Ilkka Sorsa

Salasananvaihtoratkaisun käyttöönotto pilvipalveluympäristössä

Tradenomi (AMK)

Tietojenkäsittelyn koulutus

Kevät 2018

KAJAANIN
AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Tiivistelmä

Tekijä: Sorsa Ilkka

Työn nimi: Salasananvaihtoratkaisun käyttöönotto pilvipalveluympäristössä

Tutkintonimike: Tradenomi (AMK), tietojenkäsittely

Asiasanat: virtualisointi, pilvipalvelut, salasanat, tietokannat, itsepalvelu, avoin lähdekoodi, verkkopalvelut, tietoverkot

Tämä opinnäytetyö toteutettiin toimeksiantona Oulun DataCenter Oy:lle. Opinnäytetyön tarkoituksena oli verrata itsepalveluna toimivia salasananvaihtoratkaisuja (engl. Self-Service Password Reset, SSPR) keskenään sekä löytää niistä sopivin vaihtoehto toimeksiantajan käyttöympäristöön.

Toimeksiantaja on oululainen IT-alan yritys, joka toimittaa asiakkailleen SaaS-pilvipalveluita. Kyseiset pilvipalveluratkaisut ovat toteutettu käyttämällä Citrix XenApp -virtualisointiohjelmistoa. Toimeksiantajalla on kaksi eri XenApp-versioilla toimivaa pilvipalveluympäristöä, joista uudemmassa ympäristössä ei ole vielä käytössä SSPR-ratkaisua. Tämän opinnäytetyön tarkoitus oli löytää sopiva SSPR-ratkaisu kyseiseen ympäristöön.

Opinnäytetyössä vertailtiin ensin potentiaalisia SSPR-ratkaisukandidaatteja SWOT-analyysin avulla. Kyseisten analyysien tulosten perusteella valittiin neljä ratkaisua, joista kaksi otettiin käyttöön onnistuneesti kokeiluympäristössä. Kokeiluympäristöksi opinnäytetyössä pystytettiin Citrix XenApp 7.15 LTSR -version päällä toimiva pilvipalveluympäristö, johon valitut SSPR-ratkaisut otettiin käyttöön. Lopulliset käyttöön otetut ratkaisut dokumentoitiin ja tulokset esiteltiin toimeksiantajalle.

Tämän opinnäytetyön tuloksena toimeksiantaja sai pilvipalveluympäristöönsä sopivan SSPR-ratkaisupohjan, jonka käyttöönottoa toimeksiantaja kehittää sisäisesti.

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Abstract

Author: Sorsa Ilkka

Title of the Publication: Deployment of a SSPR-solution in a Cloud Environment

Degree Title: Bachelor of Business Administration, Information Technology

Keywords: virtualisation, cloud services, password, databases, self-service, open source code, web services, information networks

This thesis was commissioned by Oulun DataCenter Oy. The purpose of this thesis was to compare different self-service password reset (SSPR) solutions and to find the most suitable solution for the employer's environment.

The employer is an IT-company located in Oulu. The employer offers a SaaS cloud service solution to its clients. The solution utilizes a virtualisation program suite called Citrix XenApp. The employer has two XenApp environments, the newer one of which does not have an existing SSPR-solution. The goal of this thesis was to find a suitable SSPR-solution for the environment.

In this thesis, potential SSPR solution candidates were first selected for comparison and subjected to a SWOT analysis. The results were compared to each other and based on the results of the comparison, four potential candidates were selected for deployment in a test environment. As a result of the tests, two candidates were successfully deployed and the deployment processes were thoroughly documented. The test cloud environment was built on Citrix XenApp, version 7.15 LTSR. The finished deployments were then demonstrated to the employer.

As a result of this thesis, the employer gained a framework for a suitable SSPR solution that makes it easy for the company to develop and self-implement a self-service password reset that is custom-made for their environment without any licence fees.

Alkusanat

Tämä opinnäytetyö on tehty toimeksiantona Oulun DataCenter Oy:lle. Haluan kiittää Oulun DataCenter Oy:n henkilökuntaa antoisasta ja opettavaisesta työharjoittelujaksosta sekä mahdollisuudesta jatkaa yhteistyötä opinnäytetyön merkeissä. Erityiskiitos Oulun DataCenter Oy:n järjestelmäasiantuntijalle Susanna Ylä-Himangalle työharjoittelujakson ohjaajana ja opinnäytetyön yhteyshenkilönä toimimisesta.

Haluan myös kiittää Kajaanin ammattikorkeakoulun opettajia yleisesti sekä opinnäytetyön ohjaavaa opettajaa Janne Koposta.

Oulussa 21.5.2018
Ilkka Sorsa

Sisällys

Symboliluettelo

Delivery Controller = Citrix XenApp-ympäristön ohjauspalvelin

Domain Controller (DC) = toimialueen ohjauspalvelin

Independent Computing Architecture (ICA) = Citrixin kehittämä, etäkäyttöön ja sovellusvirtualisoitintiin soveltuva protokolla

National Institute of Standards and Technology (NIST) = Yhdysvaltain kansallinen standardien ja teknologian instituutti

Remote Desktop Protocol (RDP) = Microsoftin kehittämä etätyöpöytäprotokolla

Self-Service Password Reset (SSPR) = itsepalveluna toteutettava salasananvaihto

Virtual Delivery Agent (VDA) = Virtuaalitoimitusagentti, virtuaalikone, jolla Citrix XenAppin tarjoamat virtualisoidut ohjelmat ajetaan

1 Johdanto

Lähtökohtana opinnäytetyössä oli tilanne, jossa Oulun DataCenter Oy:n tarjoama ODC Alusta -palvelu oli siirtymävaiheessa vanhan Citrix XenApp 6.5 -teknologialla toteutetun ympäristön ja uuden Citrix XenApp 7.15 LTSR -teknologialla toteutetun ympäristön välillä. Vanhassa ympäristössä oli käytössä kyseistä ympäristöä varta vasten kehitetty SSPR-ratkaisu, joka ei ollut yhteensopiva uuden ympäristön käyttämän Citrix NetScaler -tuotteen kanssa. Opinnäytetyön tavoitteena oli löytää uuteen XenApp 7.15 LTSR -teknologialla toteutettuun ympäristöön sopiva SSPR-ratkaisu. SSPR-ratkaisun käyttöönotto oli toimeksiantajalle tärkeää siitä syystä, että lähtötilanteessa toimeksiantajan ODC Alusta -palvelun asiakkaat joutuivat ottamaan yhteyttä toimeksiantajan tukipalveluun, kuormittaen tuesta vastaavia työntekijöitä.

Työssä valittiin aluksi kahdeksan eri SSPR-ratkaisukandidaattia. Kyseisiä ratkaisuja arvioitiin SWOT-analyysin kautta, jonka tulosten perusteella neljä ratkaisua valittiin jatkokokeiluun. Opinnäytetyössä arvioidut SSPR-ratkaisut ovat Citrix SSPR, PWM, PortalGuard, Ayehu EyeShare, Shaun Vermaakin kehittämä avoimen lähdekoodin SSPR-ratkaisu, HyperSocket Access Manager, JiJi Self Service Password Reset ja NetIQ Self-Service Password Reset. Analyysien perusteella valituista ratkaisuista valittiin jatkokokeiluun seuraavat ratkaisut: Citrix SSPR, PWM, Shaun Vermaakin SSPR-ratkaisu ja HyperSocket Access Manager.

Jatkokehitykseen kuului Citrix XenApp 7.15 LTSR -version päällä toimivan virtualisointipalvelun rakentaminen. Valmis virtualisointipalvelu toimi kokeiluympäristönä, johon valitut SSPR-ratkaisut otettiin käyttöön. Shaun Vermaakin SSPR-ratkaisua ja HyperSocket Access Manageria ei teknisten ongelmien vuoksi saatu kohtuullisessa ajassa kokeiluympäristön käyttöön valmiiksi, joten lopulliseen kokeiluympäristöön pystytettiin onnistuneesti vain Citrix SSPR ja PWM-ratkaisut. Työn lopuksi onnistuneet SSPR-ratkaisut esiteltiin toimeksiantajalle ja niiden käyttöönottoon liittyvät dokumentoinnit luovutettiin toimeksiantajan käyttöön sisäistä jatkokehitystä varten.

2 Oulun DataCenter Oy

Oulun DataCenter Oy on oululainen tietotekniikka-alan yritys, joka tarjoaa asiakkailleen konesali- ja pilvipalveluita. Yritys on perustettu vuonna 2013 [1][2]. Yrityksen toimitusjohtajana on toiminut Mika Lähteenmäki vuodesta 2016 lähtien, jolloin yrityksen pääomistaja Juha Kantola siirtyi yrityksen hallituksen puheenjohtajaksi [3]. Yrityksen liikevaihto on lähes nelinkertaistunut neljässä vuodessa: vuonna 2013 liikevaihto oli 548 000 € ja vuonna 2017 2 092 000 € [2]. Vuonna 2017 yritys työllisti kymmenen työntekijää. Yritys tarjoaa asiakkailleen neljää erilaista palvelua, jotka ovat ODC Alusta, ODC Laitetila, ODC Kapasiteetti ja ODC Jatkuvuus [4].

ODC Alusta on PaaS-palvelu, jonka tarkoituksena on muuttaa asiakkaan toimittama perinteinen työasemalle paikallisesti asennettava ohjelmisto SaaS-palveluksi. Palvelu on toteutettu Citrix XenApp -teknologian avulla. Käytännössä ratkaisu toimii siten, että asiakkaan palveluntarjoajalle toimitettu sovellus asennetaan palveluntarjoajan tarjoamalle Windows Server -palvelinklusterille, jossa jokaisessa palvelimessa on asennettuna Citrix Virtual Delivery Agent -ohjelma [5]. Palvelinklusteri kootaan Citrix XenApp -jakeluryhmäksi, jonka kautta virtualisoidut sovellukset julkaistaan käyttäjille. Käyttäjät pääsevät käsiksi julkaistuihin sovelluksiin Citrix Receiver -ohjelman kautta. Citrix Receiver siirtää virtualisoidun ohjelman dataa ICA-protokollan yli ja tuloksena on käyttöalustariippumaton virtualisoitu SaaS-sovellus [6].

