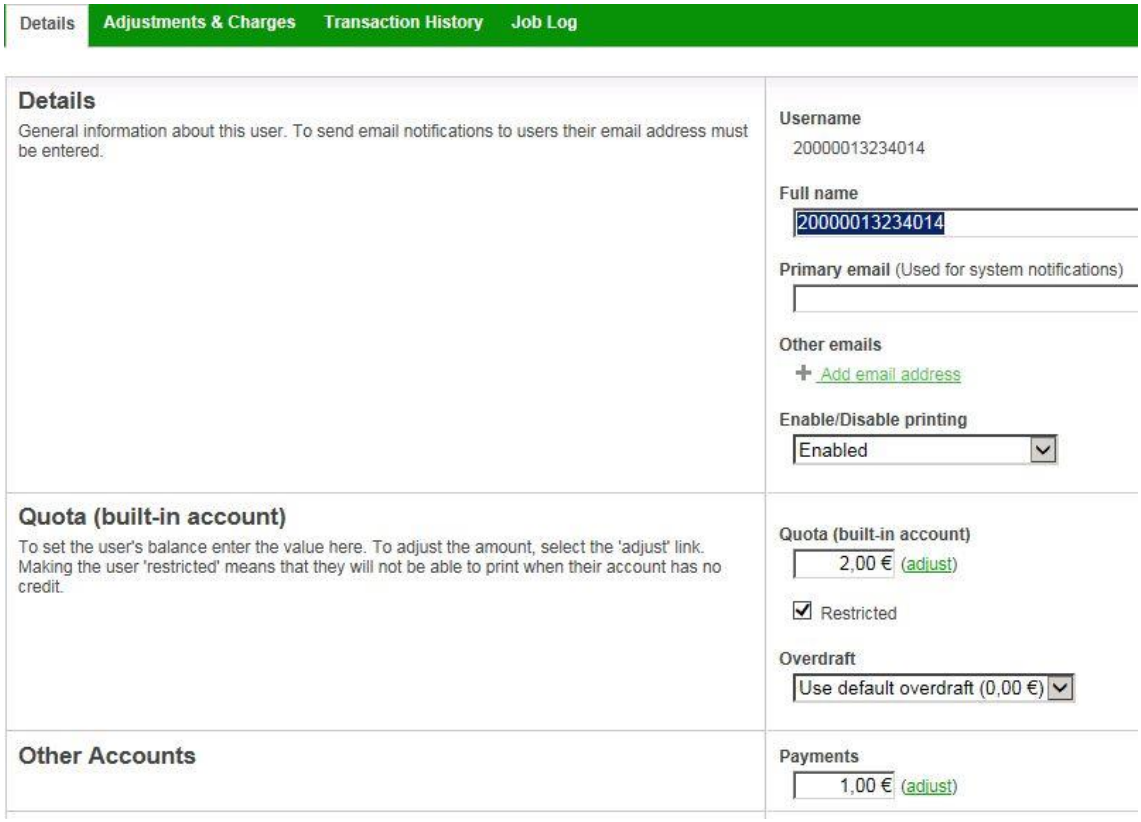
Edellisessä komennossa on kuvattuna toiminto, joka muuttaa englanninkielisen “New User” -tekstin suomenkieliseen muotoon “Rekisteröidy”. Komennossa hyödynnetään regex-lauseketta, joka etsii HTTP:n hyötykuorman ensimmäisestä 10000 merkistä ”New User” -merkkijonoa. Mikäli merkkijono löytyy, korvataan se toisella merkkijonolla ”Rekisteröidy”

```
add rewrite policy pol_loginpage_repl_register_fi
"HTTP.REQ.URL.PATH_AND_QUERY.REGEX_MATCH(re~^(/user|/a
pp)$~) && HTTP.REQ.HEADER(\"Accept-
Language\").REGEX_MATCH(re~^(fi-FI|fi$|fi,)~) &&
HTTP.RES.BODY(10000).REGEX_MATCH(re~<title>Login</titl
e>~)" rew_act_ppcut_replace_register_fi
```

Edellinen komento luo rewrite-säännön, joka suorittaa `rew_act_ppcut_replace_register_fi` -nimisen toiminnon. Säännön määrittelyssä hyödynnetään regex-lausekketta tarkistamaan http-hyötykuormasta sivun otsikko sekä http-otsikkotiedoista selaimen kielivalintatieto. Mikäli molemmat etsittävät parametrit täsmäävät, suoritetaan säännössä määritetty toiminto. Kaikki ulkoasun muokkaukseen liittyvät toiminteet on kuvattu tarkemmin liitteessä 1.

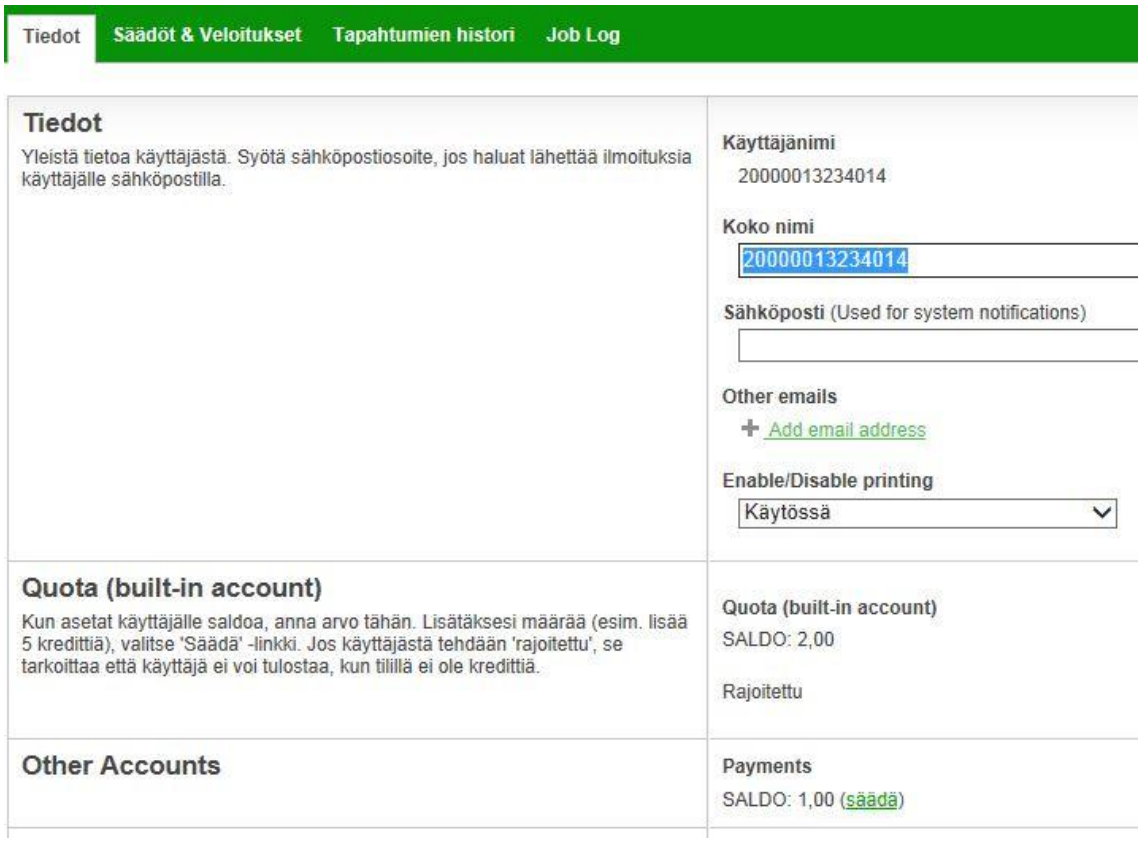
3.4.2 Ylläpitosivujen muokkaus

Järjestelmän ylläpitosivuston muokkaukseen ei tarjota sovelluksen toimittajan puolelta merkittäviä muokkausmahdollisuuksia. Järjestelmän mahdollistamat käyttöoikeuksien rajoitukset eivät mahdollistaneet riittävällä tasolla toiminteiden poissulkemista ylläpitoliittymästä. Järjestelmän kautta suoritetut käyttöoikeuksien määrittelyt altistivat myös tunnusten ylläpidon osalta huomattavan määrän virhemahdollisuuksia päivittäisen ylläpidon osalta. Tästä syystä käyttöliittymästä päätettiin poistaa sekä muokata sisältöä Netscaler-palvelimella ennen sen välitystä työaseman web-selaimelle.



Kuva 24. Ylläpitoliittymä ennen muokkauksia

Kuvassa 24 on esitetty Papercut-järjestelmän oletusnäkymä asiakastietoihin. Järjestelmän tarjoamia rajoitteita käyttäen ei ollut mahdollista estää esimerkiksi käyttäjän kiintiö-tilin muutosta ylläpitäjiltä siten, että heillä olisi ollut kuitenkin mahdollisuus muokata käyttäjän maksutiliä. Maksutilin toimintaa testattaessa havaittiin myös, että järjestelmällä on erilainen toimintalogiikka riippuen siitä, lisätäänkö käyttäjän maksutilille saldoa käyttäjän tiedot -sivulta vai käyttäjän ”säädöt ja veloitukset” -sivulta.



Kuva 25. Ylläpitoliittymä muokkausten jälkeen

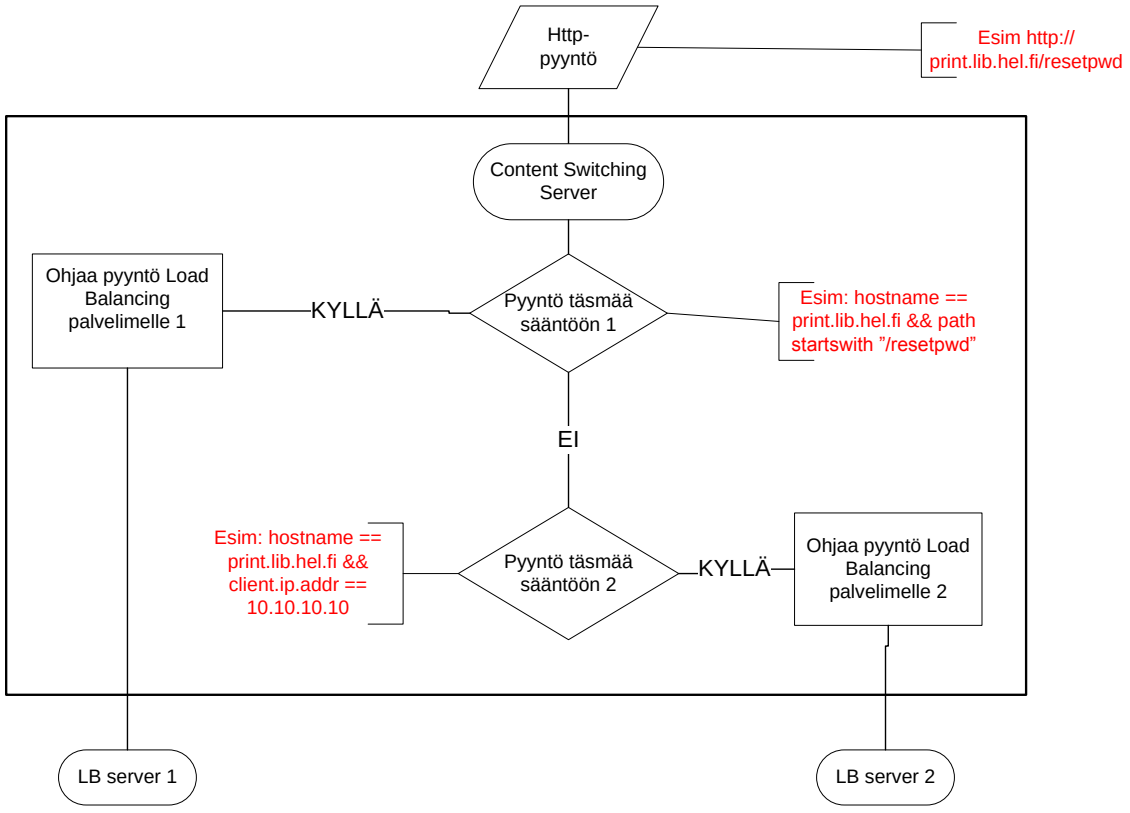
Kuvassa 25 esitetään asiakkaan tiedot -sivun ulkoasu muutosten jälkeen. Asiakkaan kiintiö-tilin muutosmahdollisuus on poistettu siten, että sen saldo esitetään edelleen sivustolla tekstimuotoisena. Samoin on poistettu muutosmahdollisuus maksutilin muokkaamiseen asiakkaan tiedot -sivulla. Edelleen nykyinen saldo esitetään tekstimuotoisena. Käyttäjän maksutilin saldoa on mahdollisuus muokata ”Säädöt ja veloitukset” -sivulla.

4 Netscaler-palvelimen asetukset

Netscaler-palvelinta hyödynnettiin Papercut-järjestelmän toteutuksessa reverse proxy -palvelimena sekä käyttäjän tunnistamisessa. Reverse proxy -toiminnallisuuden avullaPapercut-palvelu pystyttiin julkaisemaan julkiseen Internetiin suojatusta sisäverkosta. Tämän lisäksi palvelimen avulla muokattiin taustajärjestelmän välittämää http- ja html- sisältöä käyttämällä Content rewrite -säännöstöjä.

4.1 Content Switching

Content switching on Netscaler-palvelimen tekniikka, jonka avulla saapuvia pyyntöjä voidaan ohjata eri taustapalveluihin säätöpohjaisesti. Content Switching -teknologian avulla voidaan myös säästää ip-osoitteita luomalla yksi Content Switching -virtuaalipalvelin, jolle määritetään julkinen ip-osoite. Varsinaiset sovelluspalvelimet voivat käyttää ip-osoitteiden hallinnasta vastaavan IANA-organisaation määrittämiä sisäiseen käyttöön tarkoitettuja ip-osoitteita, koska kaikki yhteydet julkisista verkoista muodostetaan Content switching -palvelimeen, joka välittää pyynnöt eteenpäin taustapalveluille. Käytettäessä Content switching -virtuaalipalvelinta voidaan Load Balancing -virtuaalipalvelimet konfiguroida ilman ip-osoitteita, koska niihin ei muodosteta suoria yhteyksiä asiakastietokoneista. Content Switching -virtuaalipalvelimessa voidaan myös hyödyntää SSL-Offload-ominaisuutta, jolloin Netscaler-palvelimeen asennetaan SSL-sertifikaatti. Yhteyksien salaus puretaan Content Switching -virtuaalipalvelimella, josta eteenpäin yhteydet voidaan toteuttaa taustapalveluihin joko salaamattomina tai hyödyntäen yrityksen omia sisäisiä varmenteita.



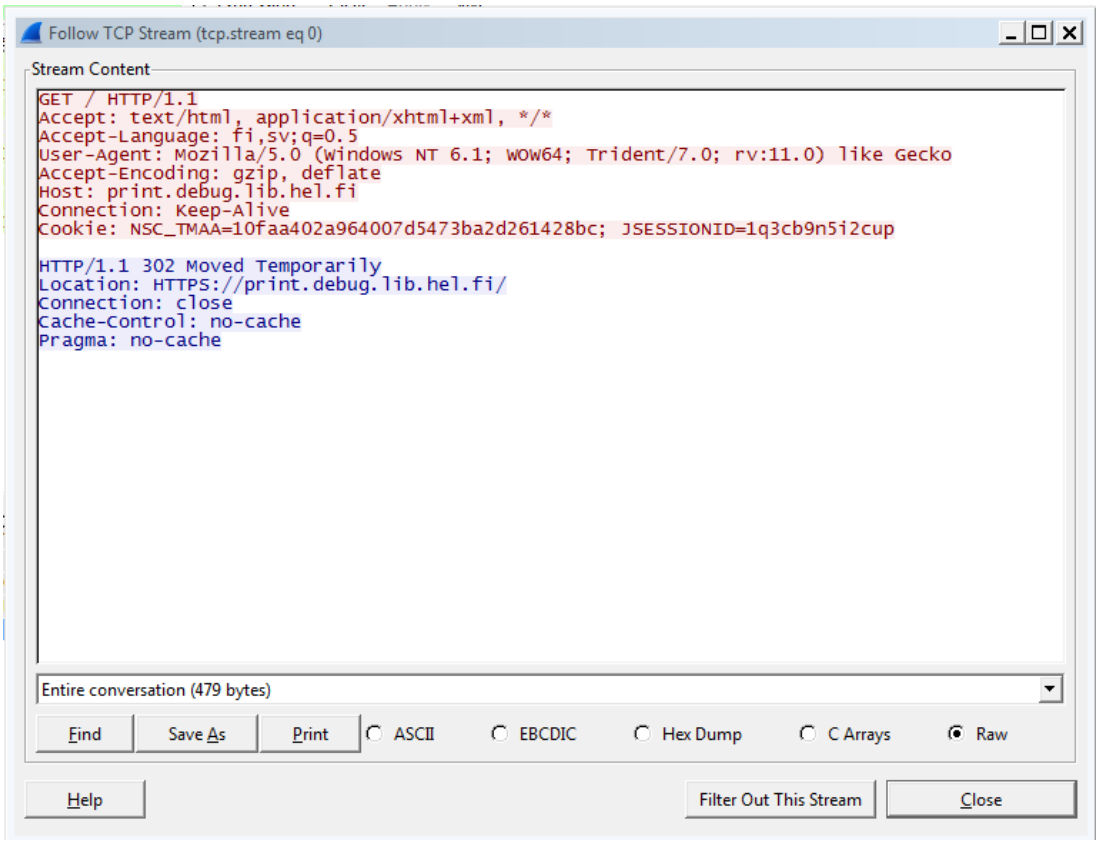
Kuva 26. Content Switching -palvelimen toiminta

Kuvassa 26 on esitetty Content Switching -virtuaalipalvelimen toimintaperiaate. Palvelin vastaanottaa http-pyynnön ja vertaa sitä määriteltyihin sääntöihin. Säännöillä on järjestysnumero, jonka mukaisessa järjestyksessä niitä käydään läpi. Kun palvelin löytää säännön, joka täsmää pyyntöön, suoritetaan http-pyynnön ohjaus säännössä määritettyyn virtuaalipalvelimeen. Virtuaalipalvelimella ei tarvitse olla erillistä ip-osoitetta, mikäli kaikki siihen muodostettavat yhteydet luodaan Content switching -palvelimen kautta. Säännöstöissä voidaan käyttää erittäin laajasti erilaisia parametrejä liittyen pyyntöön, kuten lähde- ja kohde-ip-osoitteita sekä ip-avaruuksia sekä http-kyselyn otsikkotietoja kuten isäntänimeä ja resurssipolkua. Tämän lisäksi on tarjolla myös muita vaihtoehtoja, mutta niitä ei käsitellä tässä yhteydessä, koska niitä ei tarvita järjestelmän kokonaisratkaisun toteutuksessa.

Testiä varten luotiin kaksi Content switching -virtuaalipalvelinta: ”http-debug.lib.hel.fi” sekä ”SSL-debug.lib.hel.fi”. http-debug.lib.hel.fi -palvelin vastaa standardiin http-porttiin 80. Palvelimen ainoa tehtävä on saapuvat http-pyynnöt käyttämään suojattua ssl-yhteyttä. Tämä toteutettiin luomalla Traffic Management responder -toiminto sekä -sääntö ja kiinnittämällä tämän jälkeen sääntö Content Switching -palvelimeen. Käytetyt komennot on esitetty seuraavana:

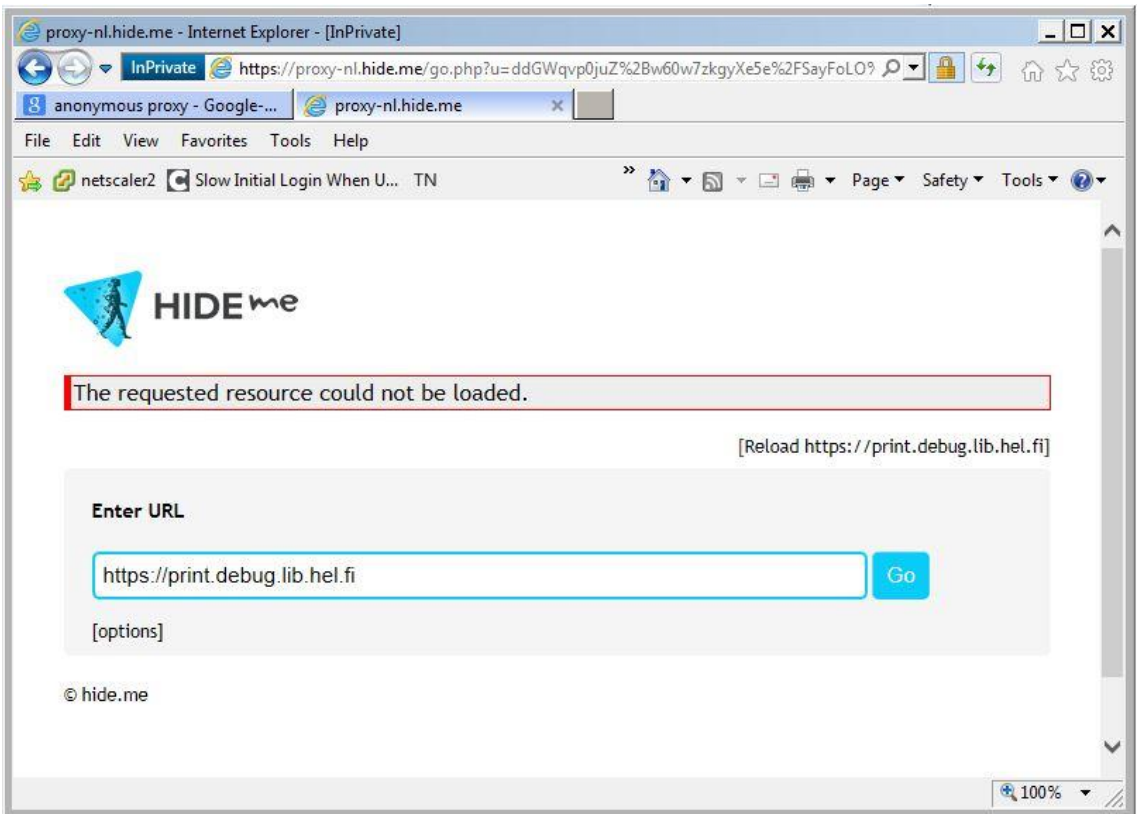
```
add responder action redirect_to_HTTPS redirect "\"HTTPS://\" +
HTTP.REQ.HEADER(\"Host\") +  HTTP.REQ.URL.PATH_AND_QUERY" -
bypassSafetyCheck YES

add responder policy pol_Redirect_TO_HTTPS "CLIENT.TCP.DSTPORT.EQ(80)"
redirect_to_HTTPS -logAction LogClientandHTTP

bind cs vserver HTTP-debug.lib.hel.fi -policyName pol_Redirect_TO_HTTPS -
priority 100 -gotoPriorityExpression END -type REQUEST
```

Salaamattoman yhteyden uudelleenohjaus salattuun yhteyteen testattiin luomalla http-pyyntö selaimella osoitteeseen http://print.debug.lib.hel.fi. Pyyntöä havainnointiin Wireshark-ohjelmalla (kuva 27). Havaintojen perusteella voitiin todeta, että tehty asetus toimii suunnitellusti.