ODC Laitetila on colocation-palvelu, joka tarjoaa asiakkaalleen oikeuden tuoda omistamiansa laitteita Oulun DataCenter Oy:n konesaleihin. ODC Laitetila -palvelu ei kuitenkaan rajoitu pelkkään räkkipaikkaan tai kokonaiseen räkkiin konesalissa, vaan palvelu sisältää myös muun muassa palomuureja, kytkimiä ja muita verkkoinfrastruktuurin komponentteja asiakkaiden tarpeisiin sovitettuna [7].

ODC Kapasiteetti on IaaS-palvelu, jolla Oulun DataCenter Oy tarjoaa asiakkailleen laskentatehoa ja tallennustilaa. Palvelun tilaava asiakas saa palveluntarjoajan konesalista sopimuksen mukaan muun muassa keskusmuistia, prosessoriytimiä ja tallennustilaa. Palveluun sisältyy myös verkkoinfrastruktuurin sekä virtuaalikoneiden tarjoaminen. Asiakas voi hallita hankkimaansa kapasiteettiaan henkilökohtaisen hallintapaneelinsa kautta [8].

ODC Jatkuvuus on Disaster Recovery-as-a-Service ja Backup-as-a-Service -palvelu, jonka tarkoituksena on turvata asiakkaan liiketoiminnalle kriittinen data. ODC Jatkuvuus-

palvelussa asiakkaan liiketoimintapalveluiden pääosainen sijoituspaikka ei ole Oulun DataCenter Oy:n konesalit tai palvelimet, mutta kyseisten palveluiden data varmuuskopioidaan tai kahdennetaan palveluntarjoajan laitteille. DRaaS-vaihtoehdossa data on suoraan käytettävissä ongelmatilanteissa, BaaS-palvelussa data on palautettavissa määrätyn ajan kuluessa [9].

3 Pilvipalvelut

Yhdysvaltain standardien ja teknologian kansallinen instituutti NIST (National Institute of Standards and Technology) on esittänyt julkaisussaan [10] pilvipalveluille sen määritelmän, mitä tässä opinnäytetyössä käytetään. NIST:n mallin mukaan pilvipalveluilla on viisi eri tunnuspiirrettä: itsepalveltavuus, saatavuus, resurssien poolaus, elastisuus ja palvelun mittaus.

Itsepalveltavuus on NIST:n mukaan sitä, että käyttäjä voi omatoimisesti ja automaattisesti tarpeen vaatiessa varata itselleen laskentakykyä, kuten palvelimen suorituskykyä ja tallennustilaa, ilman että hänen tarvitsee ottaa palveluntarjoajan työntekijään yhteyttä.

Saatavuudella määritellään NIST:n mukaan siten, että pilvipalvelu on saatavissa internetyhteyden yli useammalla alustalla, kuten mobiililaitteilla, tableteilla, kannettavilla tietokoneilla ja työasemilla.

Resurssien poolaus määritellään siten, että palveluntarjoajan laskentakapasiteetti ja -resurssit ovat yhdistetty sillä tarkoituksella, että resurssit voidaan jakaa useamman käyttäjän kesken. Resursseja voidaan dynaamisesti jakaa erinäisille pilvipalveluille erinäisten mittareiden, kuten käytön ja kuluttajien tarpeiden mukaan. Käyttäjät eivät tarkalleen tiedä missä resurssit fyysisesti sijaitsevat. Käyttäjät voivat esimerkiksi epätarkasti tietää valtiotasolla, kaupunkitasolla tai datacentertasolla missä resurssit sijaitsevat.

Elastisuus tarkoittaa sitä, että käyttäjän palvelun resursseja voidaan skaalata liukuvasti ja nopeasti, joissakin tapauksissa automaattisesti, käyttäjän tarpeiden mukaan. Hyvin toteutettuna elastisuus voi aiheuttaa kuluttajalle kuvan siitä, että palvelun käyttökapasiteetti on rajaton ja resursseja voidaan tarjota välittömästi ilman viivettä.

Palvelun mittaus tarkoittaa sitä, että pilvipalveluissa on käytössä mittausominaisuus, joka mittaa palvelun käyttöä jollain mittarilla, kuten muistin käytöllä, laskentatehon käytöllä, verkon käytöllä tai aktiivisten käyttäjien määrällä. Mittausohjelmisto optimoi sekä hallitsee resursseja näiden mittareiden tulosten perusteella. Mittareista saatuja tietoja voidaan monitoroida, hallita ja raportoida, luoden läpinäkyvyyttä palvelun toiminnasta sekä palveluntarjoajalle että asiakkaalle.

NIST määrittelee pilvipalveluille kolme eri palvelumallia: SaaS, PaaS ja IaaS. SaaS (Software-as-a-Service, ohjelmisto palveluna) on pilvipalvelumalli, jossa käyttäjä käyttää palveluntarjoajan tarjoamaa, pilvipalveluinfrastruktuurin päällä toimivaa, ohjelmistoa. SaaS-

mallin mukaiset ohjelmistot ovat käyttöjärjestelmäriippumattomia ja usein myös alustariippumattomia: ohjelmia käytetään verkkoselaimen tai erillisen ohjelmakäyttöliittymän kautta. Käyttäjällä ei ole pääsyä eikä hallintaoikeuksia ohjelman takana toimivaan pilvi-infrastruktuuriin, kuten pilvipalvelimiin, käyttöjärjestelmiin tai tallennustilaan. Käyttäjän hallinnassa ovat vain hänelle julkaistujen yksittäisten SaaS-ohjelmien asetukset, joskus eivät edes ne.

SaaS-mallia on kuvailtu sitä edeltävän ASP (Application Service Provider) -mallin korvaajaksi. [11] ASP-mallissa palveluntarjoaja asentaa omalle laitteistolleen tarjottavan ohjelmiston ja tarjoaa siihen pääsyä internetyhteyden yli [12]. ASP-malli on huomattavasti SaaS-mallia vanhempi ja siitä puuttuukin modernin pilvipalvelumallin edut: ASP-palvelut eivät ole elastisia eikä niiden takana olevia resursseja ole poolattu.

PaaS (Platform-as-a-Service, alusta palveluna) on pilvipalvelumalli, jossa palveluntarjoaja tarjoaa käyttäjälle alustan, jolle käyttäjä voi pystyttää, asettaa ja asentaa palveluntarjoajan tukemia sovelluksia, ohjelmia ja ohjelmistoja. Käyttäjällä ei ole pääsyä eikä hallintaoikeuksia alustan alla toimivaan pilvi-infrastruktuuriin, kuten palvelimiin, verkkoon ja käyttöjärjestelmiin. Käyttäjä voi hallita pystyttämiään sovelluksia sekä mahdollisia alustan hienosäätöasetuksia.

IaaS (Infrastructure-as-a-Service, infrastruktuuri palveluna) on pilvipalvelumalli, joka tarkoittaa kuluttajalle laskentatehon, tallennustilan, verkkojen ja muiden tähdellisten tietoteknisten resurssien tarjoamista. Käyttäjällä on oikeus ja kyky pystyttää tarjotun infrastruktuurin päälle ohjelmistoja ja palveluja, mukaan lukien käyttöjärjestelmiä. Käyttäjä ei kuitenkaan hallitse infrastruktuurin alla toimivaa pilvi-infrastruktuuria, mutta käyttäjä voi hallita käyttöjärjestelmiä, tallennustilaa ja sovelluksia. Käyttäjällä voi myös olla oikeus hallita verkkoa osittain, esimerkiksi palomuurien osalta.

4 Citrix

Citrix, täydeltä nimeltään Citrix Systems Inc., on yhdysvaltalainen sovelluskehitysyritys. Citrix erikoistuu sovellus- ja palvelinvirtualisointiohjelmistojen kehittämiseen. Citrixillä on myös vahva osa erinäisten pilvipalvelualustaratkaisujen, kuten SaaS-palvelujen, tuottamisessa [13][14]. Toukokuussa 2018 Citrixin virtualisointituotteiden, Citrix XenAppin, Citrix XenDesktopin ja Citrix XenServerin yhdistetty markkinaosuus oli 11,32 % [15].

4.1.1 Citrixin historia

Citrix perustettiin vuonna 1989 IBM:n entisen työntekijän, Edward Iacobuccin, toimesta [13][14][16][17]. Yrityksen alkuperäinen nimi oli Citrus Systems [17], mutta nimeksi vaihdettiin Citrix Systems, kun paljastui että yritys nimeltä Citrus Systems oli jo olemassa ja kyseisen nimen omistavalla yrityksellä oli jo nimeen tavaramerkkioikeudet. Citrixin päätoimisto siirrettiin yrityksen varhaisessa vaiheessa Floridaan, jossa se on pysynyt nykypäivään saakka. Yrityksen ensimmäinen tuote oli nimeltään Citrix Multiuser, joka perustui IBM:n kehittämään OS/2-alustaan. Citrix lisensioi tuotetta varten OS/2-alustan lähdekoodin Microsoftilta. Projekti johti läheiseen yhteistyöhön Microsoftin kanssa ja osana projektia Citrix kehitti ICA-protokollan. Citrix Multiuser ei tuotteena itsessään kuitenkaan menestynyt, sillä Microsoft lopetti OS/2-alustan tukemisen ja siirtyi jatkokehittämään kehittämäänsä Windows-alustaa. [14.][16.]

Citrix jatkoi kuitenkin etäyhteysohjelmien kehittämistä Citrix Multiuserin pohjalta ja tuloksena oli kolme eri tuotetta, jotka tunnettiin tuotenimillä WinView, WinFrame ja MultiWin [18]. Multiuserin seuraajat kehitettiin olemaan yhteensopivia Microsoftin DOS- ja Windows-alustojen kanssa. Citrix lisensioi Microsoftilta WinFramen kehitystä varten Windows NT 3.51 -käyttöjärjestelmän lähdekoodin. Citrix ei saanut Microsoftilta lisensioitua enää WinFramen seuraajan, MultiWinin, kehitystä varten Windows NT 4 -käyttöjärjestelmän lähdekoodia. Päinvastoin, Microsoft lisensioi itselleen omaa kehitysprojektiaan varten Citrixin aiemmin kehittämän ICA-protokollan lähdekoodin. Tämän kehitystyön seurauksena syntyi Windows Terminal Server Edition -käyttöjärjestelmä ja Microsoftin RDP-protokolla. Citrix ei seuraavaksi julkaissut enää kilpailevaa tuotetta, vaan alkoi kehittämään laajennuksia Microsoftin Terminal Serveriin tuotenimellä MetaFrame. [16.]