Kuva 27. Salaamattoman http-pyynnön ohjaus salattuun yhteyteen

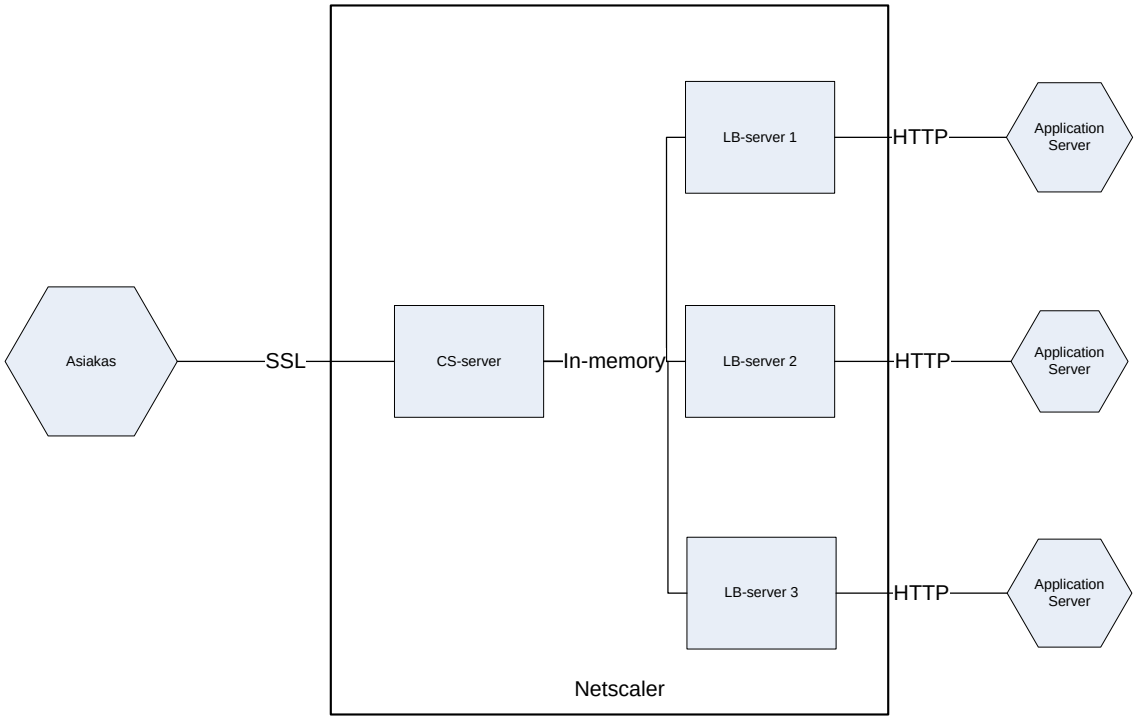
Testissä haluttiin myös varmistaa, että palvelun käyttö voidaan rajoittaa vain Suomesta saapuviin yhteyksiin. Tällä voidaan osaltaan estää mm. palveluun kohdistuvia verkkohyökkäyksiä. Tätä varten Netscaler-palvelimelle ladattiin MaxMind-yrityksen web-sivustolta GeoIP-Country-tiedosto, joka sisältää maan, johon ip-osoite on rekisteröity. Tämän jälkeen netscaler konfiguroitiin hyödyntämään tiedostoa komennolla: `add locationfile /var/geoip/GeoIPCountryWhois.csv -format GeoIP-Country`. GeoIP-tietokannan käyttöönoton jälkeen luotiin ulkomailta saapuvien yhteyksien estämistä varten responder-sääntö ”res-pol-geoip-fin-allow”.



Kuva 28. GeoIP-toiminnon testaus

Tämän jälkeen toiminto testattiin pyrkimällä muodostamaan yhteys sivustoon ulkomailla sijaitsevan anonyymi-välityspalvelimen kautta (kuva 28). Toiminto tarkistettiin lisäksi Netscalerin käyttöliittymästä, josta todettiin pyynnön täsmänneen sääntöön.

Palvelussa haluttiin hyödyntää Netscalerin tarjoamaa mahdollisuutta ssl-salauksen purkamiseen Content Switching -virtuaalipalvelimella. Tätä varten CS-palvelimelle luotiin yksityinen sertifikaatti ”*.debug.lib.hel.fi”. Tämän jälkeen yhteydet testijärjestelmässä taustapalveluihin muodostettiin yrityksen sisäisessä verkossa salaamattomana. Toiminnon logiikka on esitetty tarkemmin kuvassa 29.



Kuva 29. SSL-salauksen purku Content Switching -palvelimella

Tulostuspalvelun toteutuksessa hyödynnetään kahta eri sovelluspalvelinta: Papercutjärjestelmän sovelluspalvelinta sekä resetpwd-palvelun tuottavaa palvelinta. Tämän lisäksi yhteydet Papercut-palveluun haluttiin ohjata suojatusta verkosta hyödyntäen kertakirjautumislogiikkaa, joka toteutetaan Netscaler-palvelimella. Näiden ehtojen perusteella luotiin kolme lb-palvelinta: lb1, lb2 ja lb3. Palvelimen lb1 kautta ohjataan liikenne salasanan vaihtopalveluun (”resetpwd”). Palvelimen lb2 kautta ohjataan liikenne varsinaiselle sovelluspalvelimelle, mutta yhteyden muodostusta varten käyttäjän tulee tunnistautua omalla lähiverkkotunnuksellaan. Palvelimen lb3 kautta muodostetaan normaalit asiakasyhteydet. Edellä mainittujen määritysten toteuttamiseksi luotiin kolme sääntöä, joiden tuli täyttää seuraavat ehdot:

- Sääntö 1: Mikäli http-pyynnön polku alkaa merkkijonolla ”/resetpwd”, pyyntö tulee ohjata palvelimelle lb1.
- Sääntö 2: Mikäli yhteys on muodostettu ylläpitoverkosta, pyyntö tulee ohjata palvelimelle lb2.
- Sääntö 3: Mikäli mikään edellä mainittu ei täsmää, muodostetaan yhteys palvelimelle lb3.

Edellä mainitussa listauksessa Load Balancing -virtuaalipalvelimien nimiä edustavat ainoastaan numerot selkeyden vuoksi. Virtuaalipalvelinten asetukset on kuvattu

tarkemmin kappaleessa 4.2 ”Load Balancing Virtual Servers”. Säännöt on kuvattu liitteessä 1.

4.2 Load Balancing Virtual Servers

Load Balancing -virtuaalipalvelimia määritettiin testiympäristöön kolme kappaletta (taulukko 1). Palvelimiin kiinnitettiin rewrite-säännöstöjä, joilla muokataan mm. html-koodia sen virratessa laitteen läpi palvelimelta työasemaan sekä muokataan http-liikenteen otsikkotietoja.

Taulukko 1. Load Balancing virtual servers

LB Palvelin	**Taustapalvelu**	**selite**
HTTPS-resetpwd	01printsrv02:8080	LB palvelin ohjaa liikenteen resetpwd-palveluun taustajärjestelmän tcp portissa 8080
HTTPS-admin	01printsrv02:443	LB ohjaa liikenteen Papercut-palveluun. Käytetään ,kun liikenne saapuu henkilökunnan lähiverkon osoite-avaruudesta. Palvelin vaatii selaimelta integroidun käyttäjätunnistuksen
HTTPS-default	01printsrv02:443	Ohjaa liikenteen papercut-palveluun

Netscaler-palvelimen Content switching -toiminnallisuus ohjaa saapuvan liikenteen ”HTTPS-admin”-palvelimelle, kun järjestelmän ylläpitoliittymään kirjaudutaan luotetusta verkosta. Palvelin autentikoi käyttäjän selaimen välittämän kerberos-tiketin perusteella sekä lisää taustajärjestelmään lähetettävään http-pyyntöön http-otsikon ”x-username”, jonka parametriksi tulee kerberos-tiketistä saatava käyttäjänimi. http-otsikkotiedon lisäys toteutettiin Content rewrite -ominaisuuden avulla. Ensin luotiin toiminto (action), joka lisää otsikkotiedon, ja tämän jälkeen luotiin sääntö, mikä suorittaa toiminteen, mikäi siinä määritetyt ehdot täyttyvät. Lopuksi sääntö kiinnitettiin lb-palvelimeen. Toiminto, sääntö sekä kiinnitys lb-palvelimeen on kuvattu seuraavana komentoriviltä toteutettuna.

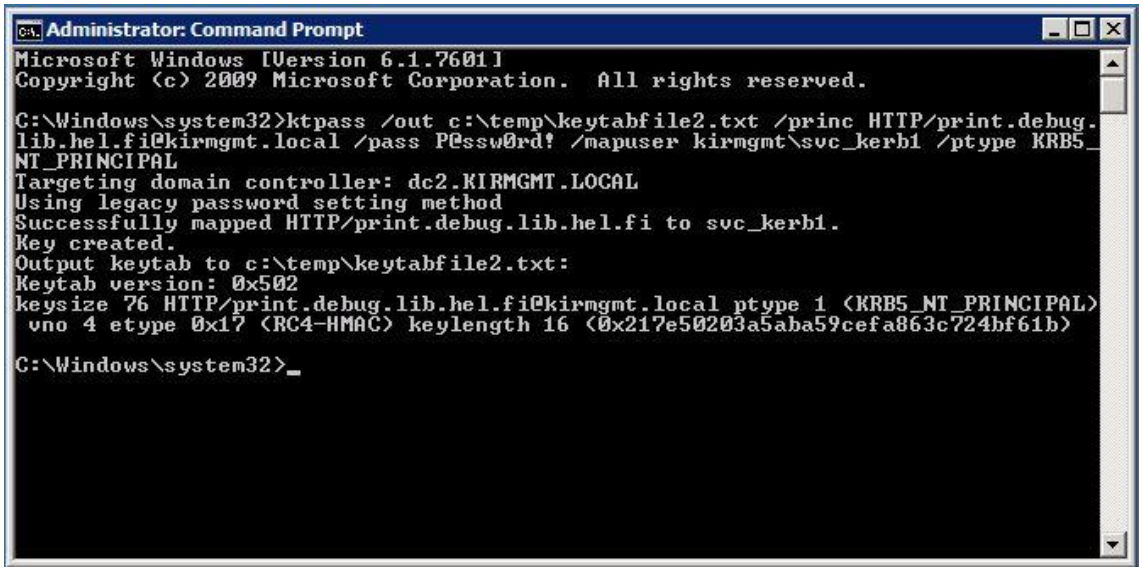
```
add rewrite action ACT_TESTI_ADD_HEADER insert_http_header x-username
HTTP.REQ.USER.NAME -bypassSafetyCheck YES
```

```
add rewrite policy POL_TESTI_ADD_HEADER "HTTP.REQ.HEADER(\"x-username\").EXISTS.NOT"
ACT_TESTI_ADD_HEADER

bind lb vserver HTTPS_admin -policyName POL_TESTI_ADD_HEADER -priority 100 -
gotoPriorityExpression END -type REQUEST
```

Halutun lopputuloksen aikaansaamiseksi jouduttiin Netscaler-palvelimelle luomaan useita Content Rewrite -säännöstöjä. Nämä säännöstöt sekä esimerkki säännön toteuttamisesta on esitetty liitteessä 1.

4.3 Kerberos-autentikointi

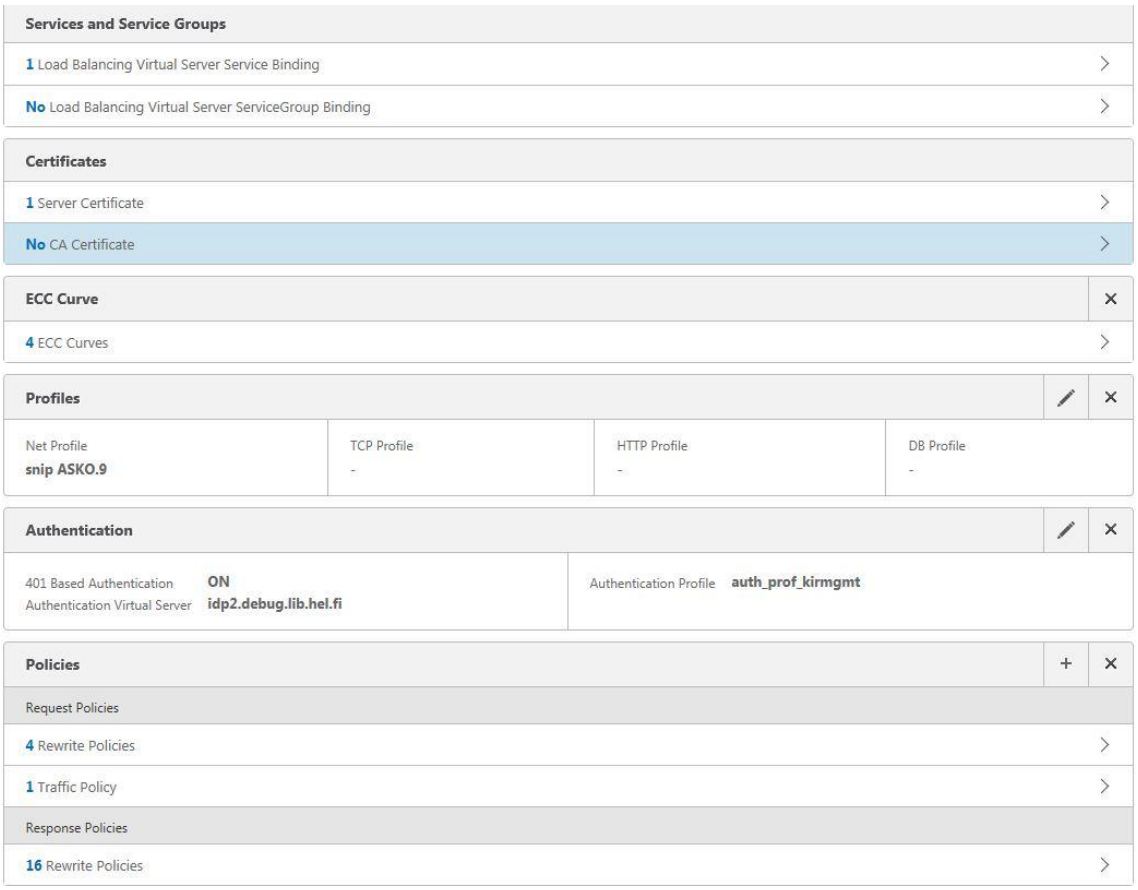
Netscaler-palvelimessa käyttäjien tunnistamisesta vastaa AAA-palvelin. Palvelin voi autentikoida käyttäjän monella eri tavalla kuten LDAP-, Radius- sekä Kerberos- ja NTLM-protokollien avulla. Tässä opinnäytetyössä määritettiin Netscalerin AAA-virtuaalipalvelin tunnistamaan käyttäjät integroidulla Windows-todennuksella hyödyntäen Kerberos-protokollaa. Toimintoa varten Netscaleriin luotiin AAA-palvelin idp2.debug.lib.hel.fi, joka huolehtii käyttäjien tunnistuksesta. Jotta Kerberos-todennus onnistuisi, luotiin palvelimelle oma palvelutunnus aktiivihakemistoon.



Kuva 30. Keytab-tiedoston luonti

Tämän jälkeen tunnukselle lisättiin Service Principal Name -attribuutin arvoksi http/print.debug.lib.hel.fi käyttäen Windowsin ktpass-sovellusta (kuva 30). Samalla

sovelluksella luotiin myös Netscaler-palvelimelle ladattava keytab-tiedosto, joka sisältää palvelun nimen sekä kryptatun avaimen (An Introduction to Keytabs 2010). Vastaanottaessaan Kerberos-tiketin AAA-palvelin purkaa sen salauksen käyttämällä keytab-tiedoston määrittämää avainta.



Kuva 31. LB-palvelimen käyttäjätunnistuksen määritys

Kuvassa 31 on esitetty käyttäjän tunnistuksen määritys virtuaalipalvelimeen. Kuvasta havaitaan, että todennusmenetelmänä käytetään 401-perusteista todennusta, mikä tarkoittaa, että palvelin pyytää selainta todentamaan käyttäjän hyödyntäen SPNEGOTIATE-käytäntöä (Jaganathan ym. 2006). Tuettuja todennusmenetelmiä ovat NTLM ja Kerberos. Selain vastaa palvelimen viestiin lähettämällä uudelleen sivupyynnön sisältäen nyt palvelua varten KDC-palvelimelta pyytämänsä kerberos-tiketin. Netscaler lb -palvelin välittää tiketin AAA-palvelimelle idp2.debug.lib.hel.fi. Mikäli AAA-palvelin kykenee purkamaan tiketin suojauksen käyttämällä omaa kerberos-avaintaan, on paketti luotetun KDC-palvelimen myöntämä, ja käyttäjä päästetään järjestelmään. Tämän jälkeen AAA-palvelin palauttaa tiedon onnistuneesta autentikoinnista lb-palvelimelle, joka jatkaa liikenteen normaalia prosessointia.

5 Tietoturva

Järjestelmän tietoturvaa tarkasteltiin suunnittelu- ja toteutusvaiheessa monesta näkökulmasta: verkkoliikenteen salauksen, verkkoliikenteen palomuuriasetusten, salasanojen, ylläpitoyhteyksien sekä SQL-palvelimen tietoturvan näkökulmasta. Tässä luvussa käydään läpi tärkeimmät tietoturvaan liittyvät asiat näistä osa-alueista.

Verkkoliikenteen salauksella tarkoitetaan liikenteen sisällön suojaamista siten, että ulkopuolinen taho ei voi tarkastella sen sisältöä. Tyypillinen tapa toteuttaa verkkoliikenteen salaus on suojata se SSL/TLS-tekniikalla. Tämä metodi on käytössä Internet-liikenteen suojauksessa. Toinen tapa suojata verkkoliikenteen sisällön suojaamiseen on IPSEC-tunnelointi. Tämä metodi soveltuu kuitenkin enimmäkseen sisäverkon liikenteen salaukseen sekä Internetin yli tapahtuvien VPN-yhteyksien salaamiseen. Tulostusjärjestelmässä kaikki http-liikenne suojattiin ssl-tekniikalla. Palvelua varten hankittiin palvelinsertifikaatti, jonka myöntäjänä toimii TeliaSonera Server CA v1. Kyseisen myöntäjän sertifikaatti on asennettuna valmiiksi Internet explorer-, Chrome- sekä Firefox-selaimiin. Sertifikaatti asennettiin Netscaler load balancing -palvelimelle, joka toimii reverse proxy -palvelimena kaikille Papercut-palveluun suuntautuville http(s)-yhteyksille. Netscaler-laitteelta taustajärjestelmään eli Papercut-palvelimelle yhteys suojattiin käyttäen yrityksen sisäisen varmennepalvelimen myöntämää sertifikaattia, joka on asennettu Papercut-palvelimelle. Näillä asetuksilla http-yhteys suojataan kokonaisuudessaan asiakkaalta sovelluspalvelimelle asti, eikä verkkoliikennettä voida ulkopuolisen toimesta tarkastella.

Yleinen tapa suojata verkkopalveluita ja palvelimia on suojata ne palomuurilla estäen asiaan kuulumaton verkkoliikenne palvelimelle. Palomuurit suodattavat liikennettä useimmiten OSI-mallin tasoilla 3,4 ja 7 (Firewall_(computing) 2015). Tulostusjärjestelmän palvelimet suojattiin Windows-palvelimen omalla palomuurilla sekä erillisellä palomuurilaitteistolla, joka kykenee analysoimaan ja suodattamaan liikennettä myös OSI-mallin sovelluskerroksella 7. Paikallisella palomuurilla suojattiin palvelin siten, että siihen voidaan muodostaa ylläpitotehtävissä käytettäviä etätyöpöytäyhteyksiä ainoastaan erillisestä ylläpitoverkosta. Tämän lisäksi avattiin Papercut-palvelun tarvitsemat portit 80 ja 443. Muut järjestelmään suuntautuvat yhteydet estettiin. Erillisellä palomuurilaitteistolla suojataan yhteyksiä julkisesta verkosta DMZ-alueella sijaitsevalle Netscaler-palvelimelle sekä DMZ-alueelta Papercut-palvelimelle suuntautuvaa liikennettä.