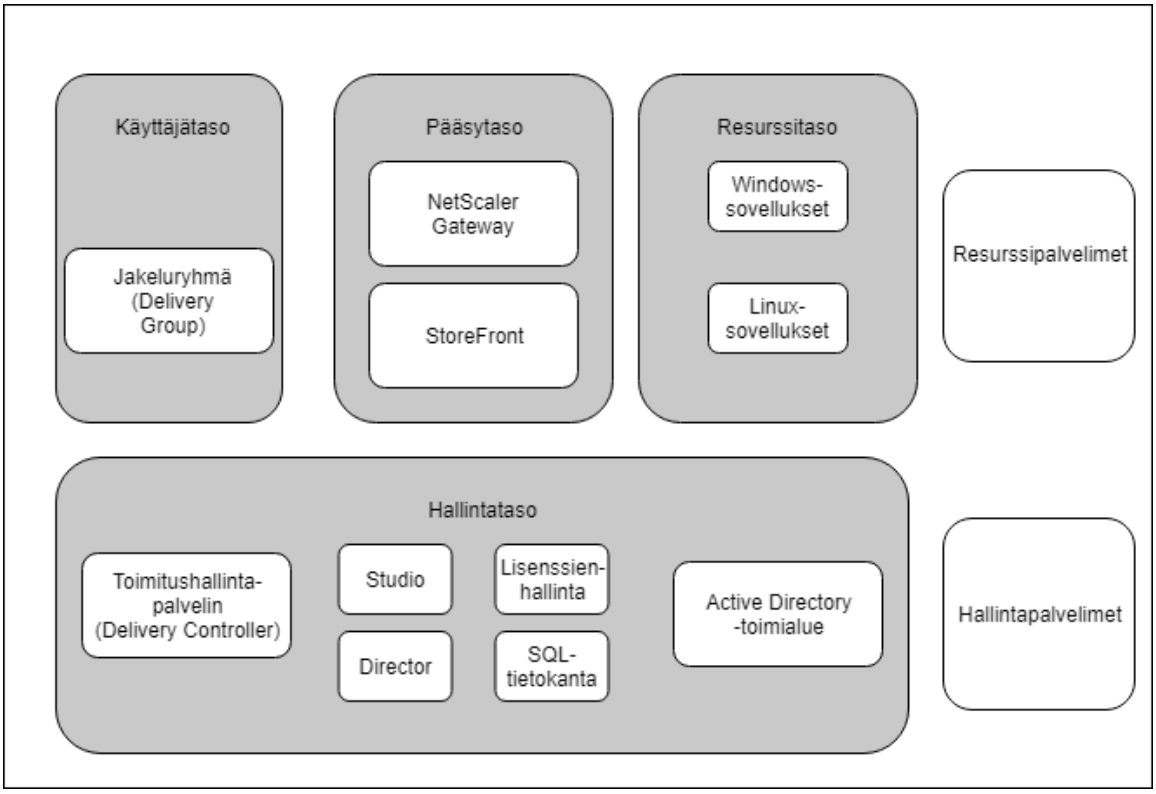
Nykypäivänä Citrixillä on tarjonnassa virtualisointia varten kolme eri ohjelmistoa: Citrix XenApp, Citrix XenDesktop ja Citrix XenServer.

4.1.2 ICA-protokolla

ICA (Independent Computing Architecture, itsenäinen laskenta-arkkitehtuuri) on Citrixin kehittämä protokolla, jota Citrixin virtualisointituotteet edelleen käyttävät käyttäjäsessio-yhteyksiin. Ensimmäinen versio ICA:sta kehitettiin vuonna 1989 Citrix Multiuser -tuotetta varten [14][16]. ICA on korkean tason protokolla, joka toimii usean standardisoidun verkkoprotokollan, kuten TCP/IP, IPX/SPX ja NetBIOS:in, päällä [19]. OSI:n seitsenkerroksisessa protokollamallissa ICA sijoittuu kerrokselle 6, eli esitystapakerrokselle. [20.] ICA-protokolla on toiminut merkittävässä asemassa etätyöpöytäteknologian kehityksessä, sillä se toimi esikuvana Microsoftin RDP-protokollalle [16].

4.1.3 Citrix XenApp & XenDesktop

Citrix XenApp ja Citrix XenDesktop ovat Citrixin tarjoamia virtualisointiohjelmistoja, joiden pääkäyttötarkoitus on sovellusvirtualisointi: käyttäjä voi muuttaa perinteisen työasemalle tai palvelimelle asennettavan sovelluksen virtualisoiduksi sovellukseksi, joka toimii ikään kuin samalla periaatteella mitä SaaS-palvelut. Tämä tuo mukanaan kaikki SaaS-palvelujen edut, kuten käyttöalustariippumattomuuden ja hallinnan keskittämisen. Citrix XenDesktop tarjoaa samat sovellusvirtualisointiominaisuudet kuin Citrix XenApp -ohjelmisto, mutta sen avulla voidaan myös luoda kokonaan virtualisoituja työpöytiä käyttäjille. [21.] Tyypillisen Citrix XenApp -ympäristön komponentit ovat kuvan 1 mukaiset.



Kuva 1. Tyypillisen Citrix XenApp -ympäristön komponentit.

Citrix XenApp- ja Citrix XenDesktop -ympäristöt muodostuvat useasta eri komponentista jotka voidaan jakaa eri tasoihin: käyttäjätasoon, pääsytasoon, resurssitasoon ja hallintatasoon. Käyttäjätasosta, pääsytasosta ja resurssitasosta huolehtivat komponentit ajetaan resurssipalvelimilla, hallintatasosta huolehtivat komponentit ajetaan hallintapalvelimilla.

Käyttäjätasoon kuuluva jakeluryhmä on Studio-hallintaohjelmassa määritelty hallintayksikkö, joka koostuu käyttäjistä, käyttäjäryhmistä ja Studiossa luoduista konekatalogeista. Konekatalogi on yksikkö, joka sisältää yhden tai useamman virtuaalitoimitusagenttipalvelimen. Virtuaalitoimitusagenttipalvelin (eng. virtual delivery agent, VDA) on palvelin, jolle Citrix XenAppin virtuaalitoimitusagenttiohjelma on asennettu. Agentti mahdollistaa palvelimelle asennettujen sovellusten virtualisoinnin ja niiden ajon Citrix Receiver -ohjelman kautta. Virtuaalitoimitusagenttipalvelimet kuuluvat resurssipalvelimiin.

Pääsytaso sisältää käyttäjien palveluun pääsystä huolehtivat komponentit: NetScaler Gatewayn ja StoreFrontin. NetScaler Gateway on kuormanjakopalvelu, joka ei ole pakollinen komponentti valmiissa Citrix XenApp -ympäristössä. StoreFront on komponentti, joka vastaa käyttäjille näkyvästä kirjautumisnäkymästä, käyttäjien sisäänkirjautumisesta sekä julkaistujen sovellusten esittämisestä käyttäjille.

Resurssitaso sisältää virtuaalitoimitusagenttipalvelimille asennetut ohjelmat, joita käyttäjien on mahdollista käyttää. Ohjelmat ajetaan virtuaalitoimitusagenttipalvelimilla ja ohjelman kuva, ääni ja muu data siirretään loppukäyttäjän laitteelle Citrix Receiver -ohjelman kautta käyttäen ainakin osittain Citrixin omaa ICA-protokollaa.

Hallintatason komponentteihin sisältyvät toimitushallintapalvelin, Studio-palvelin, Director-palvelin, lisenssienhallintapalvelin, SQL-tietokantapalvelin ja Active Directory -toimialue. Kaikki muut palvelut paitsi Active Directory -toimialueesta vastaavat palvelut on mahdollista asentaa yksittäiselle hallintapalvelimelle, mutta varsinkin suuremmissa kokoonpanoissa on suositeltavaa asentaa jokainen komponentti erilliselle palvelimelle. Studio on Citrix XenApp -ympäristön hallintaohjelmisto, jolla voidaan muun muassa hallinnoida julkaistuja virtuaalisovelluksia, konekatalogeja ja jakeluryhmiä. Studion kautta hallitaan myös StoreFront-palvelun asetuksia. Director on tarkkailuun tarkoitettu hallintakonsoli, johon on koottu erilaisia tietoja XenApp-palvelun käytöstä. Directorista näkee muun muassa käytössä olevien yhteyksien määrän, epäonnistuneet kirjautumisyritykset ja sen, kuinka kauan käyttäjien avaamien virtualisoitujen sovelluksien käynnistymisessä kuluu aikaa.

Lisenssienhallintapalvelin vastaa Citrix-ympäristön lisenssien hallinnasta. Citrixin lisenssien hallinta on kaksiosainen prosessi: ensin järjestelmänvalvojan tulee kirjautua Citrixin lisenssienhallintasivustolle, jonka kautta järjestelmänvalvoja allokoi omistamansa lisenssit jollekin laitteelle. Allokointiperusteita voivat olla esimerkiksi laitteen IP-osoite ja laitteen MAC-osoite. Allokoinnin jälkeen järjestelmänvalvoja lataa lisenssitiedoston lisenssipalvelimelle ja asettaa sen käyttöön lisenssienhallintaohjelmiston kautta. Lisenssienhallintaohjelmiston kautta tapahtuvat muut lisensseihin liittyvät, kuten vanhan lisenssin käytöstä poistaminen.

SQL-tietokantapalvelin hallintatason komponenttina sisältää Citrix XenApp -ympäristön toimintaan kuuluvaa dataa. Active Directory -toimialue vastaa muun muassa käyttäjätileistä, käyttöoikeuksista, käyttäjäryhmistä ja käyttäjien autentikoinnista. Valmiiseen Citrix XenApp -palveluun kirjaudutaan toimialueen käyttäjätileillä. Jokaisen Citrix XenApp -palveluun kuuluvan palvelimen tulee olla toimialueen jäsen. [22.]

Citrix Receiver on apuohjelma, joka asennetaan loppukäyttäjän laitteelle. Periaatteessa kaikki liikenne loppukäyttäjän laitteen ja Citrix XenApp -ratkaisun välillä tapahtuu Receiverin kautta. Receiveristä on kaksi versiota: paikallisesti asennettava versio jota voidaan käyttää joko verkkoselaimen kautta tai erillisenä ohjelmana sekä HTML5-pohjainen versio, jota voidaan käyttää HTML5-yhteensopivan verkkoselaimen kautta.