Salasanojen suojauksella estetään tai vaikeutetaan salasanojen lukemista, mikäli ne saadaan haltuun tietokannasta. Salasanan tallentamisessa suositellaan käytettäväksi salasanan tarkistussummaa, joka on muodostettu salasanasta sekä satunnaisesta merkkijonosta, josta käytetään sanontaa suolaus. Salasanan tarkistussumman suolauksella vaikeutetaan merkittävästi salasanojen murtamiseen kuluvaa aikaa, koska sillä estetään valmiiden salasana-tarkistussummataulukoiden käyttö salasanan murtamisessa (Safe Password Hashing). Papercut-järjestelmässä on kahdenlaisia käyttäjätunnuksia - erilliseen käyttäjähakemistoon tallennettuja sekä järjestelmän sisäisessä tietokannassa ylläpidettäviä käyttäjätunnuksia. Erillisissä käyttäjähakemistoissa sijaitsevien käyttäjätunnusten salasanat on suojattu hakemiston omalla suojausmenettelyllä eikä tässä dokumentissa oteta kantaa niiden turvallisuuteen. Papercut-palvelimelle ei tallenneta eikä sijoiteta välimuistiin erillisissä käyttäjähakemistoissa sijaitsevien käyttäjätunnusten salasanoja tai näiden tarkistussummia (How/where are the "internal user" passwords stored? 2011).

Järjestelmän sisäisten käyttäjätunnusten salasanat on suojattu käyttäen salasanasta sekä käyttäjätunnuksesta ja siihen lisätystä suolausta muodostettua tarkistussummaa (How/where are the "internal user" passwords stored? 2011). Järjestelmään voidaan myös kirjautua käyttäjätunnukseen sidottua toimikorttia sekä pin-koodia hyödyntämällä. Järjestelmää tutkittaessa havaittiin, että ylläpitoliittymässä käyttäjän pin-koodi voidaan esittää selväkielisenä. Tämän perusteella pääteltiin, että pin-koodia ei ole voitu tallentaa käyttäen samaa yksisuuntaista suojausta kuin salasanojen tallennuksessa. Asiaa tutkittiin tarkastelemalla järjestelmän tietokantaa, jolloin havaittiin, että pin-koodin on tallennettu järjestelmän tietokantaan selväkielisenä. Tämä muodostaa merkittävän riskin, mikäli mahdollinen murtautuja onnistuu pääsemään käsiksi tietokantapalvelimelle. Havaintojen perusteella tehtiin tukipalvelupyyntö Papercut-järjestelmän valmistajalle, joka päätti toteuttaa pin-koodin salauksen käyttäen samaa algoritmia kuin salasanojen tallennuksessa. Ominaisuus on lisätty järjestelmän versioon 15.

Kuva 32. PIN-koodin salaus tietokannassa

Palvelimen päivityksen jälkeen muutos pin-koodin tallennuksessa tarkastettiin kuvassa 32 näkyvällä SQL-kyselyllä. Kuvasta havaitaan, että muutoksen jälkeen rekisteröity pin-koodi (user_id 15015) on tallennettu järjestelmän tietokantaan tarkistussummana. Ennen muutosta tallennettu pin-koodi taas on edelleen salaamaton. Testeissä havaittiin myös, että tallentamalla käyttäjätunnuksen tiedot ylläpitoliittymästä muuttamatta mitään olemassa olevia tietoja salasi käyttäjätunnuksen pin-koodin järjestelmän tietokannassa. Tätä tietoa hyväksikäyttämällä luotiin php-sovellus, joka Papercutin xmlrpc-rajapintaa hyödyntämällä salasi kaikkien olemassa olevien käyttäjätunnusten pin-koodin järjestelmän tietokannassa.

SQL-palvelimen tietoturvaa tarkasteltaessa kiinnitettiin erityistä huomiota toimikorttitietojen tarkistuksessa käytettyihin SQL-määrityksiin sekä SQL-palvelimen käyttöoikeuksiin. SQL-palvelimen käyttöoikeuksien osalta käytettiin pienimmän tarpeellisen käyttöoikeuden periaatetta. Tietokantayhteyden muodostusta varten määritettiin erillinen käyttäjätunnus, jolle määritettiin SQL-palvelimella pääsy ainoastaan Papercut-järjestelmän omaan tietokantaan. Muihin tietokantoihin tunnukselle ei myönnetty pääsyä. Järjestelmän omaan tietokantaan tunnukselle annettiin valmistajan suositusten mukainen db_owner-rooli. Toimikorttien tietojen tarkistamiseksi Papercut-järjestelmä konfiguroitiin muodostamaan yhteys erilliseen toimikorttitietokantaan SQL-lausekkeen avulla. Toimintoa varten toimikorttitietokantaan muodostettiin Stored procedure, jolle Papercut välittää toimikortinnumeron tietojen noutoa varten. Yhteydessä käytetylle käyttäjätunnukselle määritettiin tämän jälkeen toimikorttitietokantaan suoritus (EXECUTE) käyttöoikeus ainoastaan kyseiseen Stored Procedureen. Tällä estetään mahdollisten suorien select-lausekkeiden käyttäminen tietokantaa vasten, mikäli käyttäjätunnus joutuu ulkopuolisten tahojen haltuun. Lisäksi toiminnolla voidaan merkittävästi rajoittaa SQL injektio-tyyppisiä hyökkäyksiä, mikäli

hyökkääjä onnistuu ujuttamaan sql-kyselyyn omaa koodiaan. Riski tähän on kuitenkin pieni, koska kyseessä on järjestelmän sisäinen toiminto, johon ei tarjota mahdollisuutta käyttäjän omille syötteille esimerkiksi web-liittymästä.

Stored-proseduureilla voidaan mm. parantaa tietokannan turvaa SQL-injektiohyökkäyksiä vastaan (Microsoft) sekä yksinkertaistaa asiakassovellusten rakentamista piilottamalla varsinainen tietokantarakenne. Hyödyntämällä tietokannan käytössä stored-proseduureja voidaan käyttäjiltä estää suora pääsy tietokannan tauluihin, jolloin käyttäjä ei voi esimerkiksi käyttää suoraan select-lausekkeita tiedon hakemiseen. Kaikki tiedon hakeminen tietokannasta suoritetaan käyttäen Stored proseduureja, joihin käyttäjälle myönnetään suoritusoikeus (execute). Stored proseduurien määrityksissä huomioitiin, että niille välitettävät tiedot käsitellään kyselyssä Swanin esimerkin mukaisesti parametreina, jolloin niihin mahdollisesti sisältyvää sql-koodia ei suoriteta, koska se ei ole osa kyselyn suunnitelmaa (Swan 2011).

6 Yhteenveto

Projektissa käsiteltiin monipuolisesti tietotekniikka eri osa-alueita kuten verkkotekniikkaa, tulostusta, pääsynhallintaa, tietokantoja sekä salausta. Projekti osoitti, että järjestelmien käyttöönotto suurissa yrityksissä vaatii laaja-alaista osaamista eri teknologioiden osalta sekä pitkäjänteistä suunnitelmallisuutta ja itseopiskelua. Projektin tulosten perusteella toteutettiin Helsingin kaupunginkirjastolle asiakas- ja henkilökuntaympäristöön integroidu tulostuksenhallintajärjestelmä, jolla lisättiin tulosteiden tietosuojaa, pienennettiin tulostuskustannuksia sekä saavutettiin säästöjä tulostuksen asiakaspalvelutilanteisiin liittyvässä ajankäytössä.

Projekti tutustutti itseni syvällisemmin moniin jo aiemmin tuttuihin teknologioihin sekä avasi kokonaan uuden näkymän verkkoliikenteen optimointiin ja muokkaukseen Netscaler-laitteistolla. Erittäin mielenkiintoisena ja opettavaisena koin myös SSIS-palveluiden hyödyntämisen tietojen siirrossa järjestelmien välillä.

Lähteet

An Introduction to Keytabs. 2010. Verkkodokumentti. Stanford University. <https://itservices.stanford.edu/service/kerberos/keytabs>. Luettu 17.2.2015.

Demilitarisoitu alue (tietotekniikka). 2014. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/Demilitarisoitu_alue_(tietotekniikka)>. Luettu 3.1.2015.

DNS. 2015. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/DNS>. Luettu 14.12.2014.

Firewall (computing). 2015. Verkkodokumentti. Wikipedia. < http://en.wikipedia.org/wiki/Firewall_(computing)>. Luettu 18.12.2014.

Generic Security Services Application Program Interface. 2014. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Generic_Security_Services_Application_Program_Interface>. Luettu 25.2.2015.

Hypertext Transfer Protocol. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol>. Luettu 10.1.2015.

How/where are the "internal user" passwords stored?. 2011. Verkkodokumentti. Papercut. <http://www.papercut.com/kb/Main/InternalUserSecurity>. Luettu 20.2.2015.

Jaganathan K, Zhu L, Brezak J.2006. SPNEGO-based Kerberos and NTLM HTTP Authentication in Microsoft Windows. Verkkodokumentti. <http://www.ietf.org/rfc/rfc4559.txt>. Luettu 19.2.2015.

Load Balancing. Verkkodokumentti. Citrix. <http://support.citrix.com/proddocs/topic/netscaler/ns-lb-wrapper-con-93.html>. Luettu 20.2.2015.

Managing Permissions with Stored Procedures in SQL Server. Verkkodokumentti. Microsoft. <https://msdn.microsoft.com/en-us/library/bb669058(v=vs.110).aspx>. Luettu 20.2.2015.

Print processors and data types. Verkkodokumentti. Microsoft. <https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_printconcepts_cpu_datatypes.mspx?mfr=true>. Luettu 17.2.2015.

Query String. 2014. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Query_string>. Luettu 6.1.2015.

Safe Password Hashing. Verkkodokumentti. PHP Group. <http://php.net/manual/en/faq.passwords.php>. Luetty 20.2.2015.

Schemers R, Allbery R. 2014. WebAuth Technical Specification. Verkkodokumentti. <http://webauth.stanford.edu/protocol.html#rfc.section.1.1.2>. Luettu 15.2.2015.

Swan, Brian. 2011. Do Stored Procedures Protect Against SQL Injection?. Verkkodokumentti. <http://blogs.msdn.com/b/brian_swan/archive/2011/02/16/do-stored-procedures-protect-against-sql-injection.aspx>. Luettu 20.2.2015.

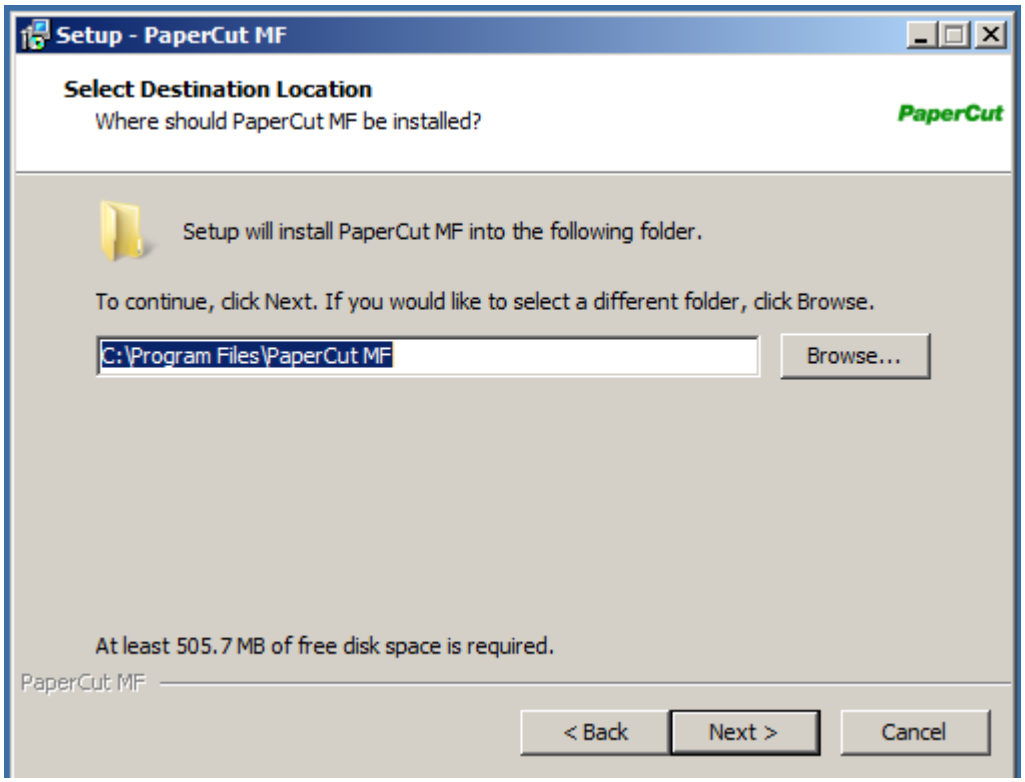
Asennuksen kuvaus

Tässä liitteessä on kuvattu Papercut järjestelmän asennus kuvakaappauksin sekä järjestelmän muut asetukset. Dokumentissa ei käsitellä Windows -palvelimen perusasennusta. Yrityksen kannalta salassa pidettävät tiedot, kuten salasanat ja ip-osoitteet on korvattu xxxx-merkinnöillä sekä kuvissa yliviivauksella.

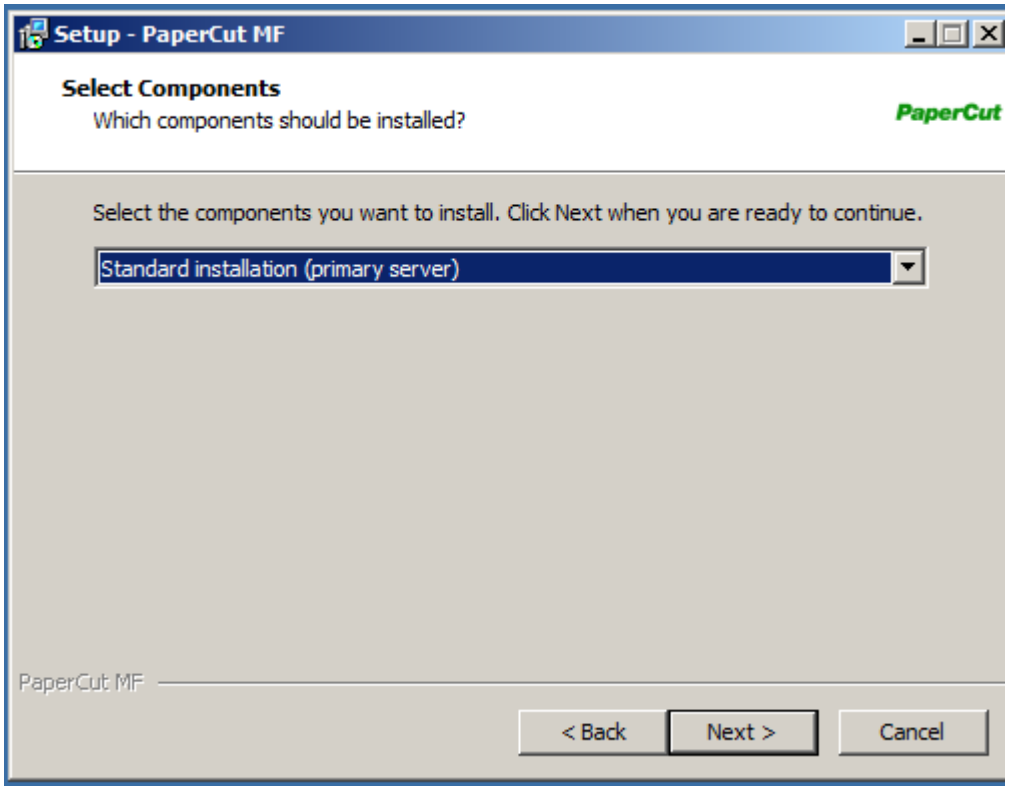
Sisällys

1 Palvelimen asennus

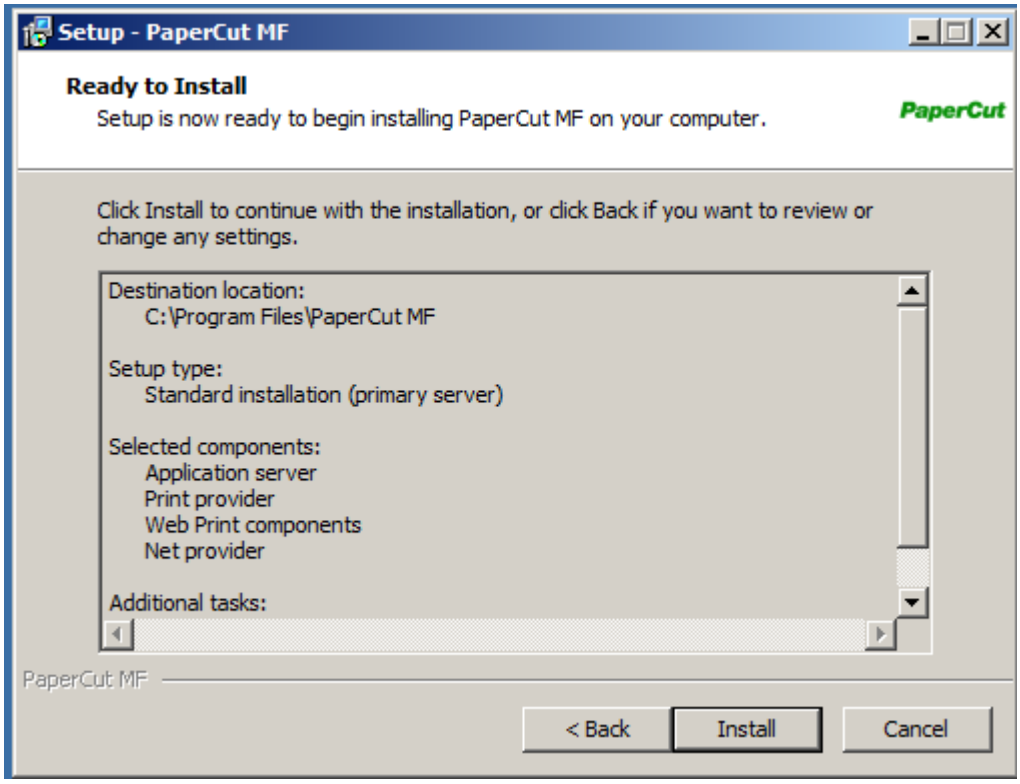
Järjestelmä asennettiin Windows Server 2008 R2 palvelimelle oletushakemistoon. Asennuksen valinnat on kuvattu alla kuvissa 1-3