4.1.4 Citrix XenServer

Citrix XenServer on Citrixin tarjoama ja Linux Foundation Xen Projectin kehittämä avoimen lähdekoodin palvelinvirtualisointialusta, jonka käyttötarkoituksena on virtuaalikoneiden luonti ja hallinta. XenServer toimii kilpailijana muille palvelinvirtualisointiohjelmistoille, kuten VMwaren vSphere-ohjelmistolle ja Microsoftin Hyper-V-ohjelmistolle. [23.][24.]

5 SSPR-ratkaisujen vertailu

Self Service Password Reset, SSPR, viittaa ratkaisuun, jonka avulla käyttäjä voi itse vaihtaa käyttäjätilinsä salasanan ottamatta yhteyttä palveluntarjoajan tekniseen tukeen. SSPR-ratkaisun käyttöönotto vähentää palveluntarjoajan tukipalveluun tulevien yhteydenottojen määrää ja vapauttaa tukihenkilöt muiden tehtävien suorittamiseen. Yksinkertaisimmillaan SSPR-ratkaisu voidaan toteuttaa turvakysymys-vastausparilla: kyseisessä autentikaatiotavassa käyttäjä vastaa järjestelmänvalvojan asettamiin turvakysymyksiin. Kun käyttäjä unohtaa salasanansa, hän voi vastata turvakysymyksiin ja palauttaa salasanansa vastattuaan kysymyksiin oikein. Kyseisen autentikaatiotavan heikkoutena on se, että käyttäjän pitää muistaa omien turvakysymyksiensä vastaukset. Turvakysymyksien vastaukset voivat olla myös arvattavissa, joka on tietoturvariski.

Uudempi SSPR-autentikaatiometodi on SMS-autentikaatio: käyttäjän unohtaessa salasanansa hän voi syöttää järjestelmään puhelinnumeronsa, jolloin hän saa tekstiviestillä joko väliaikaisen salasanan tai linkin salasananvaihtopalveluun. Toinen tapa toteuttaa SMS-autentikaatio on se, että käyttäjä lähettää tekstiviestin salasananvaihtopalvelun puhelinnumeroon, jolloin järjestelmä etsii puhelinnumeroa vastaavan käyttäjätilin, vaihtaa sille väliaikaisen salasanan ja lähettää kyseisen salasanan käyttäjälle.

5.1 Citrix SSPR

Citrix SSPR on Citrixin tarjoama ilmainen lisäkomponentti Citrix XenApp- ja Citrix XenDesktop -ympäristöihin. Citrix SSPR-ratkaisun etuna on se, että ratkaisu integroituu suoraan Citrix StoreFront-palveluun, jolloin SSPR-ratkaisua varten ei tarvitse erillistä verkko-osoitetta. Kun Citrix SSPR on otettu käyttöön, StoreFrontin etusivulle ilmestyy uusi painike, jonka valitsemalla käyttäjä saa vaihtoehdoksi poistaa tilin lukituksen sekä vaihtaa käyttäjätilin salasanan. Kirjautuneelle käyttäjälle ilmestyy Receiverin näkymään uusi välilehti, jonka kautta käyttäjä voi hallinnoida turvakysymyksien vastauksia. [25.]

Citrix SSPR -ratkaisun heikkoutena on sen suppeat mukautusmahdollisuudet: palvelusta on mahdollista mukauttaa ainoastaan turvakysymys-vastausparien kysymyksiä ja vastauksia. Palvelu ei tarjoa muita autentikaatiotapoja. Citrix SSPR ei myöskään ole yhteensopiva NetScalerin kanssa, mutta Citrix on ilmoittanut [26] kehittävänsä yhteensopivuustilaa näiden kahden ratkaisun välillä.

Citrix SSPR -ratkaisun heikkouksista huolimatta ratkaisu päätettiin ottaa tässä opinnäytetyössä jatkokokeiluun, sillä se on ainoa Citrixin tarjoama SSPR-ratkaisu. Näin ollen kyseinen ratkaisu toimi hyvänä vertailukohtana muihin työssä käsiteltyihin SSPR-ratkaisuihin. Citrix SSPR -ratkaisun SWOT-analyysi löytyy liitteestä numero 1.

5.2 PWM

PWM, Password Management Servlets, on The PWM Project -nimisen yhteisön kehittämä avoimen lähdekoodin SSPR-ratkaisu. PWM on Java-pohjainen ratkaisu ja se vaatii toimiakseen Java Runtime Environment -ympäristön sekä Tomcat -ohjelman asennuksen. Jokainen ratkaisuun kuuluva komponentti on ilmainen.

PWM tarjoaa erittäin laajat mukautusmahdollisuudet. Valmiissa ratkaisussa voidaan muun muassa mukauttaa autentikointitapaa, salasananvaihtotapaa, käyttöliittymän ulkoasua sekä mitä tahansa ohjelmassa esiintyvää tekstiä. Ohjelmaan on myös mahdollista lisätä lisäominaisuuksia, kuten SMS-moduuli, sähköpostimoduuli ja kaksivaiheinen tunnistautuminen. Ohjelman salasananpalautusmetodeja on myös mahdollista mukauttaa: oletuksena ohjelmassa ainoa käytössä oleva salasananpalautusmetodi on turvakysymys-vastauspari, mutta ohjelmaan on mahdollista lisätä muitakin autentikaatiotapoja kuten LDAP-attribuuttien perusteella autentikaatio, tekstiviestiautentikaatio ja sähköpostiautentikaatio. [27.]

Koska PWM tarjoaa laajat mukautusmahdollisuudet vaativankin organisaation tarpeisiin, kyseinen ratkaisu päätettiin valita jatkokäyttöön. PWM-palvelun käyttöönotto voidaan myös toteuttaa kokonaan ilmaisilla ohjelmistoilla, joten ratkaisun kokonaishinta on hyvin alhainen. PWM-ratkaisun SWOT-analyysi löytyy liitteestä numero 2.

5.3 Shaun Vermaakin kehittämä avoimen lähdekoodin SSPR-ratkaisu

Shaun Vermaakin kehittämä avoimen lähdekoodin SSPR-ratkaisu on samannimisen henkilön kehittämä, nimeämätön SSPR-ratkaisu. Kyseinen ratkaisu on ilmainen, C#-ohjelmointikielellä toteutettu ratkaisu. Kehittäjä tarjoaa artikkelissaan [28] latauslinkkiä kyseiseen ratkaisuun, joka avataan Visual Studio -ohjelmassa. Kyseisen ohjelman kautta ratkaisua voidaan muokata vapaasti ennen käyttöönottoa. Salasananpalautusmetodeja on yksi: turvakysymys-vastauspari.

Ratkaisu valittiin jatkokokeiluun sen takia, että toimeksiantaja esitti yhdeksi mahdolliseksi vaihtoehdoksi oman SSPR-ratkaisun kehittämisen. Shaun Vermaakin kehittämä ratkaisu tarjosi erinomaisen pohjan tälle lähestymistavalle. Shaun Vermaakin kehittämän ratkaisun SWOT-analyysi löytyy liitteestä numero 3.

5.4 HyperSocket Access Manager

HyperSocket Access Manager on Hypersocket Softwaren kehittämä SSPR-ratkaisu. HyperSocket Access Manager otetaan käyttöön asentamalla valmis virtuaalilaite, joka sitten konfiguroidaan käyttöönottovaiheessa. Kyseisestä ratkaisusta on saatavilla sekä ilmaisversio että käyttäjämäärän mukaan laskutettu maksullinen versio. Ilmaisversio sisältää itse SSPR-ratkaisun, jossa on yksi salasananpalautusmetodi: turvakysymys-vastauspari. Maksullinen versio sisältää muitakin salasananpalautusmetodeja, kuten esimerkiksi Captcha-autentikaation, salasanahistoria-autentikaation, PIN-koodi-autentikaation ja monivaiheisen autentikaation. [29.]

Ratkaisun ilmaisversion ominaisuudet olivat niin kattavat, että ratkaisu päätettiin ottaa jatkokokeiluun mukaan. Ratkaisussa katsottiin myös olevan potentiaalia mahdolliseen jatkokehitykseen maksullisen version muodossa. HyperSocket Access Managerin SWOT-analyysi löytyy liitteestä numero 4.

5.5 PortalGuard

PortalGuard on PistolStar Inc:n kehittämä verkkoportaalien luontiin tarkoitettu ohjelmisto, jonka yhtenä komponenttina on SSPR-ratkaisu. PortalGuardilla on mahdollista luoda turvallinen ja skaalautuva verkkoportaali. Muita PortalGuardin ominaisuuksia ovat Single Sign-On -ympäristön luontityökalu, kaksivaiheinen autentikaatio kirjautumisessa ja kontekstuaalisen autentikaation käyttöönotto. [30.]

PortalGuard SSPR-ratkaisun käyttöönottohinta on 5000 dollaria ja lisenssin hinta on 5000 dollaria vuodessa. Täyden PortalGuard-ratkaisun käyttöönottohinta on 20000 dollaria ja lisenssin hinta on 5000 dollaria vuodessa [31]. Nämä kustannukset ovat niin korkeat, että kyseinen ratkaisu todettiin sopimattomaksi tämän opinnäytetyön tarkoituksiin. PortalGuardin SWOT-analyysi löytyy liitteestä numero 5.

5.6 Ayehu EyeShare

Ayehu EyeShare on Ayehu Software Technologiesin kehittämä automaatioalusta. EyeShare on kattava automaatioalusta, jolla on mahdollista luoda myös omaa ympäristöä varten räätälöity SSPR-ratkaisu. EyeSharen etuna on myös se, että siihen on mahdollista lisätä SMS-moduuli, jolloin käyttäjät voivat lähettää tiettyyn puhelinnumeroon salasanan-vaihtopyynnön, jonka järjestelmä käsittelee ja vaihtaa käyttäjän salasanan väliaikaiseen salasanaan, jonka järjestelmä sitten lähettää takaisin käyttäjälle. [32.]

Ratkaisu todettiin liian järeäksi tämän opinnäytetyön tarkoituksiin. Ratkaisun käyttöönoton hinnasta ei myöskään saatu selvää arviota. Näiden seikkojen perusteella ratkaisua ei päätetty ottaa jatkokokeiluun mukaan. EyeSharen SWOT-analyysi löytyy liitteestä numero 6.

5.7 JiJi Self Service Password Reset

JiJi Self Service Password Reset on JiJi Technologies -yrityksen kehittämä SSPR-ratkaisu. Ratkaisu tukee muun muassa monitahoista autentikaatiota ja SMS-autentikaatiota. Ratkaisu integroituu myös Microsoftin Outlook Web App -ympäristöön. [33.]

Koska Jiji Self Service Password Resetin markkinaetuna on Outlook Web App -ympäristöön integroituminen, eikä kohdeympäristössä ei ole käytössä OWA-komponentteja, todettiin kyseinen ratkaisu jatkokehitykseen sopimattomaksi. JiJi Self Service Password Resetin SWOT-analyysi löytyy liitteestä numero 7.

5.8 NetIQ Self Service Password Reset

NetIQ Self Service Password Reset on Micro Focus -yrityksen kehittämä SSPR-ratkaisu. NetIQ SSPR pohjautuu The PWM Projectin kehittämään PWM-ratkaisuun ja on siitä kaupallinen versio. Ratkaisu toimitetaan virtuaalisena laitteena, joka on konfiguraation jälkeen valmis käyttöön. Koska NetIQ SSPR perustuu PWM-ratkaisuun, [26] siinä on myös erittäin laajat mukautusvaihtoehdot. [34.]

Kyseinen ratkaisu todettiin jatkokokeiluun tarpeettomaksi, sillä PWM itsessään on jo erittäin laaja opinnäytetyön tarkoitukseen sopiva ratkaisu. Ratkaisun hinta on myös tuntematon.

6 Kokeiluympäristön käyttöönotto

Opinnäytetyön yhtenä vaiheena otettiin käyttöön Citrix XenApp -kokeiluympäristö. Kokeiluympäristön versiona toimi versio 7.15 LTSR. Kokeiluympäristö koostui kahdesta Windows Server 2016 toimialueen ohjauspalvelimesta, toimitushallintapalvelimesta sekä virtuaalitoimitusagenttipalvelimesta. Ympäristöön sisältyi myös toimialue ja siihen sisältyvä Active Directory -hakemistopalvelu. Kokeiluympäristö otettiin käyttöön toimeksiantajan tarjoamassa VMware vCloud -ympäristössä.

6.1 Ohjauspalvelinten ja toimialueen luonti

Kokeiluympäristön käyttöönotto aloitettiin luomalla kaksi Windows Server 2016 -virtuaalikonetta, joille kummallekin asetettiin kaksi prosessoriydintä, neljä gigatavua keskusmuistia sekä 40 gigatavua kovalevytilaa. Molempiin palvelimiin asennettiin Windows Server 2016 Standard -käyttöjärjestelmä. Käyttöjärjestelmän asennuksen jälkeen virtuaalikoneille asetettiin aliverkosta omat IP-osoitteet sekä ne nimettiin uudelleen taulukon 1 mukaisesti.

	testdc01.ilkkatest.local	testdc02.ilkkatest.local
IP-osoite	10.0.0.102	10.0.0.103
Aliverkon peite	255.255.255.0	255.255.255.0
Oletusyhdyskäytävä	10.0.0.1	10.0.0.1
Ensisijaisen nimipalvelimen osoite	127.0.0.1	127.0.0.1
Toissijaisen nimipalvelimen osoite	8.8.8.8	8.8.8.8

Taulukko 1. Toimialueen ohjauspalvelinten verkkoasetukset.

Seuraavaksi ensimmäiselle palvelimelle asennettiin AD DS -rooli, jonka asennus onnistuu Server Manager -ohjelman ”Add roles and features” -apuohjelman avulla. Asennuksen

jälkeen palvelin ylennettiin toimialueen ohjauspalvelimeksi Active Directory Domain Services Configuration Wizard -apuohjelman avulla. Apuohjelmassa luotiin uusi metsä ja asetettiin toimialueelle nimeksi ilkkatest.local. Metsän ja toimialueen toiminnalliseksi tasoksi asetettiin Windows Server 2016. Toimialueen palautustilan salasana myös asetettiin tässä vaiheessa. Palvelin on ensimmäinen DNS-palvelin uudessa metsässä, joten DNS-delegaatiota ei tarvinnut asettaa. Apuohjelma pyysi tarkastamaan palvelimen NetBIOS-nimen, jonka annettiin olla TESTDC01. Active Directory Domain Servicesin tietokannan, lokitiedostojen ja SYSVOL-kansioiden polut jätettiin niiden oletussijainteihin. Lopuksi ohjauspalvelimen asennus viimeisteltiin, virtuaalikone käynnistettiin uudelleen ja palvelin oli toiminnallinen ilkkatest.local-toimialueen ohjauspalvelin. Sama prosessi toistettiin toisella ohjauspalvelimella, mutta uuden metsän luonnin sijasta palvelin lisättiin olemassa olevaan toimialueeseen.

6.2 Citrix XenApp -toimitushallintapalvelimen luonti

Citrix XenApp -toimitushallintapalvelinta varten luotiin virtuaalikone, jolle asetettiin viisi gigatavua keskusmuistia, kaksi prosessoriydintä sekä 100 gigatavua kovalevytilaa. Nämä vaatimukset kovalevytilaa lukuun ottamatta täyttävät Citrixin minimijärjestelmävaatimukset [35]. Pienempi kovalevytilan määrä ei aiheuttanut kokeilujakson aikana kuitenkaan negatiivisia vaikutuksia. Virtuaalikoneelle asennettiin Windows Server 2016 -käyttöjärjestelmä ja käyttöjärjestelmän asennuksen jälkeen sille asetettiin seuraavat IP-asetukset ja nimi taulukon 2 mukaisesti.

	testdec01.ilkkatest.local
IP-osoite	10.0.0.101
Aliverkon peite	255.255.255.0
Oletusyhdyskäytävä	10.0.0.1
Ensisijaisen nimipalvelimen osoite	10.0.0.102
Toissijaisen nimipalvelimen osoite	10.0.0.103

Taulukko 2. Citrix XenApp -toimitushallintapalvelimen verkkoasetukset.

IP-asetusten asettamisen jälkeen palvelin liitettiin toimialueeseen ja käynnistettiin uudelleen.

Uudelleenkäynnistyksen jälkeen virtuaalikoneeseen asetettiin Citrix XenApp 7.15 LTSR -asennusohjelman sisältävä ISO-tiedosto. Tiedoston sisältämä asennusohjelma avattiin ja avautuneesta näkymästä valittiin ensiksi XenApp- ja sitten ”Delivery Controller” -valinta. Avautuvassa asennusohjelmassa hyväksyttiin lisenssisopimus. Seuraavaksi asennusohjelma kysyi haluttuja komponentteja, joista valittin kaikki. Valitut komponentit olivat seuraavat: itse toimitushallintapalvelinohjelmisto, Citrix Studio, Citrix Director, lisenssipalvelinohjelmisto ja Citrix StoreFront. Suurempia tuotantoympäristöjä varten Citrix suosittelee asentamaan komponentit erillisille koneille [36], mutta pienessä kokeilukokoonpanossa komponentit voitiin asentaa samalle koneelle.

Seuraavaksi asennusohjelma kysyi, asennetaanko Microsoft SQL Server 2012 SP2 Express ja Windowsin etätuki-ominaisuus. Microsoft SQL Server 2012 SP2 Express -ohjelma päätettiin asentaa, sillä kokeilukokoonpanossa ei ollut erillistä SQL-palvelinta jo ennestään luotuna eikä sellaista ollut tarpeellista luoda kyseiseen kokeiluympäristöön. Windowsin etätuki-ominaisuutta ei tarvinnut asentaa, sillä sitä käytetään Citrix Directorin varjostus-ominaisuuteen, jota ei tässä käyttöympäristössä tarvittu. Seuraavaksi asennusohjelma pyysi avaamaan Windowsin palomuurista portteja erinäisiä komponentteja varten. Portit voi avata itse tai antaa asennusohjelman avata ne. Asennusohjelman annettiin avata kyseiset portit. Taulukko 3 havainnollistaa avattuja portteja, jotka olivat seuraavat:

Toimitushallinta-palvelinohjelmisto	Citrix Director	Lisenssipalvelinoh-jelmisto	Citrix StoreFront
80 TCP	80 TCP	7279 TCP	80 TCP
443 TCP	443 TCP	27000 TCP	443 TCP
		8083 TCP	
		8082 TCP	

Taulukko 3. Citrix XenApp -toimitushallintapalvelinohjelmistojen vaatimat portit.

Lopuksi asennusohjelma näytti yhteenvedon valituista vaihtoehdoista ja suoritti itse asennuksen. Asennusprosessin ja uudelleenkäynnistyksen jälkeen palvelin oli toiminnallinen toimitushallintapalvelin.