Kuva 33. Asennuskansion valinta



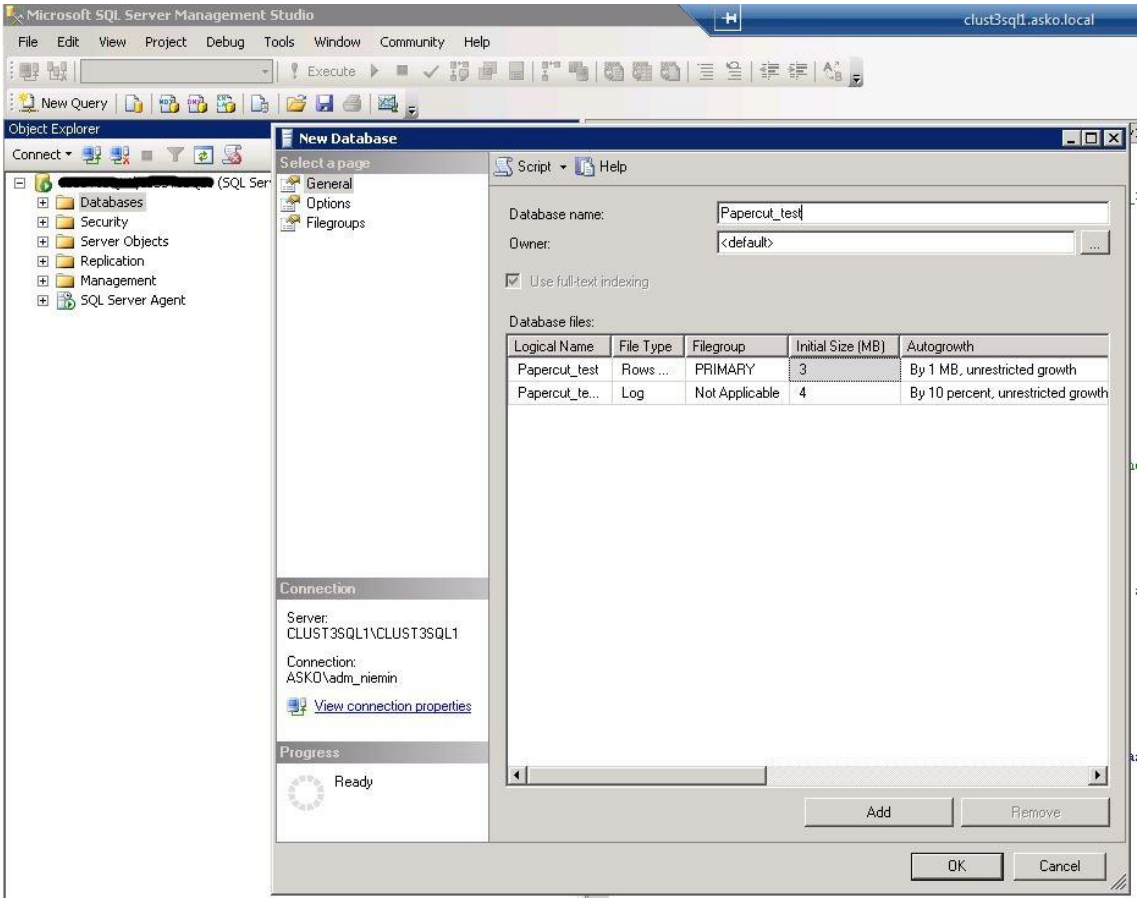
Kuva 34. Palvelimen roolien valinta



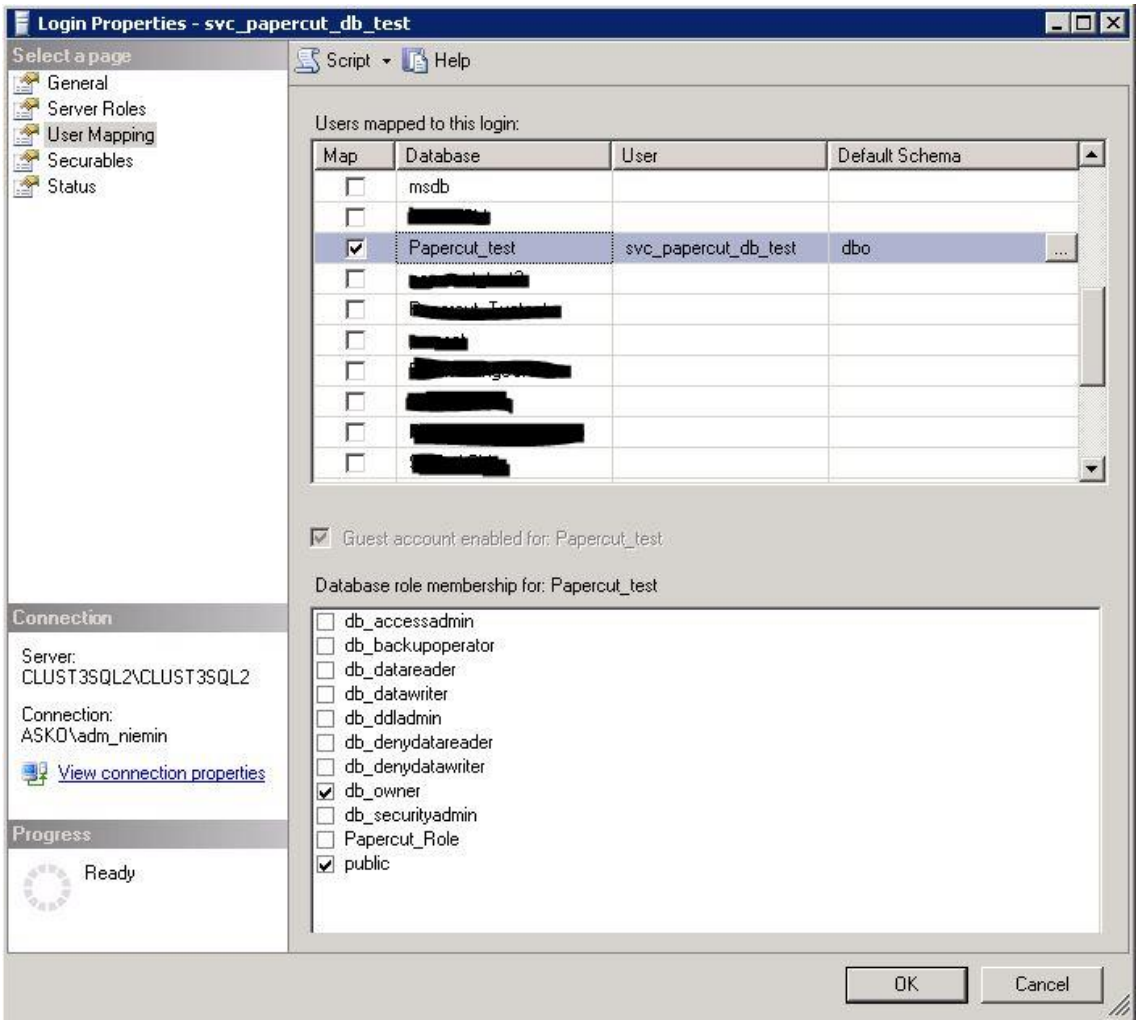
Kuva 35. Asennuksen yhteenveto

1.1 Tietokannan määritys

Asennuksen jälkeen Papercut määritettiin hyödyntämään ulkoista SQL-server tietokantaa. Aluksi erilliselle tietokantapalvelimelle luotiin tyhjä tietokanta sekä määritettiin käyttäjätunnus, jolla Papercut voi käyttää tietokantaa. Tämän jälkeen järjestelmän asetustiedostoa ”server.properties” muokattiin siten, että sinne lisättiin tietokantapalvelimen yhteystieto sekä alustettiin ensin luotu tietokanta komentoriviltä suoritettavalla init-db -komennolla (kuvat 4 -7).



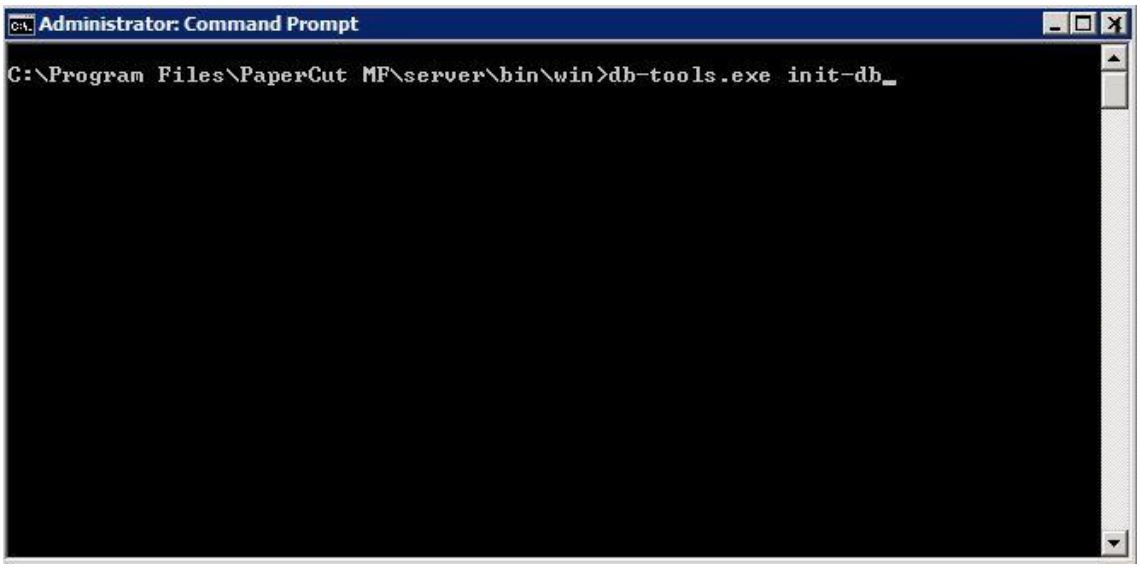
Kuva 36. Tietokannan luonti.



Kuva 37. Käyttöoikeuksien määritys tietokantaan

```
# MS SQLServer connection example
# IMPORTANT: The username below is a SQL Server user, not a Windows user.
database.type=SQLServer
database.driver=net.sourceforge.jtds.jdbc.Driver
database.url=jdbc:jtds:sqlserver://XXXXX /Papercut_test
database.username=svc_papercut_db_test
database.password=XXXXXXX
```

Kuva 38. SQL-palvelimen yhteysosoitteen lisäys asetustiedostoon



Kuva 39. Tietokannan rakenteen määritys.

1.2 Palvelimen asetukset - asetustiedosto

Papercut palvelimen tietoliikenneasetuksia sekä palvelimen sertifikaattiasetuksia hallitaan erillisen server.config-tiedoston avulla. Testiä varten palvelimen käyttämät tcp-portit muutettiin järjestelmän oletusporteista yleisesti käytössä oleviin http ja https-portteihin 80 ja 443. Tämän lisäksi palvelimelle luotiin oma sertifikaatti joka tallennettiin erilliseen avainsäilöön. Konfiguraatiotiedostossa määriteltiin avainsäiliön sijainti sekä salasana. Seuraavana on kuvattu testipalvelimen server.config-tiedosto muutosten osalta. Oletusarvoihin jätettyjä asetuksia ei ole kuvattu.

```
######### Server Config Properties #########

### Server Port (Default: 9191 and SSL: 9192) ###
# IMPORTANT: Use these options only if directed by support.
#server.port=9191
#server.ssl.port=9192
server.port=80
server.ssl.port=443
#server.force-host-header=print.debug.lib.hel.fi

### SSL Key/Certificate ###
# Custom SSL keystore example (recommend placing in the custom directory)
```

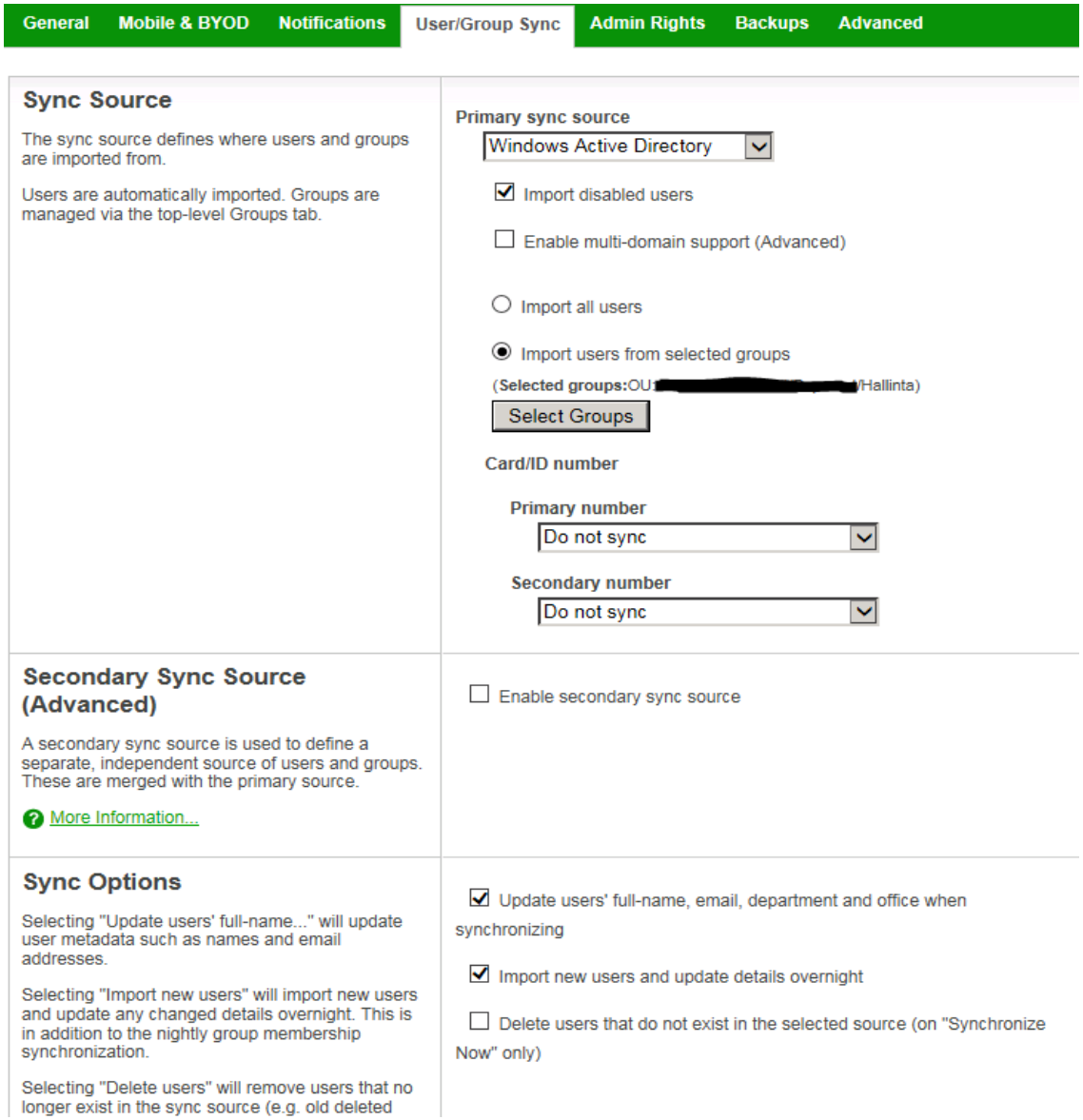
```
server.ssl.keystore=custom/01printsrv02-ssl-keystore
server.ssl.keystore-password=XXXXXXXXX
server.ssl.key-password=XXXXXXXX
```

2 Järjestelmän asetukset

Järjestelmän asetuksia hallinnoidaan web-selaimella käytettävästä ylläpitoliittymästä. Järjestelmä tallentaa kaikki asetukset tietokantaan, josta ne voidaan helposti dokumentoida esimerkiksi erilliseen csv-tiedostoon. Tämän haittapuolena on kuitenkin se, että asetusten nimestä ei kaikissa tapauksissa voida suoraan päätellä, mitä se koskee. Tästä syystä testiympäristössä käytetyt asetukset on kuvattu alla kuvakaappauksin.

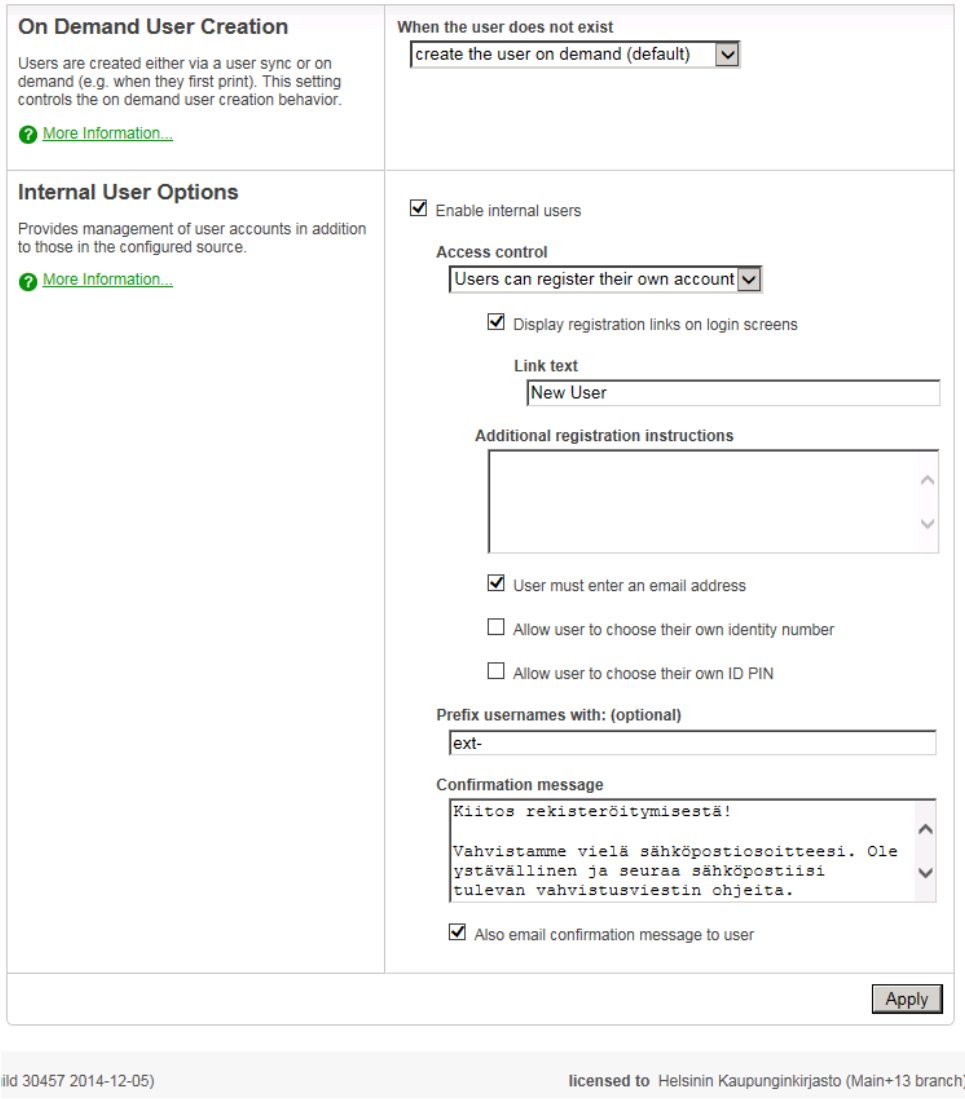
2.1 Käyttäjätietojen synkronointi

Järjestelmään tuodaan ajastetusti ylläpitäjien käyttäjätunnukset Windowsin Aktiivihakemistosta. Tämän lisäksi järjestelmä hakee asiakkaiden käyttäjätunnusten tiedot Aktiivihakemistosta ensimmäisen tulostuksen yhteydessä.



Kuva 40. Käyttäjätietojen synkronointi

Kuvan 8 mukaisesti järjestelmään tuodaan ajastetusti ainoastaan ylläpitoon käytettävät Windows-käyttäjätunnukset. Tietojen lähteeksi määritettiin Aktiivihakemiston käyttäjäryhmä joka sisältää kaikki ylläpitotunnukset.

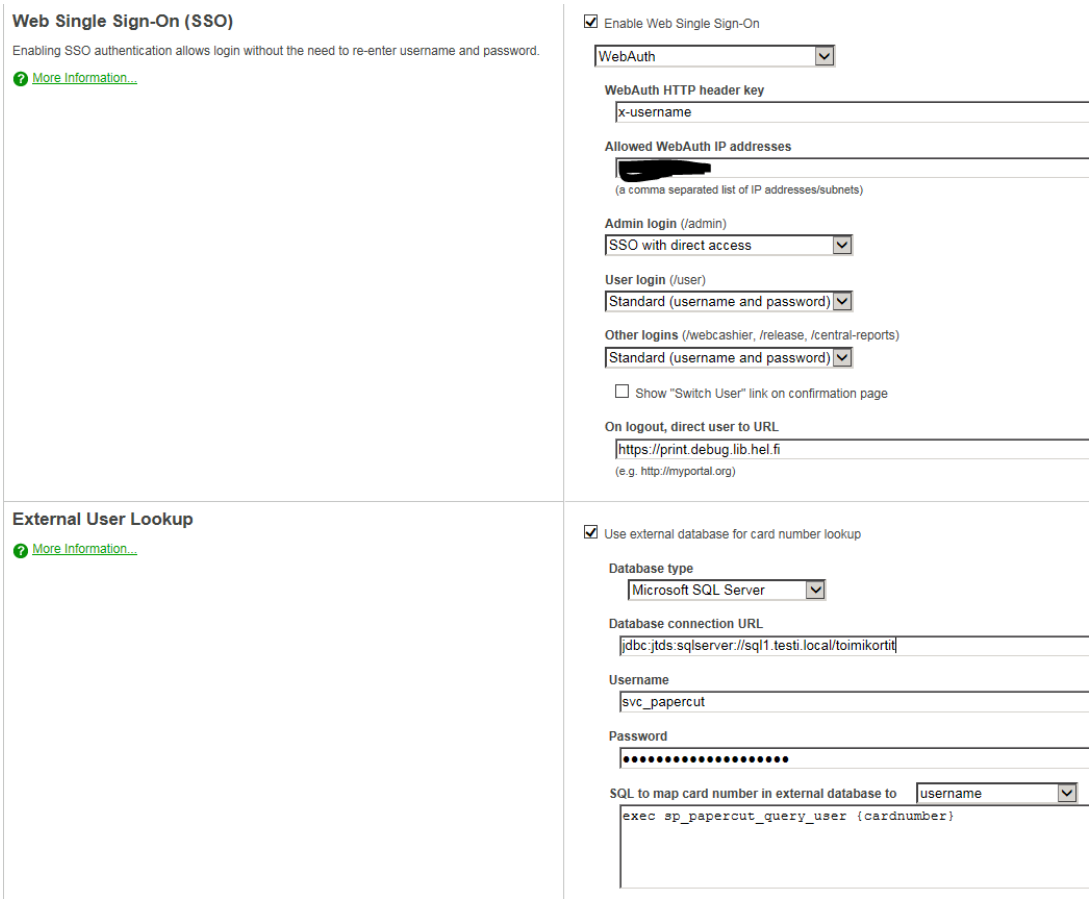


Kuva 41. Tunnusten luonti

Kuvan 9 mukaisesti määritettiin, että tulostajien käyttäjätiedot haetaan järjestelmään tarpeen mukaan eli käytetään järjestelmän ”Create Users on -demand”. Tämän lisäksi käyttäjien on mahdollista rekisteröidä itselleen käyttäjätunnus, jonka avulla he voivat hyödyntää mobiilitulostusta vaikka heillä ei olisi kirjaston työasemajärjestelmän asiakastunnusta.

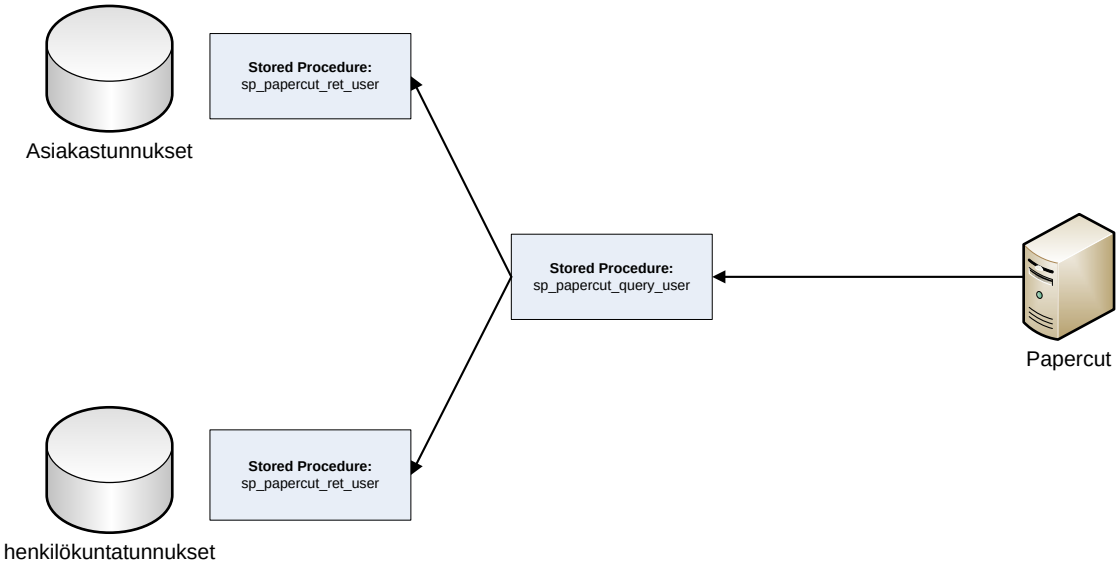
2.2 Toimikortin tarkastaminen ulkoisesta tietolähteestä

Monitoimilaitteille sekä tulostusasemille voidaan kirjautua kirjastokortin numerolla sekä tähän liitetyllä PIN-koodilla sekä vaihtoehtoisesti kirjastokortin numeroon liitetyllä sähköpostiosoite-aliaksella. Lisäksi henkilökunta voi kirjautua laitteille henkilöstökortilla joka on liitetty Windows-käyttäjätunnukseen. Kirjautumisen yhteydessä toimikortin tiedot sekä siihen liitetty käyttäjätunnus haetaan ulkoisesta tietokannasta, jolloin voidaan useita erillisiä tietolähteitä toimikortin tarkistukseen.



Kuva 42. toimikorttitietojen tarkistus erillisestä tietokannasta

Kuvassa 10 on esitetty, kuinka testijärjestelmä asetettiin tarkistamaan käyttäjien toimikorttitiedot erillisestä tietokannasta. Tietokantakysely lähettää parametrina toimikortin numeron ja saa palautusarvona korttia vastaavan käyttäjätunnuksen.



Kuva 43. toimikortin tietojen tarkistus

Kuvassa on esitetty toimikortin tietojen tarkistuksen toimintalogiikka. Papercut järjestelmä on yhteydessä SQL-tietokantaan, jonne se lähettää toimikortin tiedot SQL Stored Proseduurin parametrina. SQL palvelimen proseduuri poistaa vastaanottamastaan merkkijonosta välilyönnit, jonka jälkeen se etsii kortin tietoja proseduurissa määritetyistä erillisistä toimikorttitietolähteistä. kortin tietojen löydyttyä proseduuri palauttaa Papercut-järjestelmälle toimikorttia vastaavan käyttäjätunnuksen nimen.

```
USE [papercut_helsinki1]
GO
/****** Object:  StoredProcedure [dbo].[sp_papercut_query_user]    Script Date: 11/04/2014 10:14:38 ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO

-- =============================================
-- Author:                      <Author,,Name>
-- Create date: <Create Date,,>
-- Description:     <Description,,>
-- =============================================
ALTER PROCEDURE [dbo].[sp_papercut_query_user]
                -- Add the parameters for the stored procedure here
                @cardid varchar(50) = NULL

AS
BEGIN
                -- SET NOCOUNT ON added to prevent extra result sets from
                -- interfering with SELECT statements.
                SET NOCOUNT ON;
                declare @cardidclean varchar(50)
                set @cardidclean = REPLACE(@cardid,' ','')
                declare             @user varchar(50)


                declare @staffuser varchar(50)
                declare @librarycard varchar(50)
                set @librarycard = ''
                set @helsinki1user = ''

   -- Insert statements for procedure here
   -- etsitään korttia vastaava käyttäjänimi ajanvaraus- ja toimikorttitietokannoista, tallennetaan tulokset muuttujiin @librarycard ja @helsink1iuser
                exec [Ajanvaraus].dbo.sp_papercut_ret_user @cardidclean,@librarycard output
                exec [papercut_helsinki1].dbo.sp_papercut_ret_user @cardidclean, @staffuser output

                --jos löydetään korttia vastaava tunnus ajanvarausjärjestelmästä palautetaan se, muussa tapauksessa palautetaan tieto henkilökunnan toimikorttitietokannasta
                if (@librarycard != '' or @librarycard IS NOT NULL) begin
                                set @user = @librarycard
                end
                else begin
                                set @user = @staffuser
                end
                select @user
```

```
END
```

Kuva 44. sp_papercut_query_user - proseduuri

Kuvassa 12 on esitetty ”sp_papercut_query_user”-proseduuri. Proseduuri sp_papercut_query_user tarkistaa syötteenä saamansa kortin tiedot sekä ajanvarausjärjestelmän tietokannasta, että henkilökunnan toimikorttitietokannasta. Tarkistus tehdään kutsumalla kumpaankin tietokantaan tallennettua Stored Proseduuria sp_papercut_ret_user. Toimikorttitietokannan proseduurin sp_papercut_ret_user koodi on kuvattu alla. Ajanvarausjärjestelmään tallennettu sp_papercut_ret_user on muilta osin vastaava, mutta tietojen valintalauseke on vaihdettu vastaamaan kyselyn lähteenä olevan taulun rakennetta.

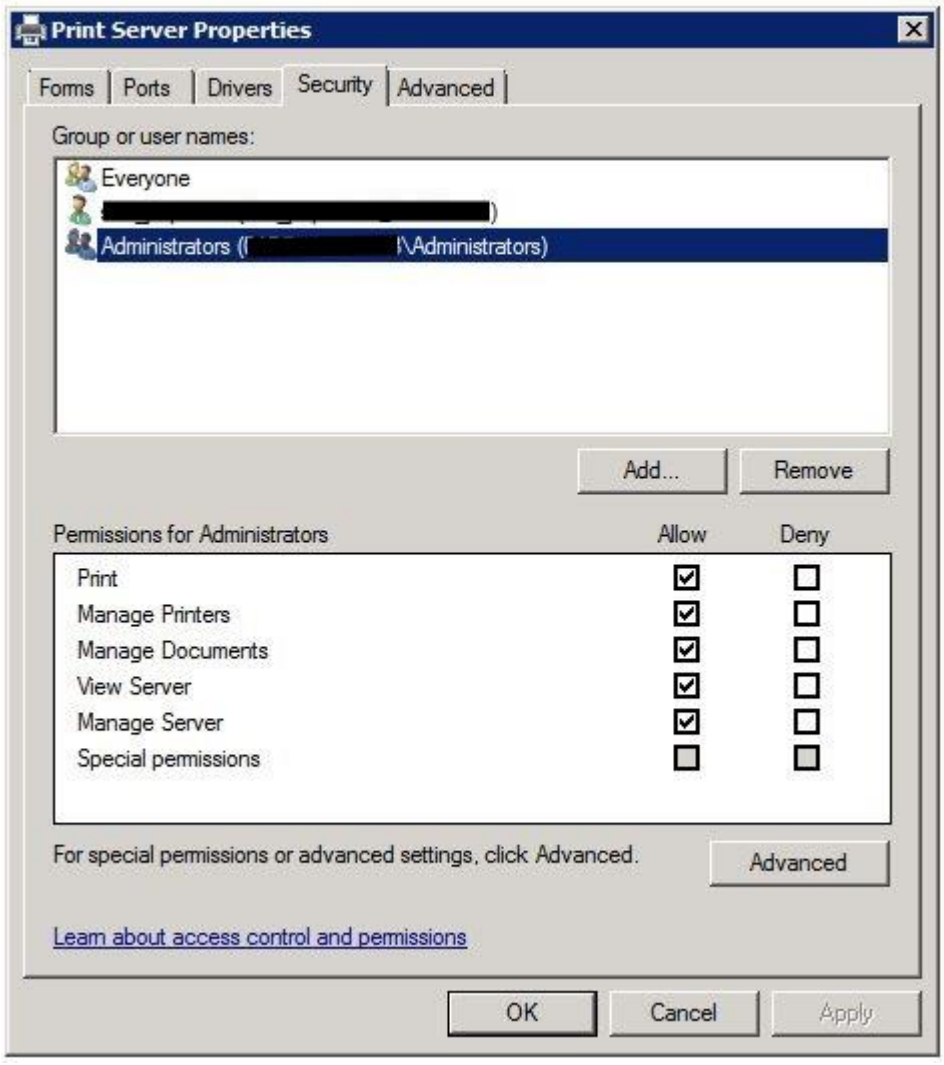
```
USE [papercut_helsinki1]
GO
/****** Object:  StoredProcedure [dbo].[sp_papercut_ret_user]    Script Date: 11/04/2014 10:30:01 ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO


-- =============================================
-- Author:                              <Author,,Name>
-- Create date: <Create Date,,>
-- Description:      <Description,,>
-- =============================================
ALTER PROCEDURE [dbo].[sp_papercut_ret_user]
                    -- Add the parameters for the stored procedure here
                    @cardid varchar(100) = NULL,
                    @username varchar(50) output

AS
BEGIN
                    -- SET NOCOUNT ON added to prevent extra result sets from
                    -- interfering with SELECT statements.
                    SET NOCOUNT ON;
                    declare @cardidclean varchar(100)
                    set @cardidclean = REPLACE(@cardid,' ','')


   -- Insert statements for procedure here
                    set @username = (SELECT top(1) LOWER(username) as "username" from CombinedUsers where
kortti1 = @cardidclean)
END
```

Kuva 45. sp_papercut_ret_user - proseduuri

Kuvassa 13 on proseduurin sp_papercut_ret_user koodi, jolla haetaan toimikortin tietoja ja palautetaan kutsuvalle proseduurille käyttäjänimi tai NULL.

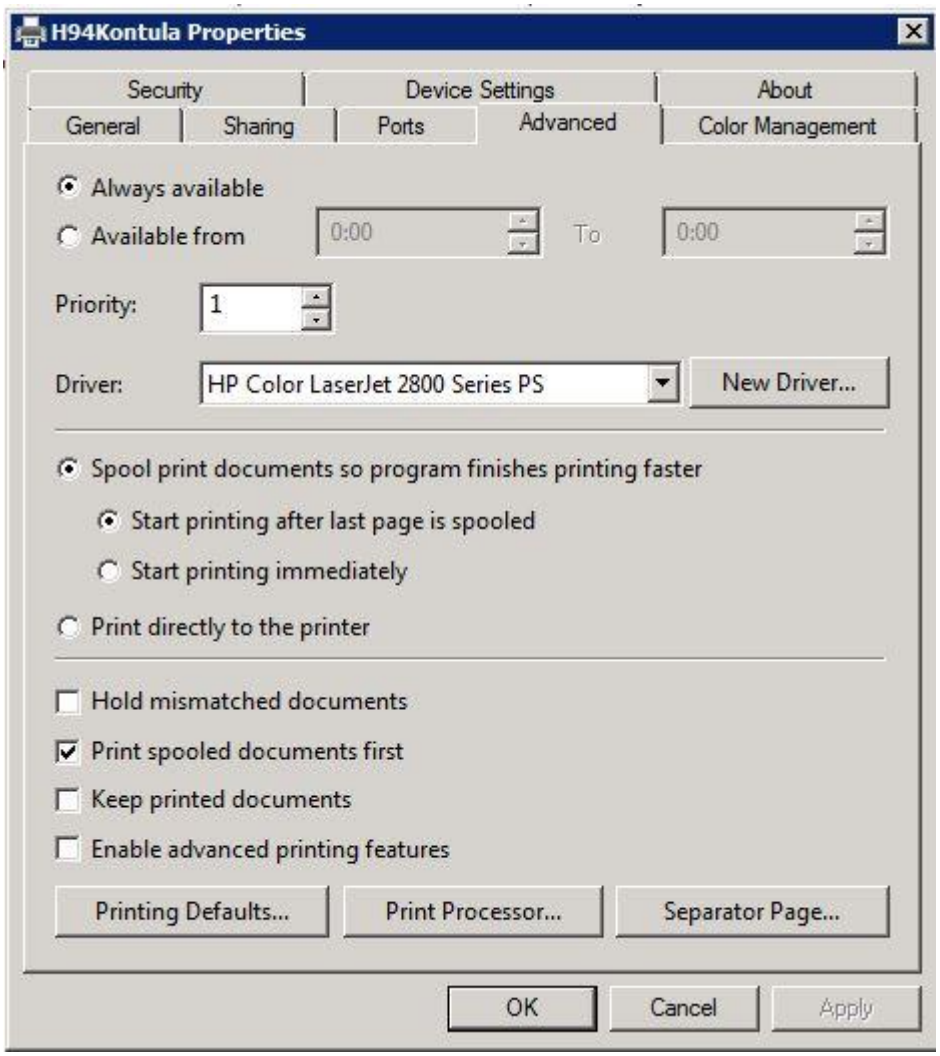
2.3 Tulostusjonot

Tulostuspalvelimelle määritettiin kullekin testikirjastolle oma virtuaalitulostin, johon asiakkaiden tulostustyöt saapuvat. Jonojen nimet ovat H10Kymppi, H53Kallio sekä H94Kontula. Tulostuspalvelimen asetuksia muokattiin kuvan XX osoittamalla tavalla siten, että tulostiemien käyttöoikeusmäärityksistä poistettiin Creator Owner-käyttäjätunnus valmistajan dokumentaation mukaisesti. Lisäksi käyttöoikeusmäärityksiin lisättiin Papercut-sovelluspalvelimen käyttämä palvelutunnus, jonka avulla sovellus hallinnoi tulosteita. Asettamalla käyttöoikeusmääreet koko palvelimen tasolle vältyttiin tarpeelta määrittää käyttöoikeudet erikseen jokaiseen tulostusjonoon.



Kuva 46. Tulostuspalvelimen käyttöoikeusmääritykset

Järjestelmän suorittaman tulostustöiden väri- ja sivu konversion vuoksi tulostimissa otettiin käyttöön RAW-tulostusformaatti kuvan 14 esittämällä tavalla poistamalla valinta ”Enable advanced printing features”



Kuva 47. RAW-formaatin määritys

Käyttäjille esitettävät viestit sekä tulostustöiden konversio määritettiin käyttämällä Papercutin tarjoamaa Advanced Print Scripting - ominaisuutta. Scripteillä voidaan laajasti vaikuttaa tulostustyön käsittelyyn sekä esittää käyttäjälle valinta ja ilmoitusikkunoita. Toiminnot suorittava koodi on esitetty seuraavana.

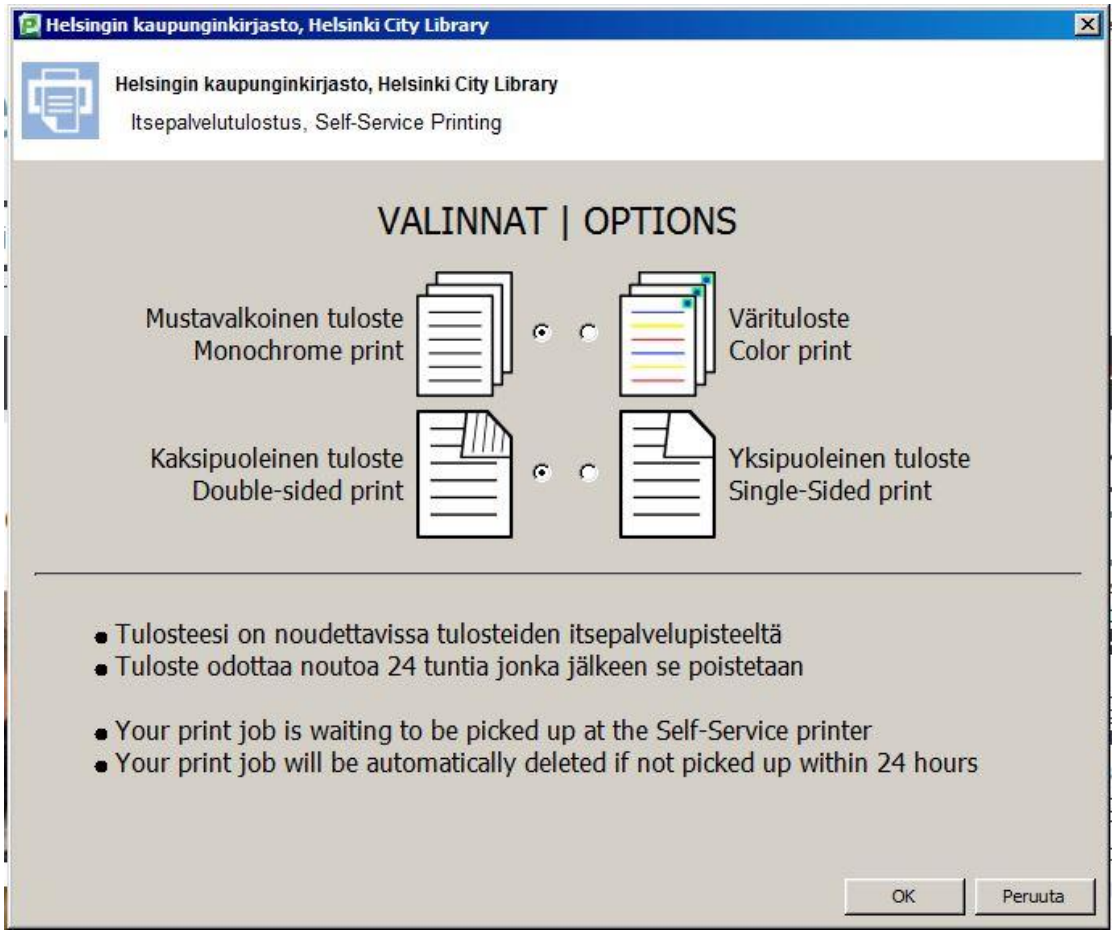
```
function printJobHook(inputs, actions) {

var LIMIT = 5;  // Show message for jobs over 500 pages.

if (!inputs.job.isAnalysisComplete) {
// No job details yet so return.
return;
}

if (inputs.job.totalPages > LIMIT) {
// Add your action code here
var RETVAL = actions.client.promptPrintCancel("Tulosteesi sisältää yli " + LIMIT +" sivua. Haluatko jatkaa?\r\nYour print job contains more than "+ LIMIT +" Pages. Do you want to proceed?",{fastResponse:true});
}

if (RETVAL == "TIMEOUT") {
actions.log.info("Dialog TIMEOUT");
return;
}

if (RETVAL == "CANCEL") {
actions.job.cancelAndLog("user cancelled the job");
return;
}

var infotitle = "Helsingin kaupunginkirjasto, Helsinki City Library";
var infodesc = "Itsepalvelutulostus, Self-Service Printing";


var infomessage = "<html>"
+"<div id='main' style='width:500px;height:400;'>"
+"<div id='otsikko' style='text-align: center; align-items: center; margin-bottom:10px;'>"
+"<span style='font-size:18px;'>VALINNAT | OPTIONS</span>"
+"</div><div id='taulukko' style='text-align: center; align-items: center; margin-bottom:10px;'>"
+"<form>"
+"<table style='margin-left:auto;margin-right:auto;text-align:center; width=100%;'>"
+"<tr>"
+"<td style='text-align:right;'><span style='font-size:12px;'>Mustavalkoinen tuloste<br>Monochrome print</span></td>"
+"<td><img src='http://%PC_SERVER%/custom/icons/mv-sivu60px.png'></td>"
+"<td><input type='radio' name='COLORSELECT' value='1' checked='checked'></input></td>"
+"<td><input type='radio' name='COLORSELECT' value='2'></input></td>"
+"<td><img src='http://%PC_SERVER%/custom/icons/vari-sivu60px.png'></td>"
+"<td style='text-align:left;'><span style='font-size:12px;'>Värituloste<br>Color print</span></td>"
+"</tr>"
+"<tr>"
```

```
+"<td style='text-align:right;'><span style='font-size:12px;'>Kaksipuoleinen tuloste<br>Double-sided print</span></td>"
+"<td><img src='http://%PC_SERVER%/custom/icons/2-sivu60px.png'></td>"
+"<td><input type='radio' name='DUPLEXSELECT' value='1' checked='checked'></input></td>"
+"<td><input type='radio' name='DUPLEXSELECT' value='2'></input></td>"
+"<td><img src='http://%PC_SERVER%/custom/icons/1-sivu60px.png'></td>"
+"<td style='text-align:left;'><span style='font-size:12px;'>Yksipuoleinen tuloste<br>Single-Sided print</span></td>"
+"</tr>"
+"</table></span>"
+"</form></div><hr>"
+"<div style='text-align:left; font-size:12px;margin-top:10px;'>"
+"<li>Tulosteesi on noudettavissa tulosteiden itsepalvelupisteeltä</li>"
+"<li>Tuloste odottaa noutoa 24 tuntia jonka jälkeen se poistetaan</li><br/>"
+"<li>Your print job is waiting to be picked up at the Self-Service printer</li>"
+"<li>Your print job will be automatically deleted if not picked up within 24 hours</li>"
+"</div></div>"
+"</html>";



// Send a message (not requiring any action) to the user that printed the job
var RETVAL = actions.client.promptForForm(infomessage,{"dialogDesc":infodesc,"dialogTitle":infotitle,"hideJobDetails":true,"timeoutSecs":45,fastResponse:true});

if (RETVAL == "TIMEOUT") {
actions.log.info("Dialog TIMEOUT");
return;
}
if (RETVAL == 'CANCEL') {
actions.job.cancel();
}
actions.log.info(RETVAL['COLORSELECT']);
if (RETVAL['COLORSELECT'] == '1') {
actions.log.info("User selected grayscale printing");
actions.job.convertToGrayscale();
}
else {
actions.log.info("User selected color printing");
}

if (RETVAL['DUPLEXSELECT'] == '1') {
actions.log.info("user selected double-sided printing");
actions.job.convertToDuplex();
}
else {
```

```
actions.log.info("user selected single-sided printing");
}
}
```