6.3 Citrix-lisenssin käyttöönotto

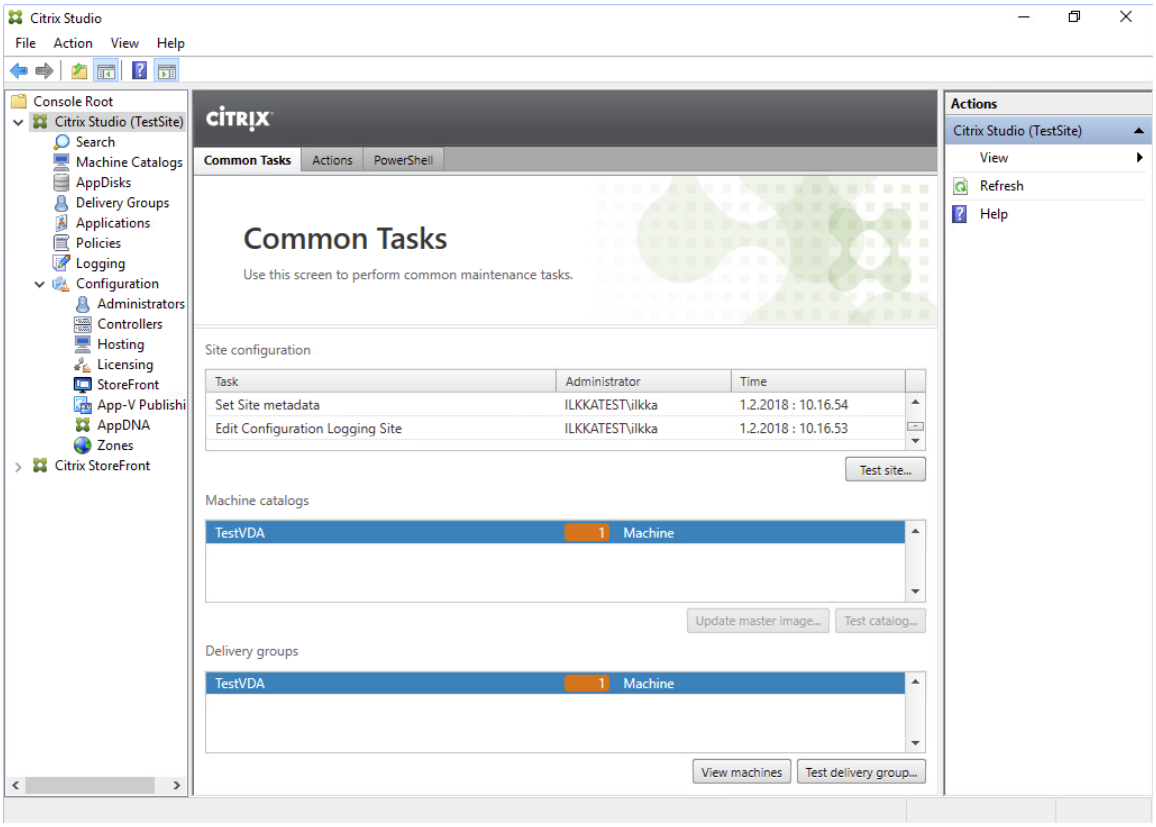
Seuraava osa käyttöönottoa oli Citrix-lisenssin käyttöönotto. Lisenssin käyttöönotto on kaksivaiheinen prosessi; lisenssi täytyy ensin allokoida tietylle lisenssipalvelimelle Citrixin verkkosivujen kautta ja sitten ladata sekä asentaa lisenssitiedosto itse lisenssipalvelimelle.

Lisenssin allokaatio tapahtuu Citrixin nettisivujen lisenssinhallintapalvelun kautta. Lisenssin allokaatioprosessi tapahtui seuraavasti: Ensiksi Citrixin lisenssinhallintapalvelun verkkosivuille kirjauduttiin Citrix-tunnuksilla. Seuraavaksi valittiin ”All Licensing Tools” -kohta, joka avasi Citrixin tarjoamat lisenssinhallintatyökalut. Sitten valittiin ”Activate and Allocate Licenses” -vaihtoehto, joka avasi näkymän, jossa kaikkia kyseiselle Citrix-tilille liitettyjä lisenssejä voidaan hallita. Seuraavaksi valittiin Citrix XenApp -lisenssi sekä painettiin ”Continue” -painiketta, jolloin avautui sivu, jossa lisenssi voitiin allokoida tietylle laitteelle. Ainoana vaihtoehtona oli ”Host ID”, joka tarkoittaa lisenssipalvelimen IP-osoitetta [37]. Lisenssi allokoitiin IP-osoitteelle 10.0.0.101. Lopuksi allokaatio viimeisteltiin painamalla ”Confirm”-nappia. Allokaation jälkeen lisenssitiedosto ladattiin lisenssipalvelimelle.

Seuraavaksi lisenssi otettiin käyttöön lisenssipalvelimella avaamalla ”Citrix License Administration Console” -ohjelma. Ohjelmaan kirjauduttiin toimialueen järjestelmänvalvojan käyttäjätunnuksella. Seuraavaksi valittiin ”Vendor Daemon Configuration” -vaihtoehto ja avautuvasta näkymästä ”Import License” -vaihtoehto. Avautuvasta ikkunasta navigoitiin lisenssitiedoston latauskansioon sekä valittiin kyseinen tiedosto. Seuraavaksi palattiin takaisin ”Vendor Daemon Configuration” -näkymään, klikattiin ”CITRIX” -vaihtoehtoa ja valittiin ”Reread License Files” -vaihtoehto. Tämä varmisti sen, että lisenssipalvelin otti käyttöön sille ladatun lisenssitiedoston onnistuneesti.

6.4 Sijannin luonti

Seuraava vaihe käyttönottoprosessia on sijainnin luonti. Sijainti tarkoittaa yksittäistä Citrix XenApp tai XenDesktop -kokoonpanoa [6] ja se toimii laajimpana hallintayksikkönä Citrix Studio -hallintaohjelmistossa. Sijainnin luonti aloitettiin avaamalla Citrix Studio -hallintaohjelmisto, jonka käyttöliittymää kuva 2 havainnollistaa.



Kuva 2. Citrix Studio -ohjelmiston käyttöliittymä.

Sijainnin luontiprosessi aloitettiin valitsemalla ”Create a Site” -valinta Citrix Studiossa. Avautuvasta apuohjelmasta valittiin ”An empty, unconfigured site” -vaihtoehto, joka nopeuttaa sijainnin luomisprosessia mutta vaatii muiden asetusten asettamista myöhemmin. Sijainnille annettiin nimeksi TestSite. Seuraavassa näkymässä apuohjelma kysyi tietokantojen luonnista. Koska ympäristöön ei ole lisätty erillistä SQL-palvelinta, asetetaan tietokantojen sijainniksi ”.\SQLEXPRESS,” jolloin tietokannat tallentuvat paikalliselle palvelimelle. Seuraavaksi apuohjelma pyysi lisenssipalvelimen osoitetta. Kenttään syötettiin ”testdec01.ilkkatest.local” ja painettiin Connect-painiketta. Ohjelma löysi lisenssipalvelimelle syötetyn lisenssin, joka valittiin kyseisen sijainnin käyttämäksi lisenssiksi. Lopuksi apuohjelma kysyi lisäominaisuuksien asentamisesta. Kyseiset lisäominaisuudet eivät olleet tärkeitä tässä kokeiluympäristössä, joten ne jätettiin asentamatta. Lopuksi apuohjelma näytti yhteenvedon valituista vaihtoehdoista ja sijainnin käyttöönotto viimeisteltiin painamalla Finish-nappia. Näin asennusohjelma loi sijannin ja otti sen käyttöön.

6.5 Virtuaalitoimitusagenttipalvelimen luonti

Seuraava vaihe käyttöönottoprosessissa oli luoda virtuaalitoimitusagenttipalvelin. Virtuaalitoimitusagenttipalvelinta varten luotiin uusi Windows Server 2016 -virtuaalikone, jolle asetettiin kuusi gigatavua keskusmuistia, yksi prosessoriydin ja 40 gigatavua kovalevytilaa. Citrix ei ole asettanut minimivaatimuksia virtuaalitoimitusagenttipalvelimille. [33] Käyttöjärjestelmän asennuksen jälkeen palvelimelle asetettiin staattinen IP, nimettiin uudelleen ja liitettiin toimialueeseen taulukon 4 mukaisesti.

	testvda01.ilkkatest.local
IP-osoite	10.0.0.104
Aliverkon peite	255.255.255.0
Oletusyhdyskäytävä	10.0.0.1
Ensisijaisen nimipalvelimen osoite	10.0.0.102
Toissijaisen nimipalvelimen osoite	10.0.0.103

Taulukko 4. Virtuaalitoimitusagenttipalvelimen verkkoasetukset.

Virtuaalitoimitusagenttiohjelmiston asennusprosessi aloitettiin asettamalla koneeseen Citrix XenApp 7.15 LTSR -ohjelmiston asennuspaketin sisältävä ISO-tiedosto. Asennusohjelma avattiin ja avautuvasta valikosta valittiin ”Virtual Delivery Agent for Windows Server OS” -vaihtoehto. Avautuvasta asennusohjelmasta valittiin ”Enable connections to a server machine” -vaihtoehto. Seuraavassa näkymässä valittiin sekä VDA-ohjelmiston että Citrix Receiver -ohjelman asentaminen. Seuraavaksi asennusohjelma kysyy toimitushallintapalvelimen osoitetta, joka syötettiin FQDN-muodossa: testdec01.ilkkatest.local. Seuraavaksi yhteyden toimivuus varmistettiin ”Test connection” -painikkeella ja lopuksi lisättiin ”Add” -painikkeella. Seuraavaksi asennusohjelma ehdotti lisäohjelmien asentamista, joista valittiin kaikki. Seuraavalla sivulla asennusohjelma pyysi avaamaan Windowsin palomuurista portteja erinäisiä virtuaalitoimitusagenttiohjelmiston komponentteja varten. Portit voi avata itse tai antaa asennusohjelman avata ne automaattisesti. Asennusohjelman annettiin avata kyseiset portit. Taulukko 5 havainnollistaa avattuja portteja.