Kuva 48. Koodi tulosteen konversioon sekä käyttäjän valintaikkunan luomiseksi

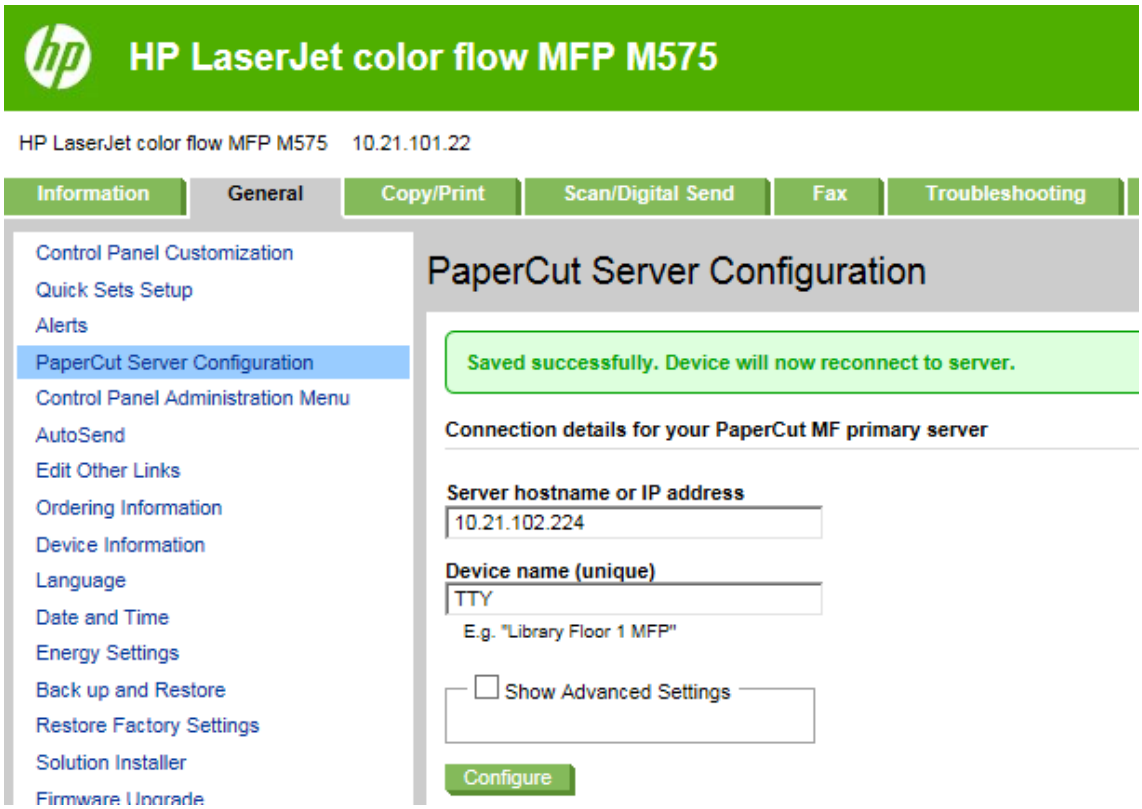
Kuvassa 16 on kaikissa virtuaalitulostimissa käytössä oleva koodi, jonka avulla käyttäjälle esitetään valintaikkuna, jossa hän voi valita halutaanko tuloste mustavalkoisena vai värillisenä sekä yksi vai kaksipuoleisena. Valintaikkuna on esitetty kuvassa 17



Kuva 49. Käyttäjän valintaikkuna

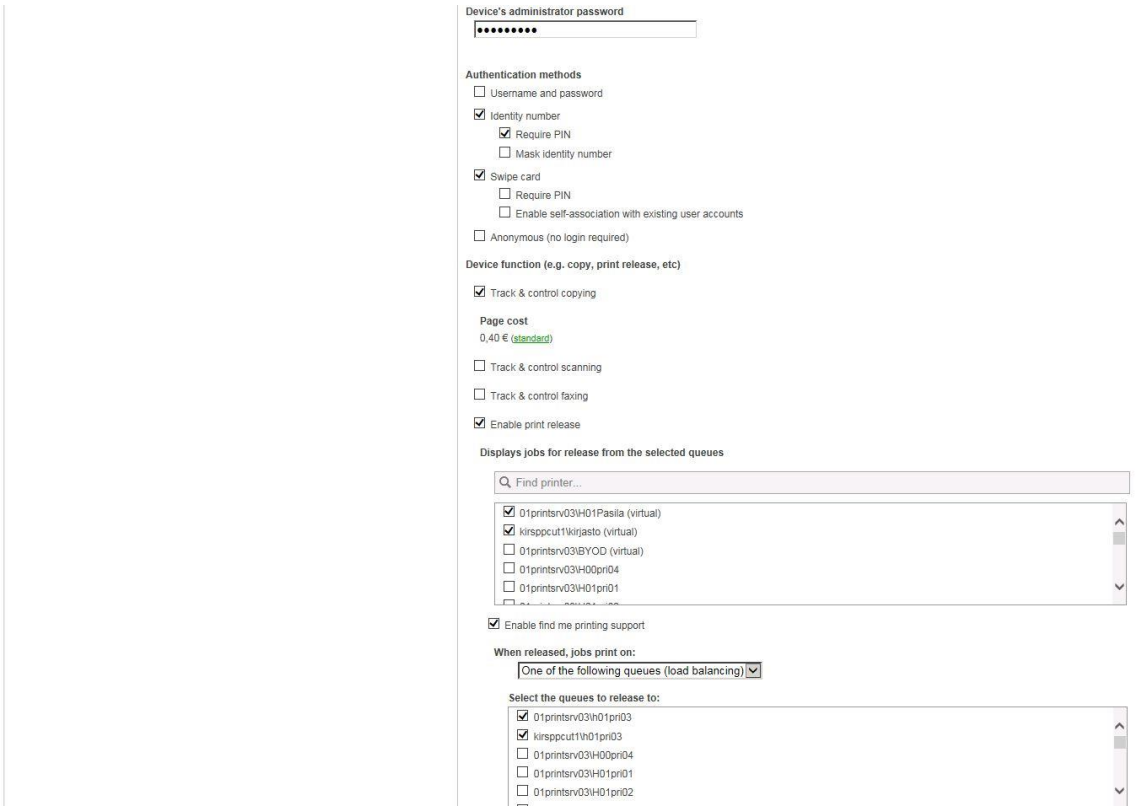
2.4 Monitoimilaitteet

Monitoimilaitteiden hyödyntäistä testattiin HP Laserjet Colot flow MFP M575-laitteella. Laitteeseen asennettiin Papercut-sovellus käyttämällä laitteen oman JetDirect web-palvelimen kautta. Tämän jälkeen laitteeseen tuli lisävalikko Papercut-järejstelmän asetuksia varten (Kuva 18). Asetuksiin lisättiin Papercut-palvelimen yhteystiedot sekä laitteen nimi joka näkyy Papercut-järjestelmän käyttöliittymässä.

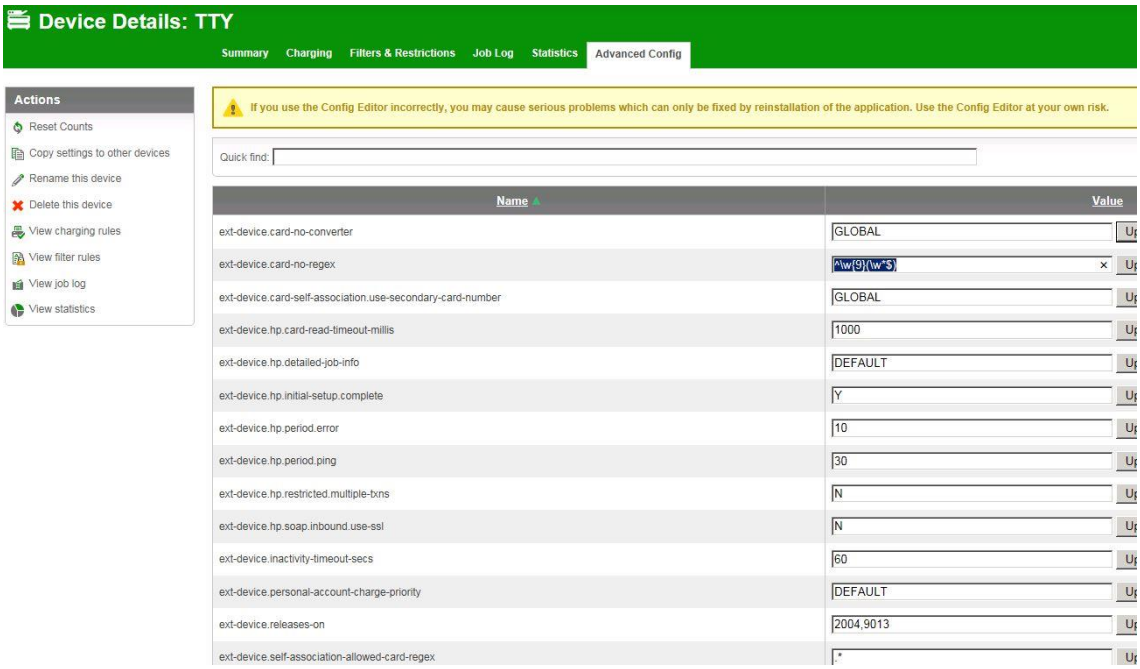


Kuva 50. Tulostusjärjestelmän yhteysasetukset HP monitoimilaitteella

Monitoimilaitteen asetusten jälkeen laitteen asetuksia muokattiin Papercut-järjestelmän käyttöliittymässä. Laitteen asetuksiin määritettiin ylläpitäjän käyttäjätunnus ja salasana. Käyttöön otettiin tulostuksen ja kopioinnin hallinta ja valvonta. Kirjautuminen mahdollistettiin lähiluettavalla toimikortilla (ei vaadittu pin-koodia) sekä syöttämällä toimikortin tieto manuaalisesti(pin vaadittiin).

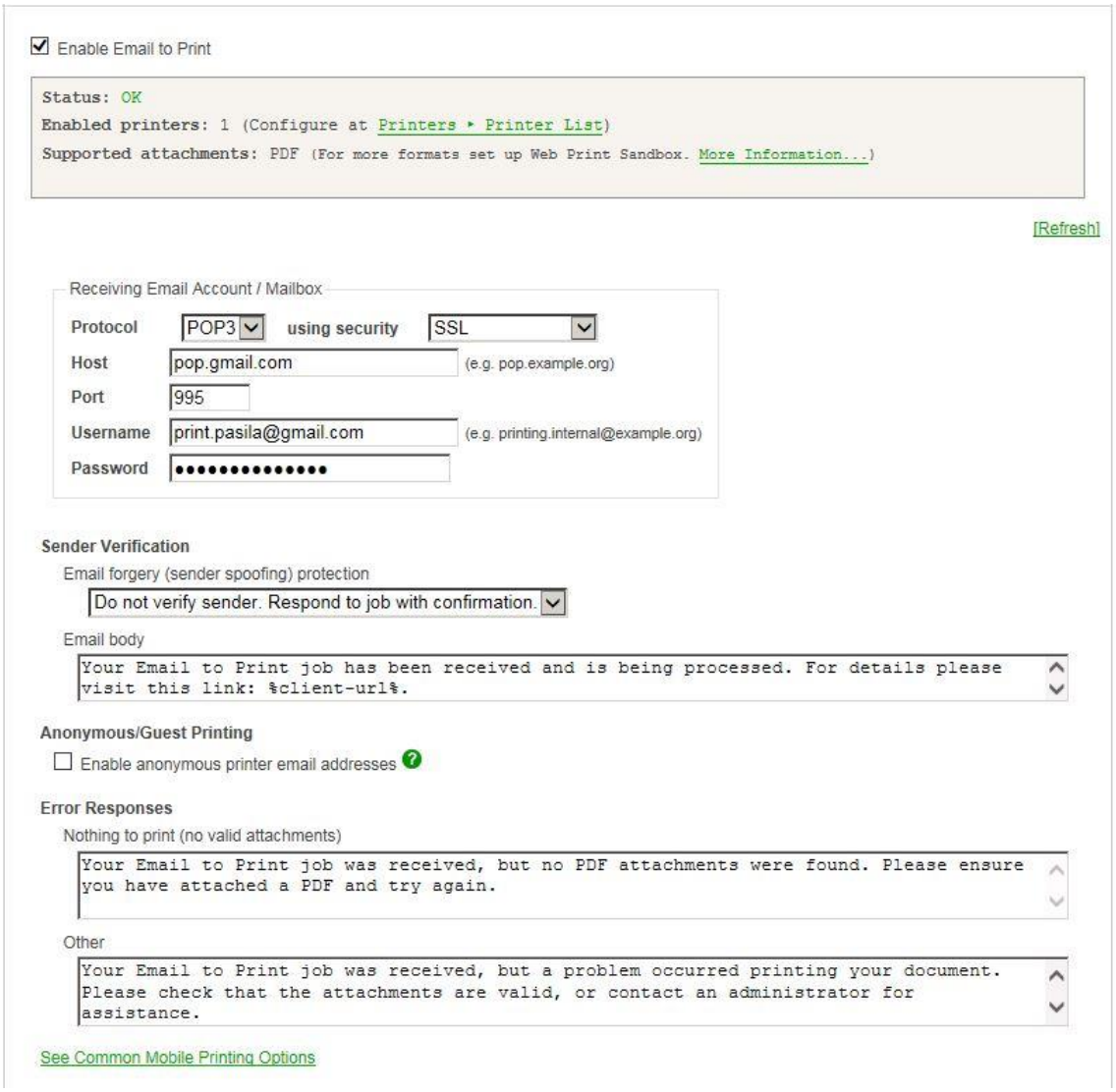


Kuva 51. Monitoimilaitteen yleiset asetukset



Kuva 52. Monitoimilaitteen lisäasetukset

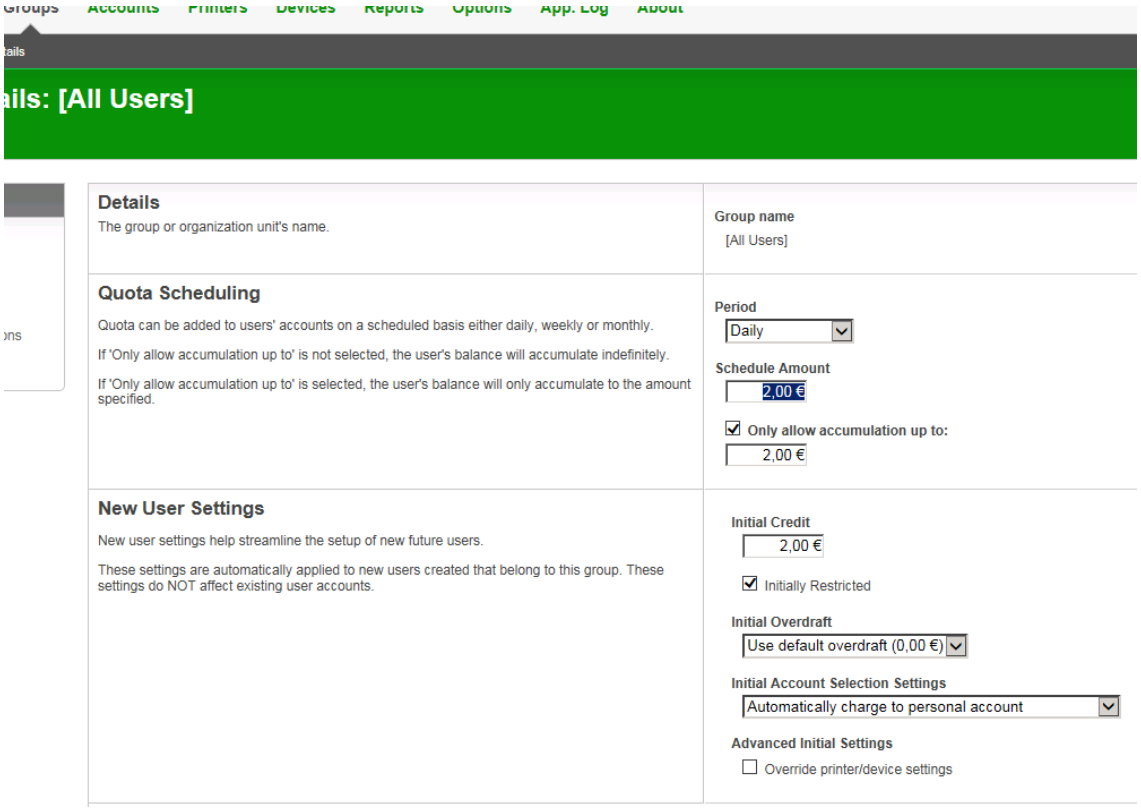
2.5 Sähköpostitulostus



Kuva 53. Sähköpostitulostuksen konfigurointi

Kuvassa 21 on esitetty sähköpostitulostuksen käyttöönotto. Ennne käyttöönottoa luotiin erillinen gmail-sähköpostitili. Järjestelmän versiossa 14.2 oli käytettävissä ainoastaan POP3-protokolla postilaatikon viestien tarkistukseen

2.6 Tulostuskiintiöt



Kuva 54. Peruskäyttäjän oletusasetukset

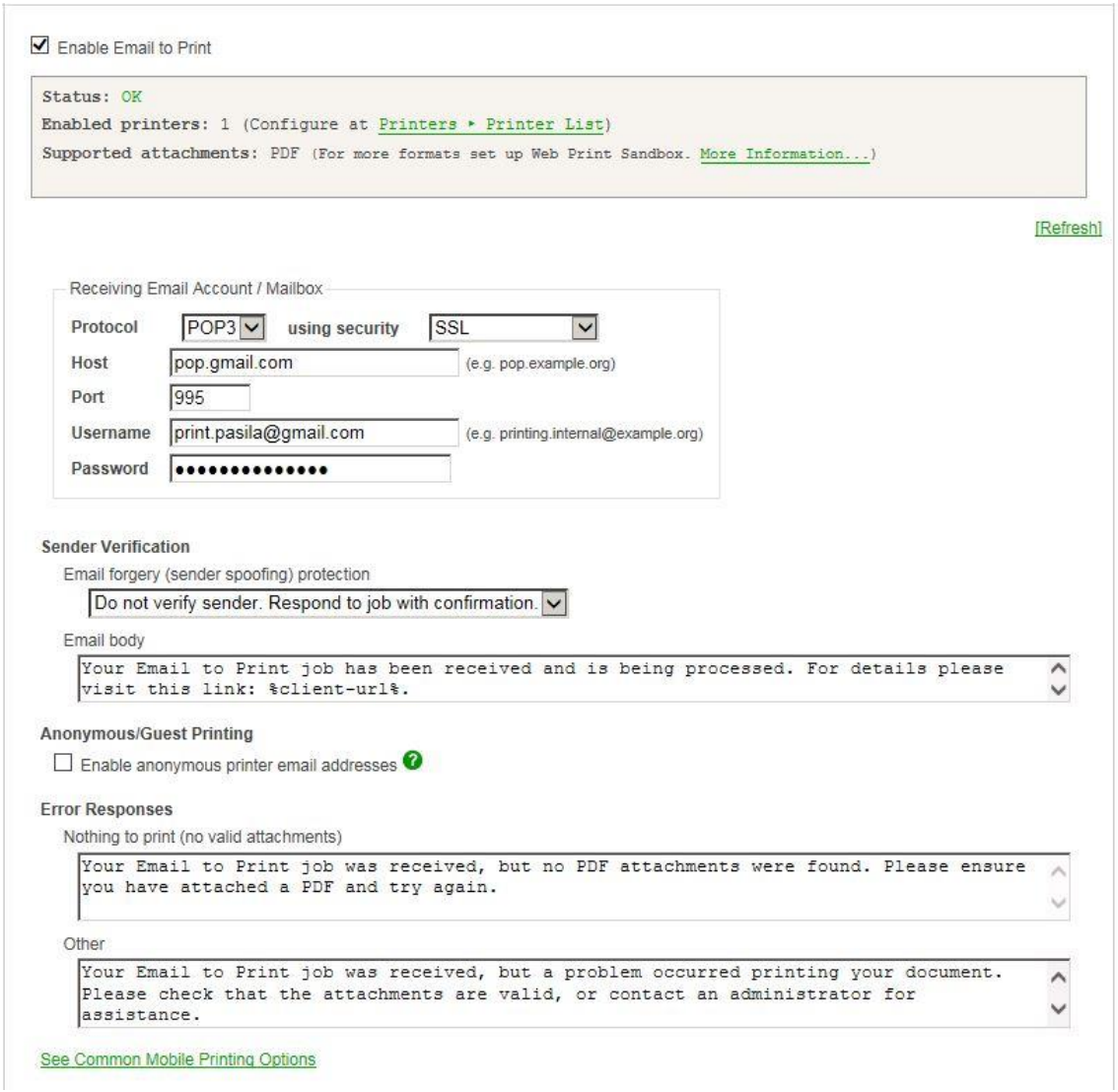
Kuvassa 22 on esitetty, kuinka Papercut-järjestelmään voidaan konfiguroida käyttäjille aloitussaldo, sekä kuinka saldoa voidaan muuttaa säännöllisesti ennalta määritetyn summan verran. Kuvasta voidaan lisäksi todeta, että testiympäristössä käyttäjän tulostussaldoon lisätään päivittäin 2€, mutta tämän lisäksi saldo ei voi kasvaa yli tämän summan (asetus ”only allow accumulation up to:”).