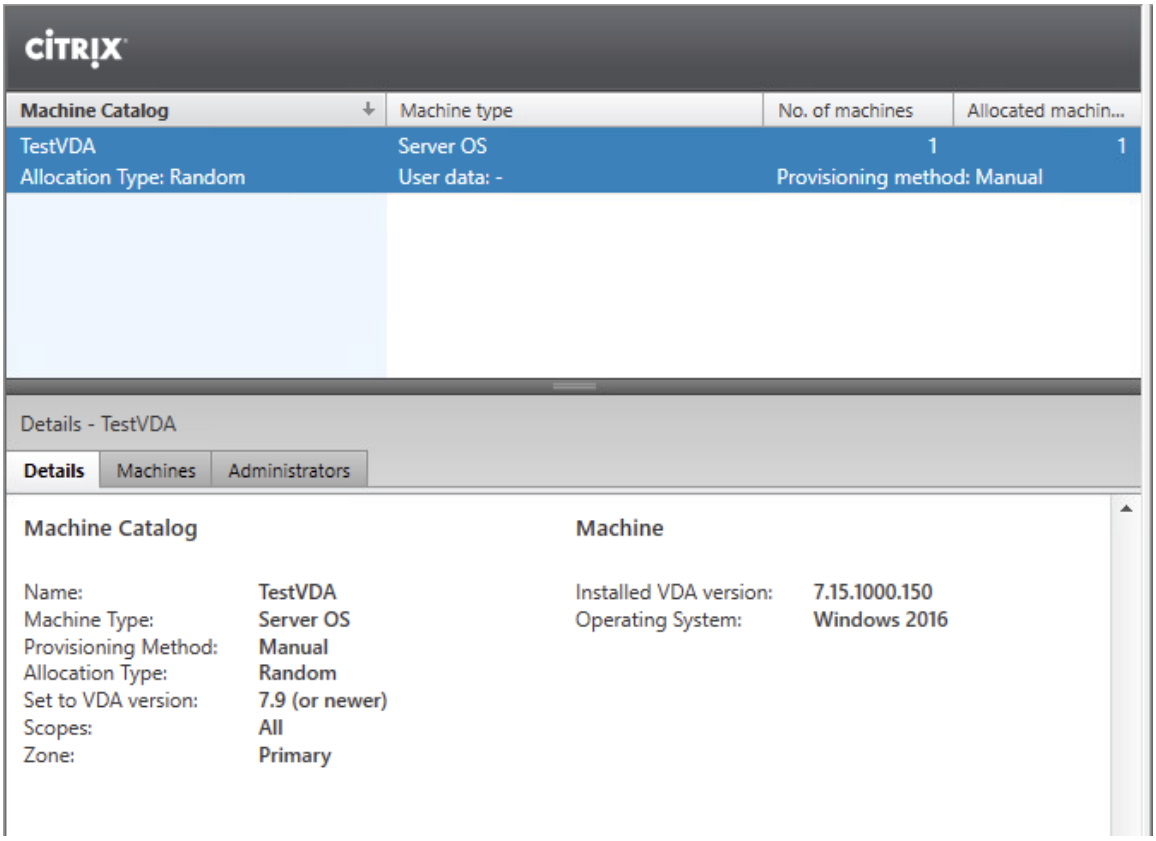
Hallintapalvelimelle tapahtuva kommunikaatio	Windowsin etätuki	Reaaliaikainen äänensiirto
80 TCP	3389 TCP	16500 – 16509 UDP
1494 TCP		
2598 TCP		
8008 TCP		

Taulukko 5. Citrix XenApp -virtuaalitoimitusagentin vaatimat portit.

Lopuksi asennusohjelma esitti yhteenvedon valituista vaihtoehdoista. Asennusprosessi aloitettiin painamalla Install-painiketta. Asennusprosessin aikana palvelin käynnistyi uudelleen kerran ja jatkoi asennusta uudelleenkäynnistyksen jälkeen. Asennuksen valmistuttua palvelin oli toimiva virtuaalitoimitusagentti.

6.6 Konekatalogin luonti

Seuraava osa käyttöönottoa oli konekatalogin luonti Citrix Studiossa. Luontiprosessi aloitettiin avaamalla toimitushallintapalvelimelta Citrix Studio -ohjelmisto, klikkaamalla oikealla hiiren painikkeella ”Machine Catalogs” -kohtaa ja valitsemalla ”Create Machine Catalog” -vaihtoehto. Tämä avasi apuohjelman, jonka avulla konekatalogi luotiin. Ensimmäisenä valittiin konekatalogin käyttämä käyttöjärjestelmätyyppi. Koska virtuaalitoimitusagentti asennettiin Windows Server 2016 -käyttöjärjestelmän päälle, valittiin ”Server OS” -vaihtoehto. Seuraavaksi apuohjelma kysyi, miten konekatalogia hallitaan. Koska konekatalogia ei haluttu tässä kokoonpanossa hallita Citrix Studion kautta, valittiin ”machines that are not power managed” ja ”another service or technology” -valinnat. Seuraavalla sivulla konekatalogiin lisättiin haluttujen virtuaalitoimitusagenttipalvelimien Active Directory -tilit painamalla ”Add computer” -painiketta ja kirjoittamalla avautuneeseen Active Directory -hakuikkunaan tietokoneen nimi. Tämän jälkeen konelistaan ilmestyi virtuaalitoimitusagenttipalvelun ILKKATEST\TESTVDA01. Lopuksi apuohjelma näytti yhteenvedon valituista asetuksista ja konekatalogille syötettiin nimi TestVDA. Konekatalogin luomisen jälkeen luotu katalogi ilmestyi Citrix Studion ”Machine Catalogs” -näkymään (kuva 3).

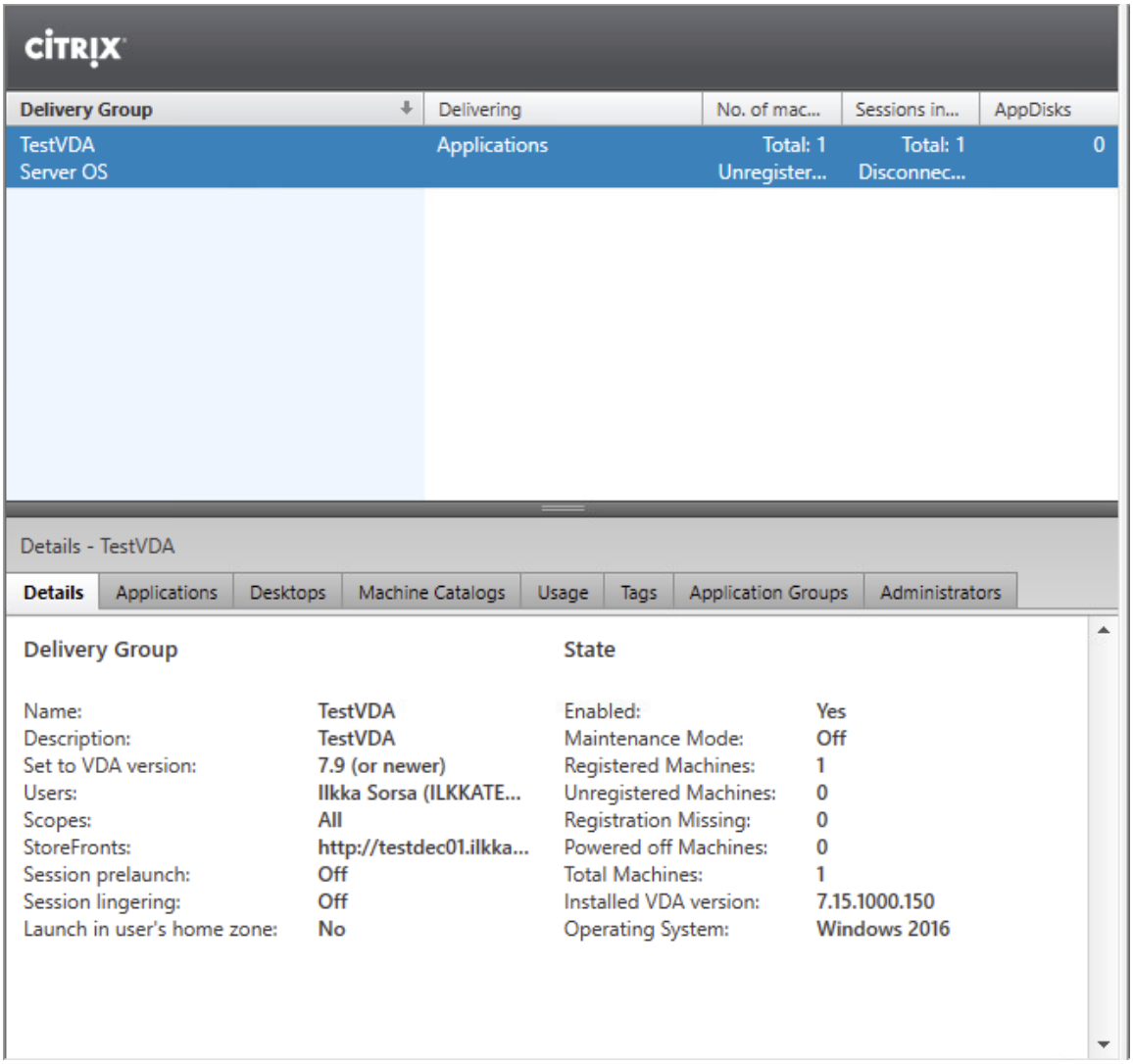


Kuva 3. Citrix Studion konekataloginäkymä katalogin luonnin jälkeen.

6.7 Jakeluryhmän luonti

Seuraavaksi jakeluryhmä luotiin Citrix Studiossa. Luontiprosessi aloitettiin avaamalla toimitushallintapalvelimelta Citrix Studio -ohjelmisto, klikkaamalla oikealla hiiren painikkeella ”Delivery Groups” -kohtaa ja valitsemalla ”Create Delivery Group” -vaihtoehto. Tämä avasi apuohjelman, jolla jakeluryhmä luotiin. Ensimmäiseksi apuohjelma kysyi, mikä konekatalogi halutaan ottaa jakeluryhmän käyttöön ja tarjosi listan tarjolla olevista konekatalogeista. Koska konekatalogeja oli luotu vain yksi kappale, valittiin se. Seuraavaksi apuohjelma kysyi, tarjotaanko käyttäjille virtualisoituja työpöytiä, sovelluksia vai molempia. Kokeiluympäristön tarkoituksena oli tarjota käyttäjille vain virtualisoituja sovelluksia, joten sitä vastaava vaihtoehto valittiin. Seuraavaksi apuohjelmassa määriteltiin se, mille käyttäjille virtualisoituja sovelluksia tarjotaan. Painamalla ”Add”-painiketta apuohjelma avasi Active Directory -hakuikkunan, jolla pystyi hakemaan käyttäjiä ja käyttäjäryhmä. Kohderyhmäksi asetettiin ”ILKKATEST\Domain Users.” Seuraavassa näkymässä pystyttiin määrittelemään käyttäjille tarjottavat sovellukset. Kokeiluympäristön toimivuuden varmis-

tamiseksi käyttäjille julkaistiin kokeilusovelluksena Windowsin laskin-sovellus. Seuraavaksi apuohjelma antoi mahdollisuuden asettaa jakeluryhmälle tietty StoreFront-palvelu käytettäväksi. Koska StoreFrontia ei oltu vielä luotu, valittiin tässä vaiheessa ”Manually, using a StoreFront server address that I will provide later” -vaihtoehto. Lopuksi apuohjelma näytti yhteenvedon valituista asetuksista ja jakeluryhmälle syötettiin nimi TestVDA. Jakeluryhmän luomisen jälkeen luotu ryhmä ilmestyi Citrix Studion ”Delivery Groups” -näkymään (kuva 4).



Kuva 4. Citrix Studion jakeluryhmänäkymä ryhmän luonnin jälkeen.