2.7 Mobiilitulostus

Mobiilitulostus koostuu kahdesta osasta: Web-käyttöliittymästä sekä sähköpostista. Web-käyttöliittymää käytetään rekisteröitymiseen järjestelmän käyttäjäksi, sekä omien tietojen tarkasteluun. Sähköpostia käytetään rekisteröinnin vahvistukseen sekä PDF-tiedostojen lähettämiseksi tulostusta varten.

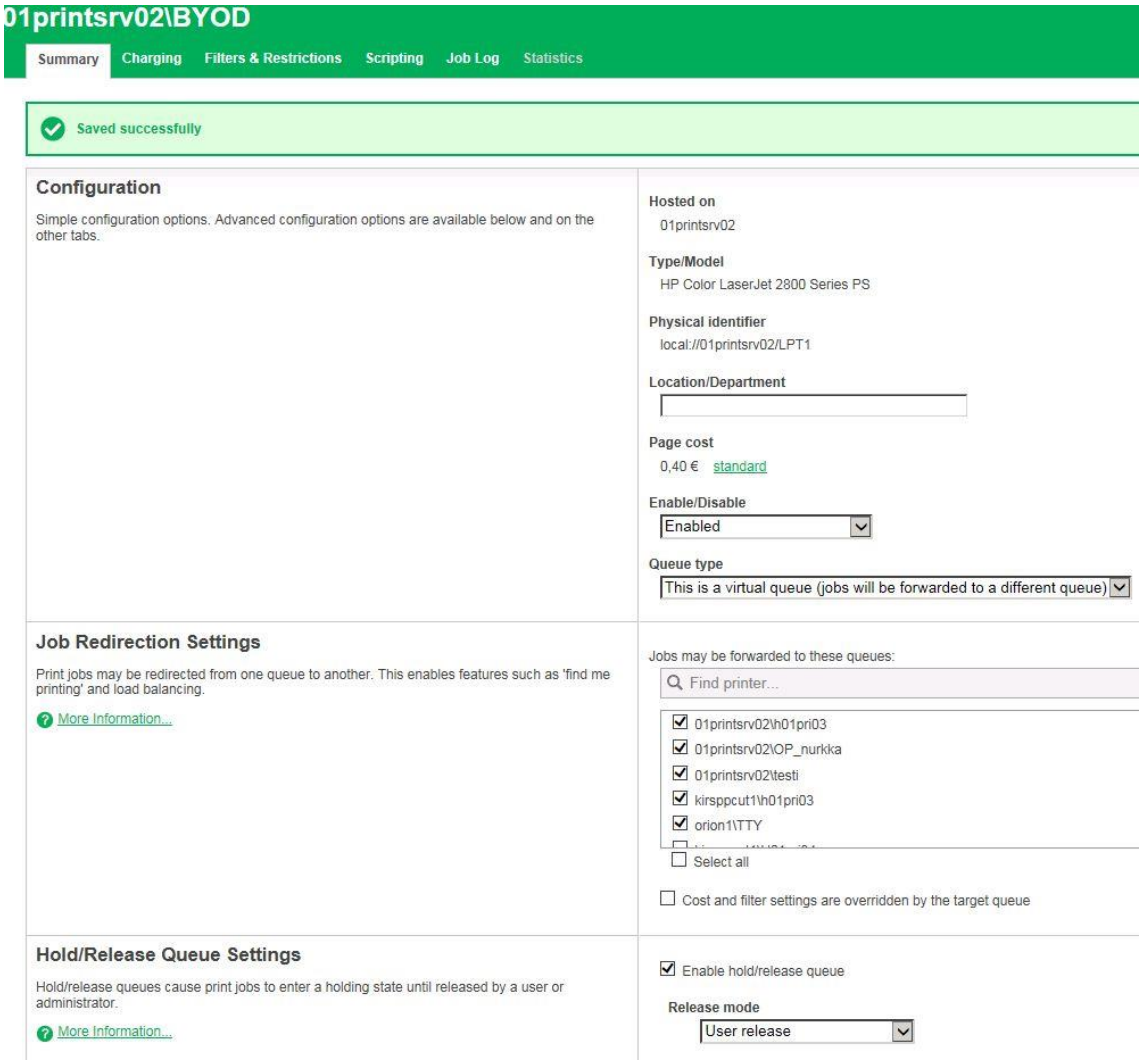
Mobiilitulostus toteutettiin sähköpostitulostuksena. Mobiilitulostuksen hyödyntäminen vaatii käyttäjän rekisteröitymisen. Tämä toteutettiin konfiguroimalla käyttäjille

mahdollisuus rekisteröityä järjestelmän käyttäjäksi itsepalveluna. Sähköpostitulostusta varten perustettiin erillinen gmail-sähköpostitili ”print.pasila@hel.fi”, jonne testikäyttäjät voivat lähettää pdf-liitetiedostoja tulostettavaksi.

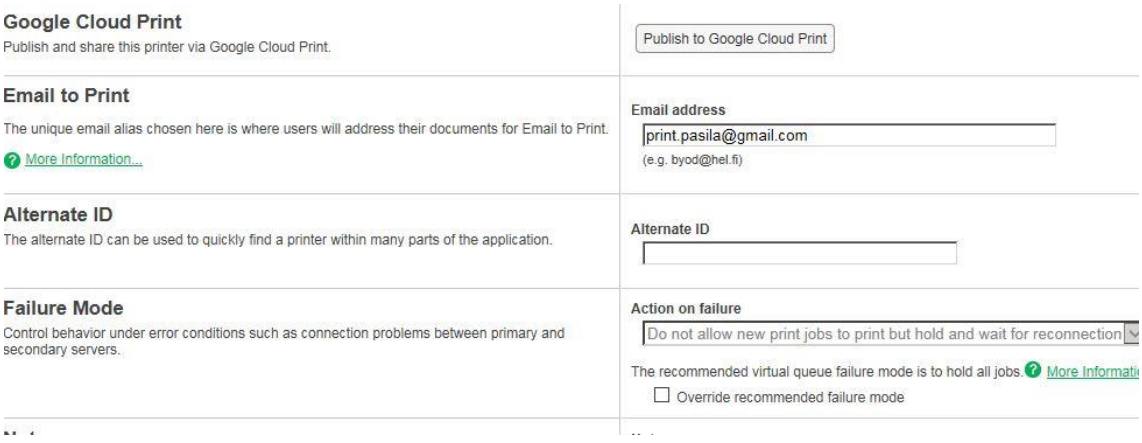


Kuva 55. Sähköpostitulostuksen käyttöönotto

Sähköpostitulostus otettiin käyttöön järjestelmän asetukset välilehdeltä Mobile & BYOD valikosta kuvan 23 mukaisesti.



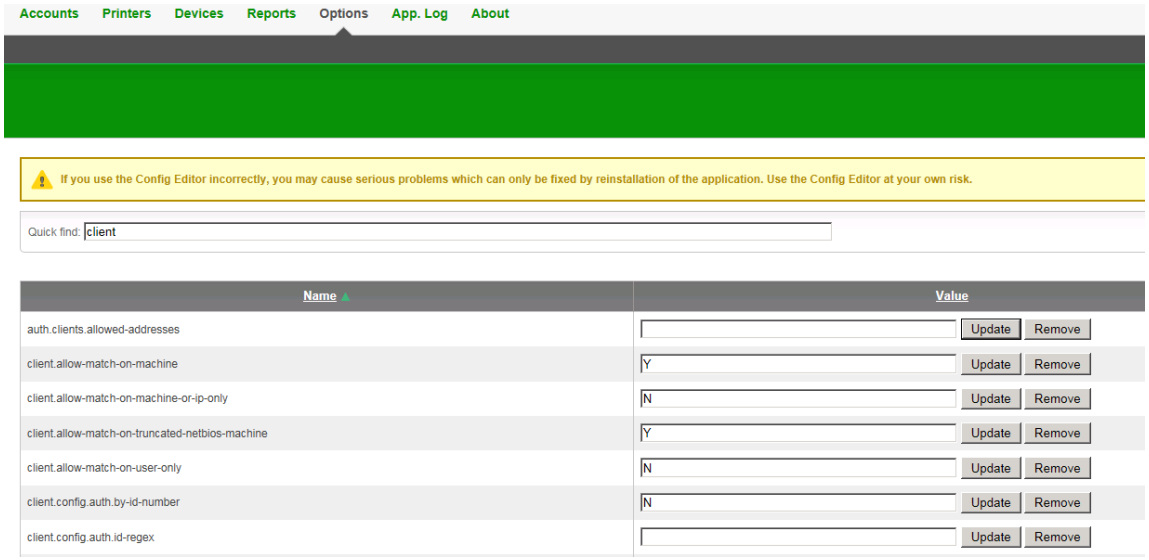
Kuva 56. Mobiilitulostuksessa käytetyn virtuaalitulostimen asetukset



Kuva 57. Sähköpostiosoitteen asetus virtuaalitulostimelle.

2.8 Muut asetukset

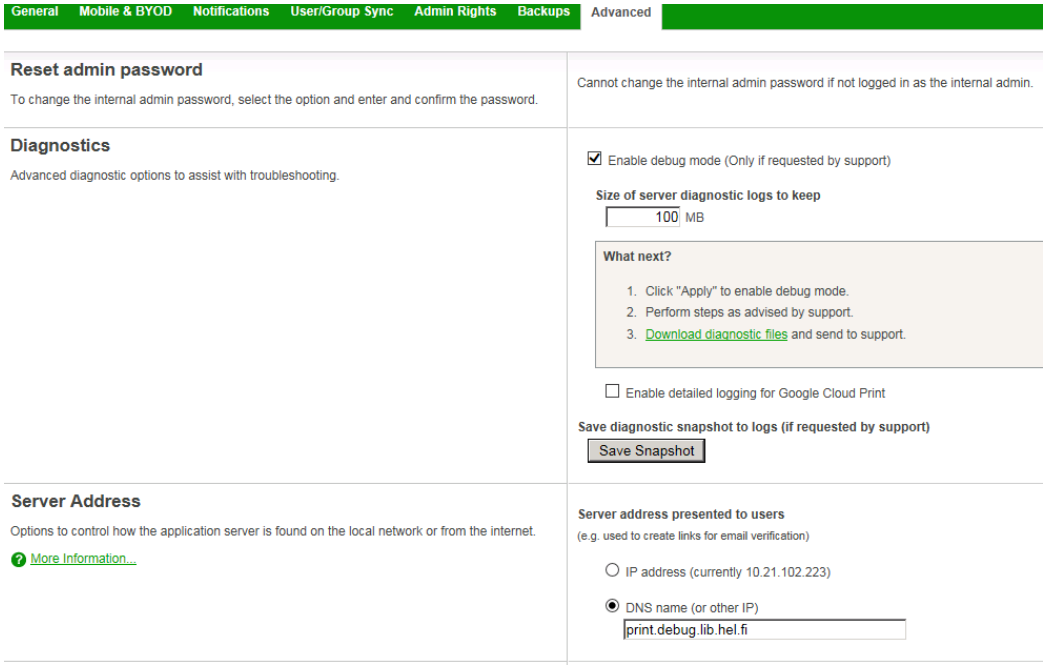
Tarvittavat asetukset Terminal Server käyttöä varten



Kuva 58. Citrix/Terminal server lisäasetukset

Järjestelmän lisäasetuksia muutettiin valmistajan dokumentaation mukaisesti, jotta käyttäjille esitettävät viestit toimivat oikein myös Citrix/Terminal Server ympäristössä. Asetus on esitetty kuvassa 26, josta voidaan havaita, että parametri client.allow.match-on-machine-or-ip-only on asetettu arvoon ”N”

DNS-isäntänimi

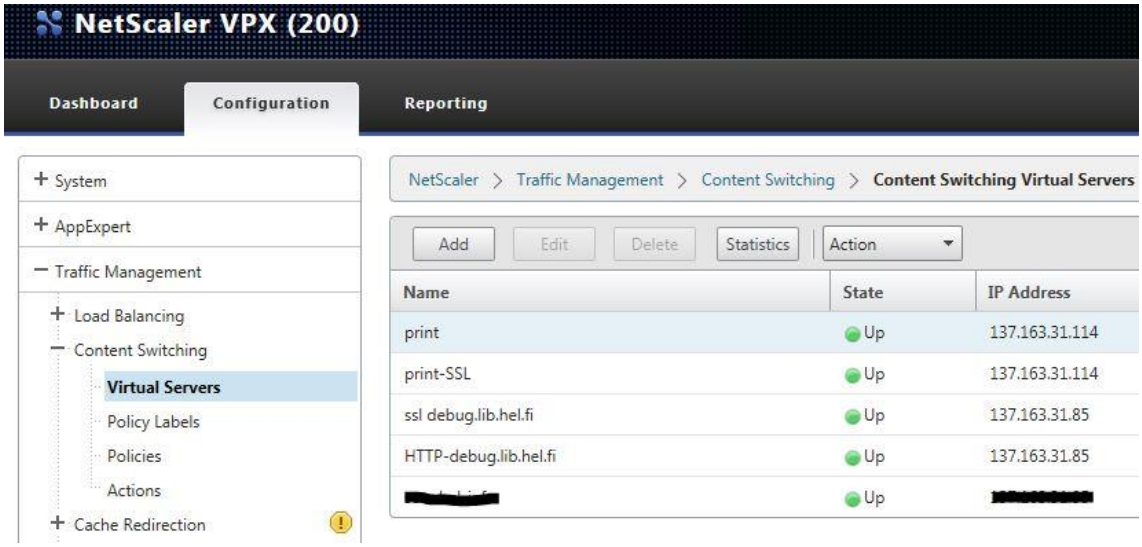


Kuva 59. Julkisen dns-nimen määritys palvelulle

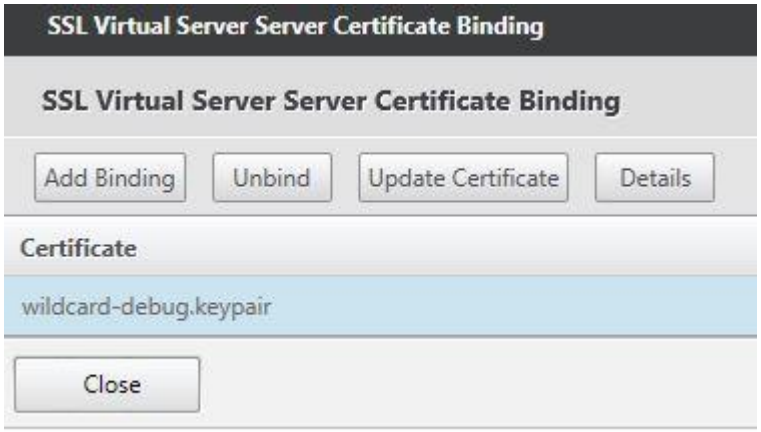
Koska järjestelmää voidaan mobiilitulostuksen osalta käyttää avoimesta internetistä, palvelimelle määritettiin julkinen dns-nimi, johon käyttäjät voivat muodostaa selainyhteyden. Tämän lisäksi järjestelmä käyttää kuvassa 27 esitettyä dns-isäntänimeä onnistuneen käyttäjärekisteröinnin vahvistusviestin sisällössä. Sähköpostiviestin sisältämä url-osoite koostuu dns-isäntänimen lisäksi palvelimen tcp-portista, joka on määritetty server.properties -tiedostossa.

3 Netscaler

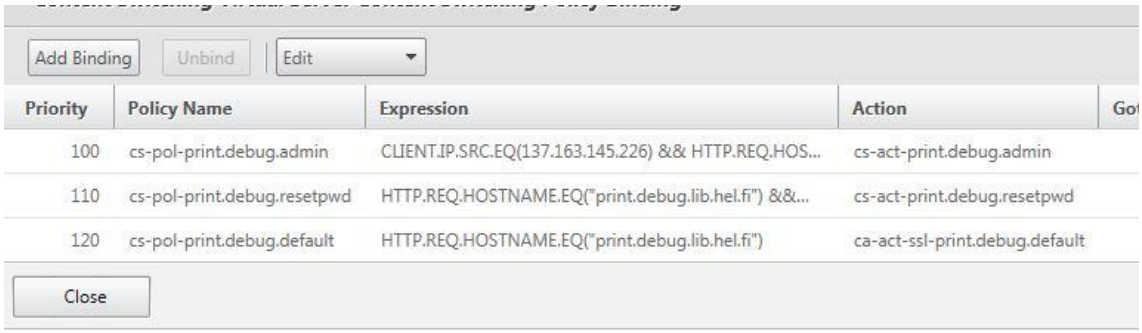
3.1 Content Switching Virtual Servers



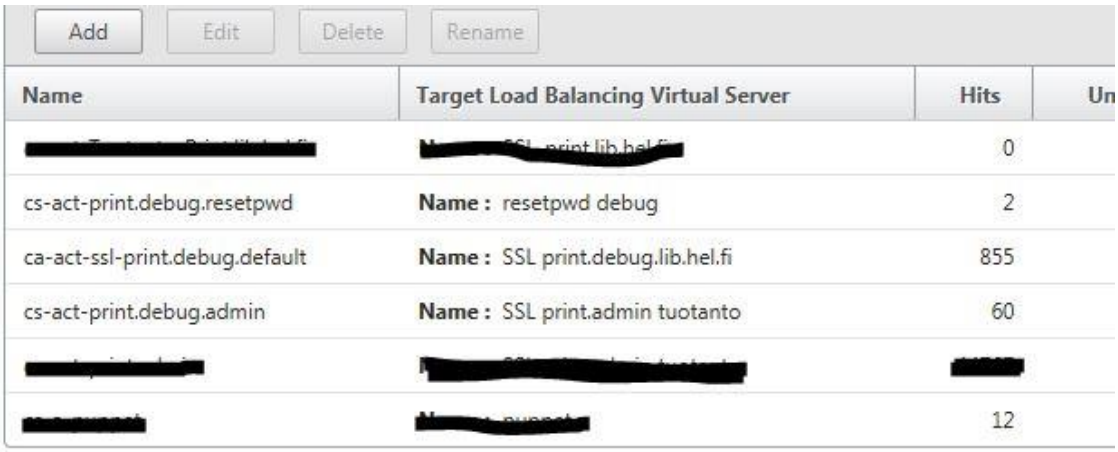
Kuva 60. Netscaler-palvelimelle luodut Content Switching -palvelimet



Kuva 61. SSL sertifikaatin määritys ssl.debug.lib.hel.fi -palvelimelle

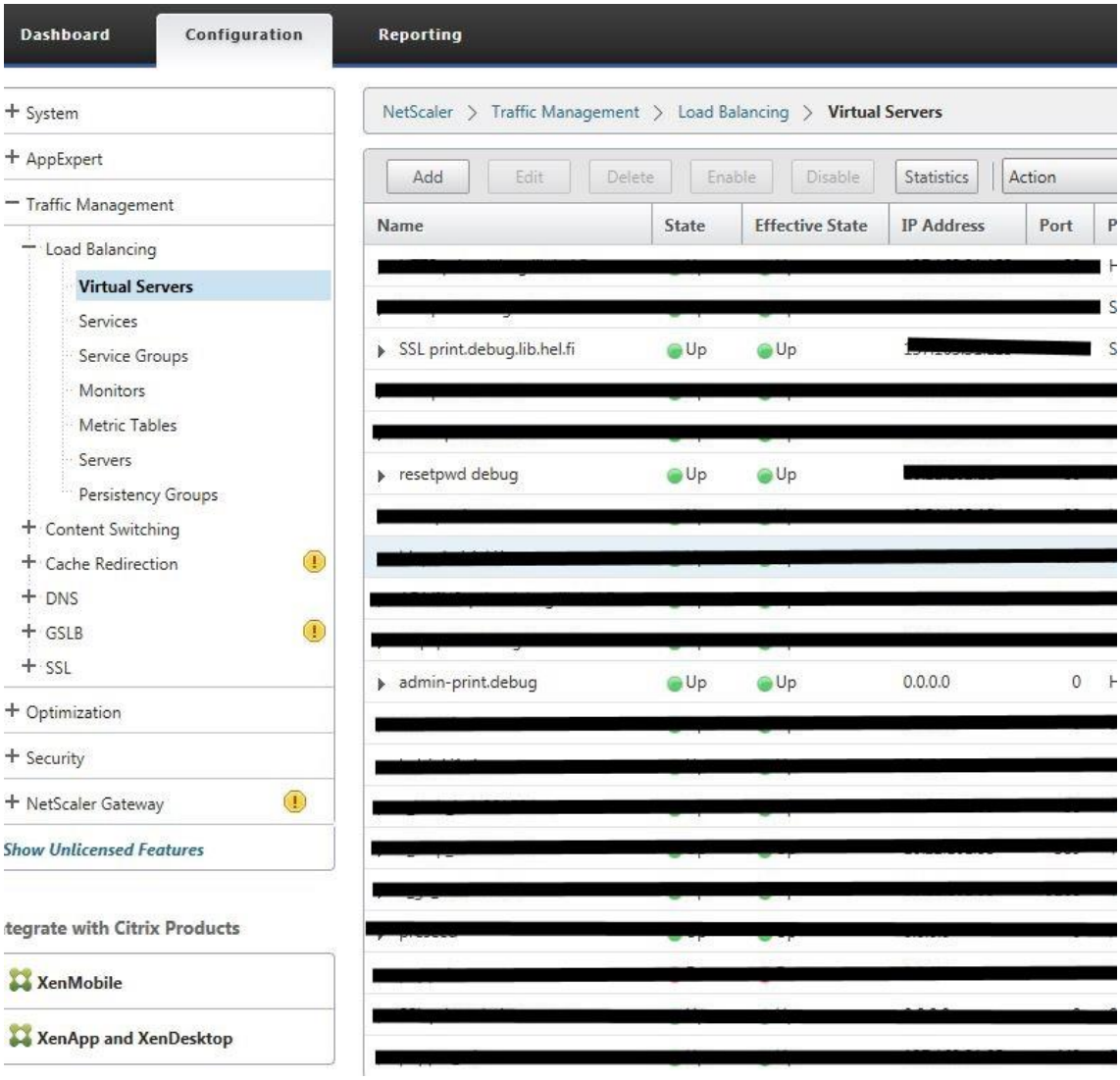


Kuva 62. Content Switching -palvelimen säännöstöt liikenteen ohjaukseen

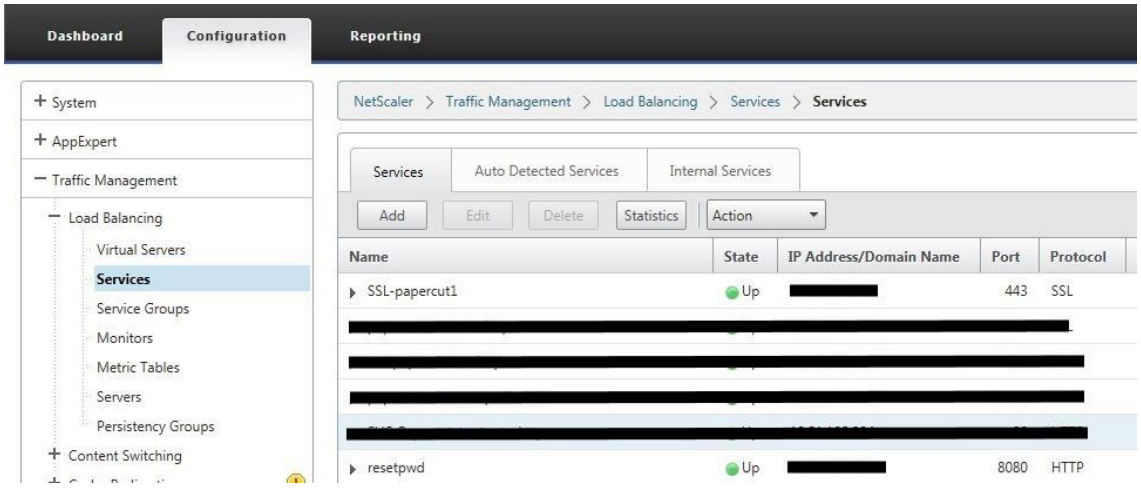


Kuva 63. Säännöstöjen suorittamat toiminteet (actions) sekä kohdepalvelimet

3.2 Load Balancing virtual servers

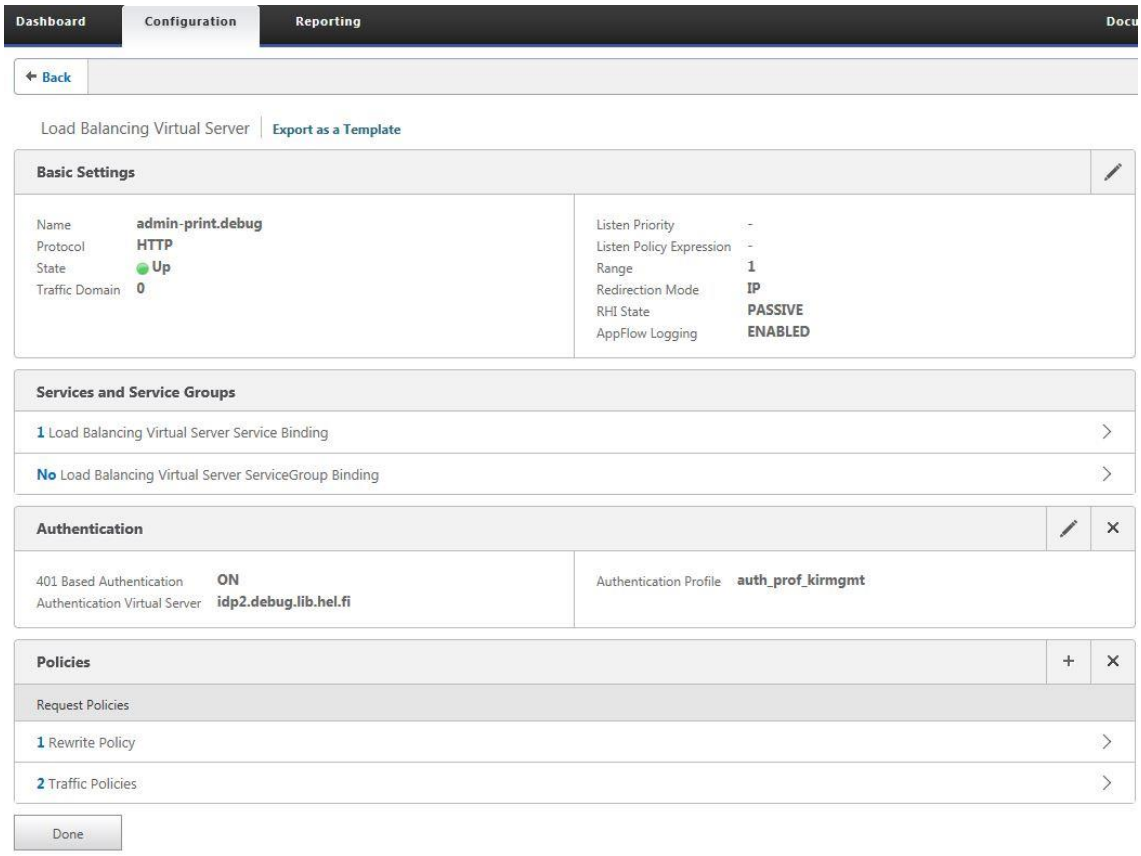


Kuva 64. LB palvelimet

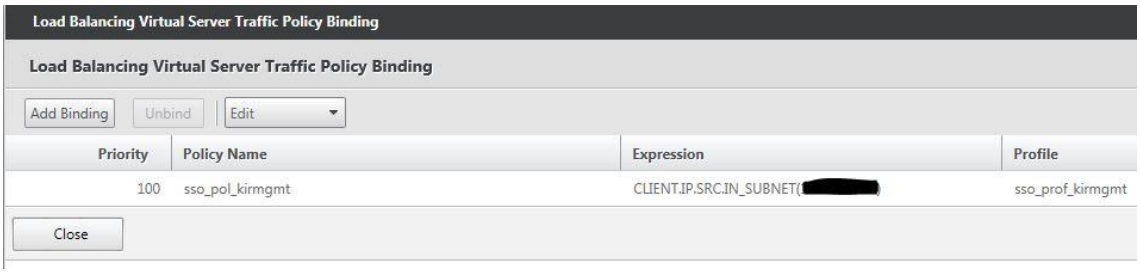


Kuva 65. Palveluiden asetukset

3.2.1 Autentikoinnin käyttöönotto

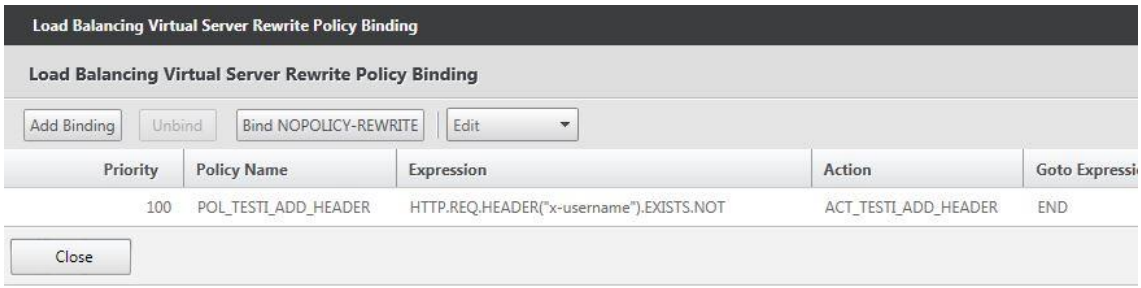


Kuva 66. Autentikoinnin käyttöönotto LB-palvelimella

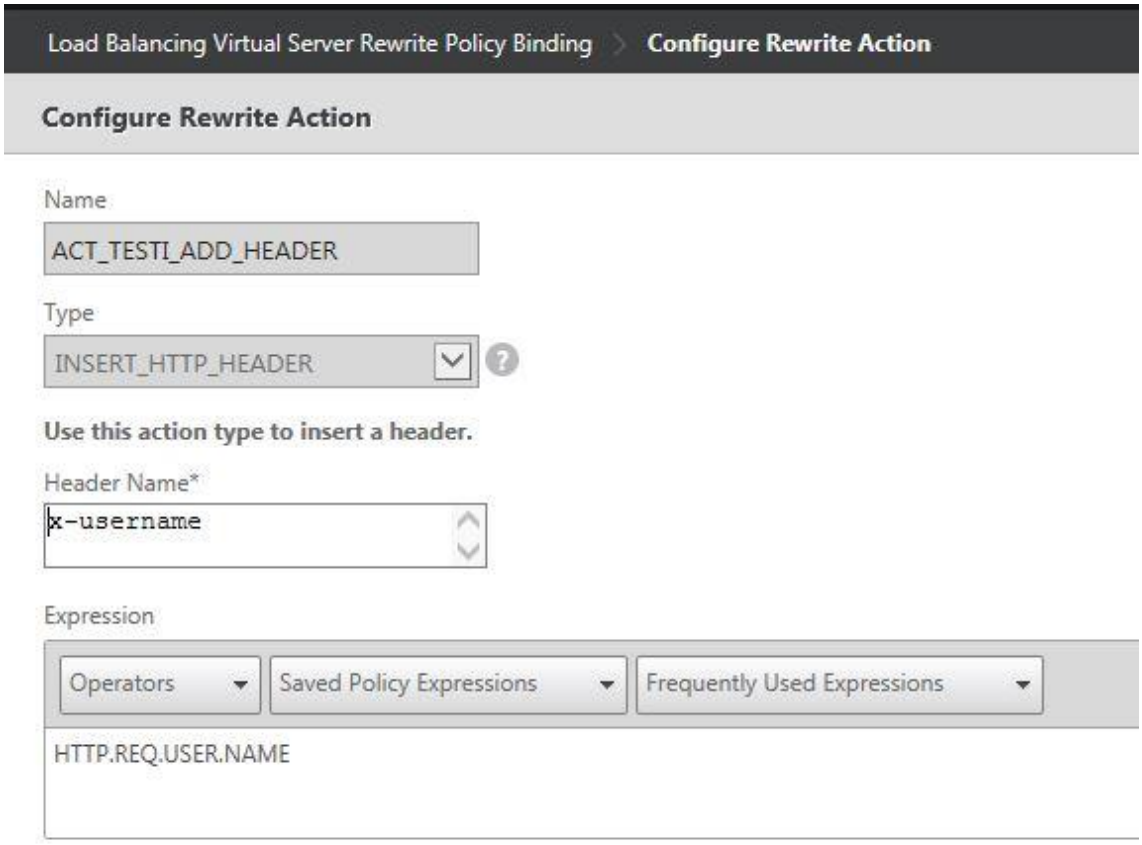


Kuva 67. traffic policy sekä siihen liitetty profiili

Kuva 68. Traffic profiilin asetukset suorakirjautumista varten

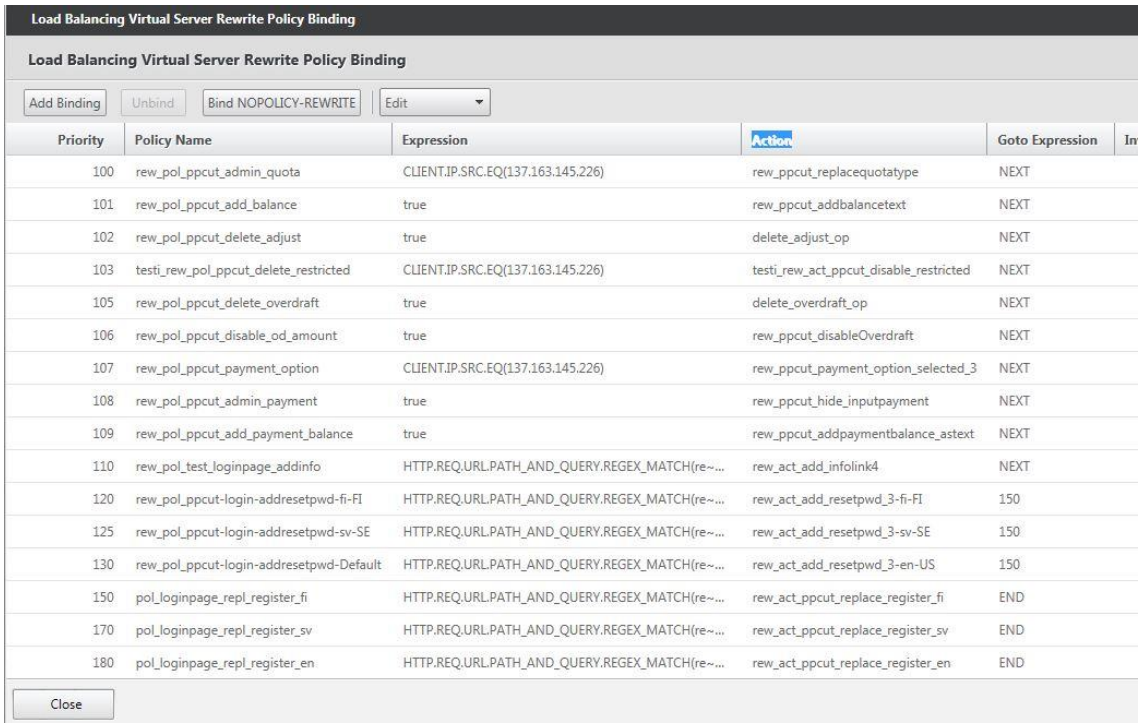


Kuva 69. sääntö otsikkotiedon lisäämiseksi

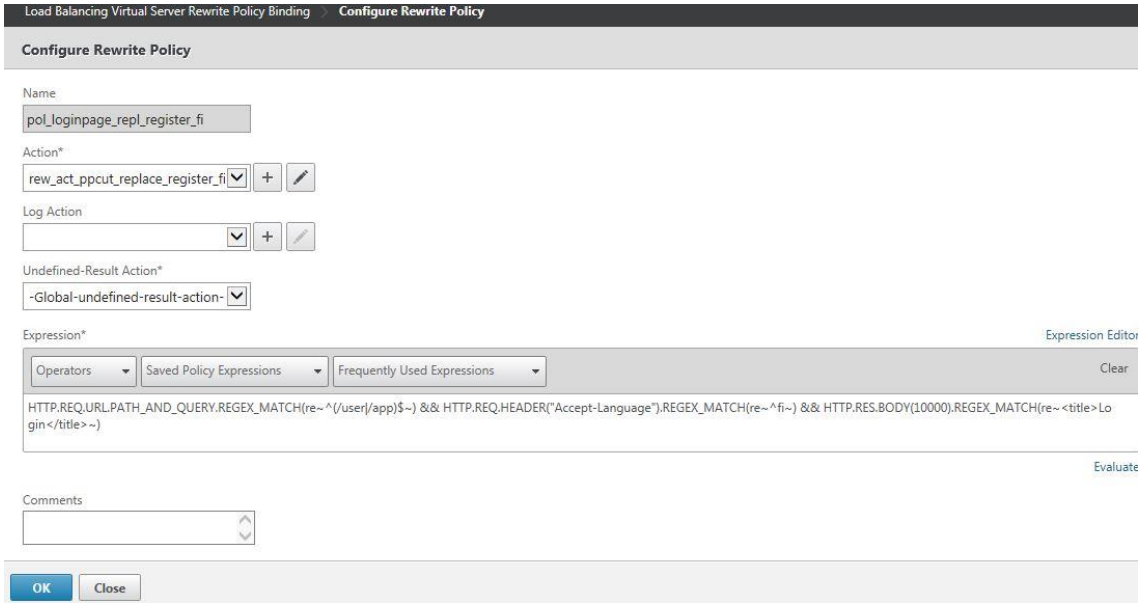


Kuva 70. Tunnistetun käyttäjän käyttäjätunnuksen lisäys http-otsikkoon

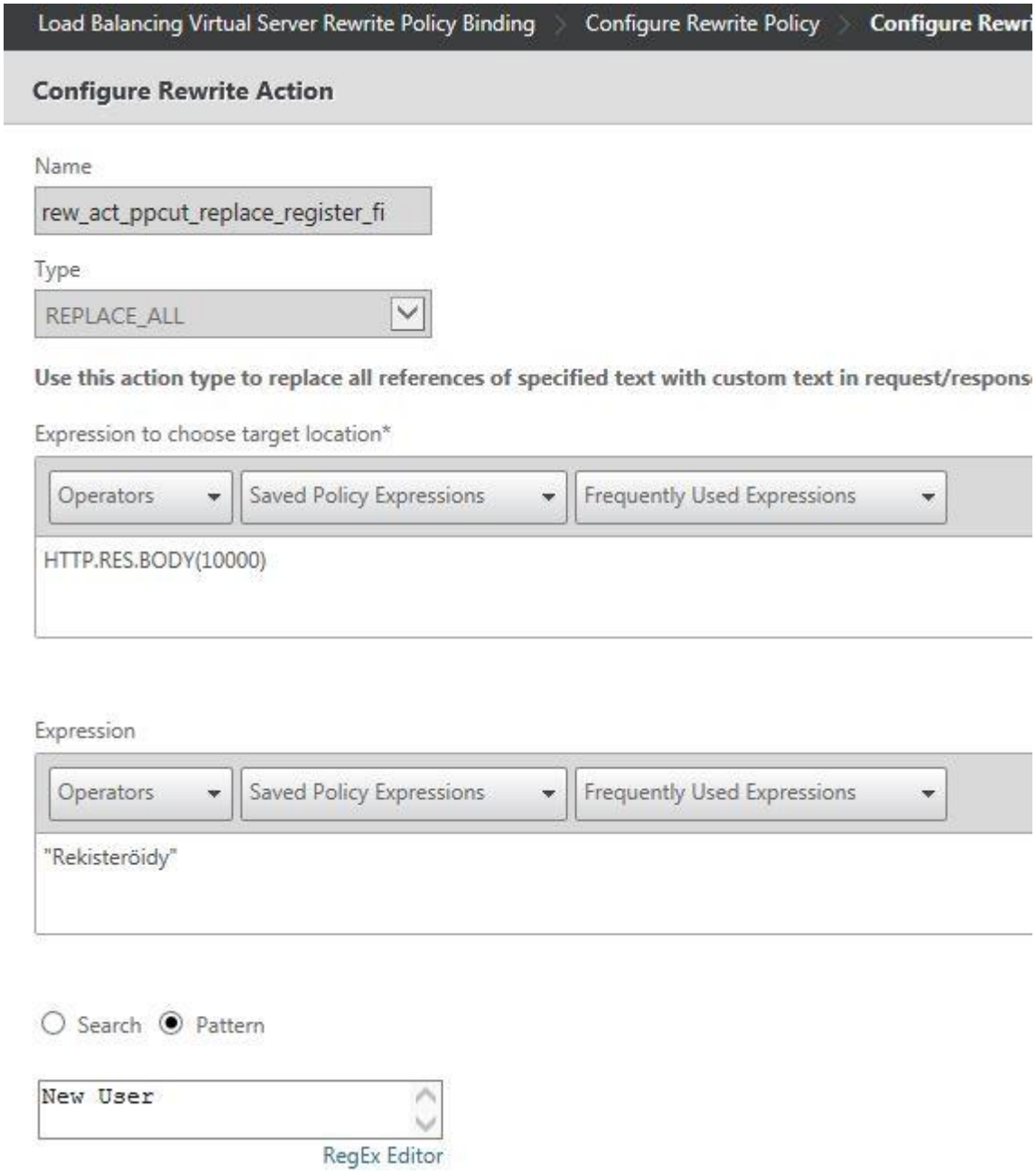
3.2.2 Sisällön muokkaaminen säännöstöillä



Kuva 71. sisältöön vaikuttavat säännöt



Kuva 72. Sääntö rekisteröitymispainikkeen kielivalinnan muuttamiseksi



Kuva 73. toiminto joka vaihtaa painikkeen tekstin

Kuvassa 41 on esitetty Content Rewrite -toiminto, jolla muutetaan http-sisällöstä ”New User” -merkkijono muotoon ”Rekisteröidy”.