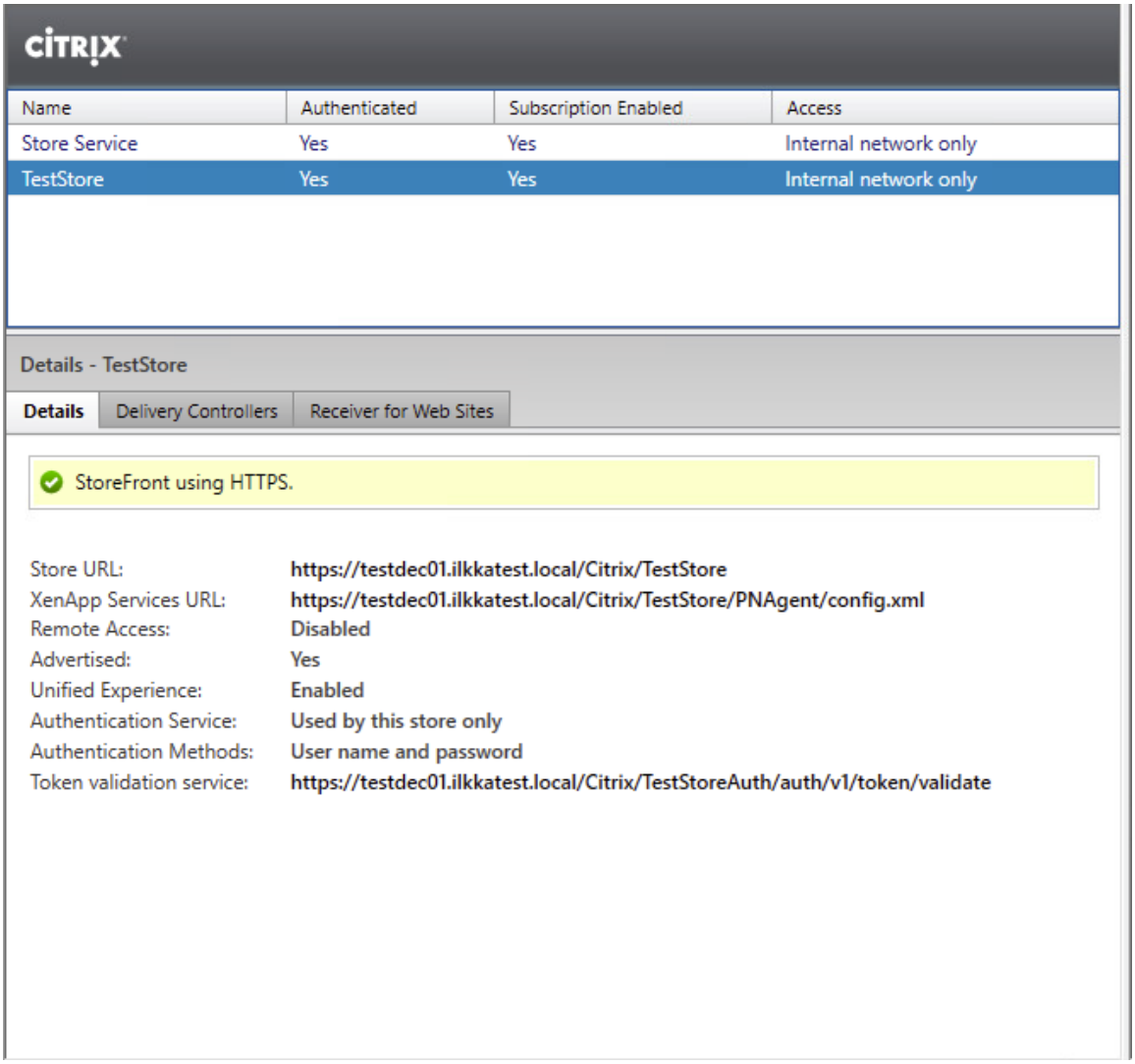
6.8 Store-palvelun luonti

Store-palvelun luontiprosessi aloitettiin navigoimalla Citrix Studion Citrix StoreFront-välilehdelle ja valitsemalla ”Create a Store” -vaihtoehto. Avautuvaan näkymään syötettiin ensiksi Store-palvelun nimi, jolle annettiin nimeksi TestStore. Seuraavalla sivulla asennusohjelma pyysi lisäämään halutut toimitushallintapalvelimet. Palvelimen lisäys aloitettiin painamalla ”Add”-painiketta ja avautuvaan ikkunaan syötettiin taulukon 6 mukaiset tiedot:

Näyttönimi	TestController
Tyyppi	XenApp (7.5 tai uudempi)
Palvelimet (kuormanjaossa)	testdec01.ilkkatest.local
Yhteystyyppi	HTTP
Portti	80

Taulukko 6. Store-palvelun toimitushallintapalvelinasetukset.

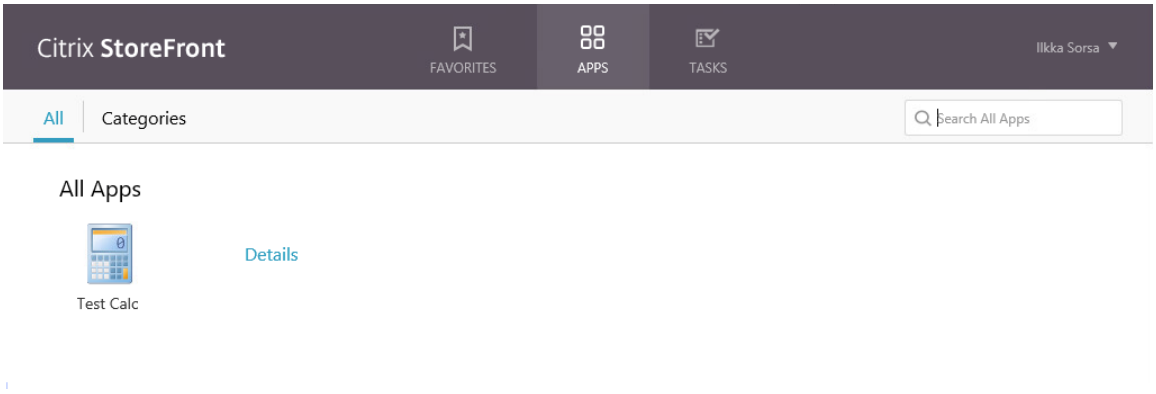
Seuraavalla sivulla apuohjelma pyysi määrittelemään, otetaanko etäyhteys käyttöön. Ominaisuus vaati Citrix NetScalerin lisäämistä kokeiluympäristöön, jota ei tässä käyttöönotossa oltu tehty. Näin ollen etäyhteyttä ei otettu käyttöön. Seuraavaksi apuohjelma kysyy, mitä todennustapoja palvelu käyttää. Tässä ympäristössä otettiin käyttöön käyttäjänimi ja salasana -todennustapa. Seuraavaksi apuohjelma kysyy, asetetaanko Store-palvelulle palveluosoite PNAgent-toiminnallisuutta varten. Tämä ominaisuus ei ollut oleellinen tässä käyttöönotossa, joten osoitetta ei asetettu. Lopuksi Store-palvelun luominen viimeisteltiin painamalla Create-painiketta. Store-palvelun luonnin jälkeen se ilmestyi Citrix Studio -ohjelman näkymään (kuva 5).



Kuva 5. Citrix Studion StoreFront-näkymä, jossa luotu Store-palvelu.

Seuraava osa Store-palvelun käyttöönottoa oli määrittää se jakeluryhmän käyttöön. Ensiksi Citrix Studion käyttöliittymässä navigoitiin ”Configuration”-välilehdelle ja kyseiseltä välilehdeltä ”StoreFront”-välilehdelle. Tällä välilehdellä valittiin ”Add StoreFront Server” -vaihtoehto, jolloin Studio avasi ikkunan, johon StoreFront-palvelimen tiedot syötettiin. Ikkunaan syötettiin StoreFront-palvelimen nimeksi ”TestStore” ja osoitteeksi http://testdec01.ilkkatest.local/Citrix/TestStoreWeb/. Seuraavaksi Citrix Studiossa navigoitiin ”Delivery Groups” -välilehdelle, josta aiemmin luotua jakeluryhmää klikattiin hiiren oikealla painikkeella ja valittiin ”Edit Delivery Group” -vaihtoehto. Avautuneessa ikkunassa navigoitiin StoreFront-välilehdelle, asetettiin valinta ”Automatically, using the StoreFront servers selected below” -valintaruutuun ja valittiin aiemmin luotu StoreFront-palvelin listalta. Lopuksi verkkoselaimella navigoitiin osoitteeseen http://testdec01.ilkkatest.local/Citrix/StoreWeb/,

joka avasi Citrix StoreFront -kirjautumissivun onnistuneesti. Palveluun kirjauduttiin toimialueen käyttäjätilillä onnistuneesti. Kuva 6 havainnollistaa sisään kirjautuneen käyttäjän näkymää.



Kuva 6. Citrix StoreFront-palvelun päänäkymä sisään kirjautuneella käyttäjällä.

6.9 Sertifikaattiauktoriteetin luonti

Käyttöönottoprosessissa luotiin toimiva Citrix XenApp -kokoonpano, mutta kyseinen kokoonpano toimi ainoastaan HTTP-protokollan kanssa. Kokoonpano haluttiin vaihtaa HTTPS-yhteensopivaksi, sillä Citrix SSPR -ratkaisu toimii ainoastaan silloin kun StoreFront on asetettu HTTPS-tilaan. Myös muut työssä arvioidut SSPR-ratkaisut vaativat SSL- tai LDAPS-sertifikaatin. Kokeiluympäristössä päätettiin luoda toimialueen hallintapalvelimesta sertifikaattiauktoriteetti ja käyttää sen itsensä allekirjoittamia sertifikaatteja.

Asennusprosessi aloitettiin avaamalla toimialueen hallintapalvelimelta ”Server Manager” -ohjelma ja valitsemalla siitä ”Add roles and features” -vaihtoehdon. Palvelimelle valittiin asennettavaksi ”Active Directory Certificate Services” -rooli. Kun apuohjelma kysyi, mitkä roolipalvelut asennetaan, valittiin ”Certification Authority” -palvelu. Lopuksi roolin asennusprosessi aloitettiin painamalla Install-nappia.

Roolin asennuksen jälkeen asennusohjelma pyysi vielä tietoja, joiden perusteella sertifikaattiauktoriteettipalvelu otettiin käyttöön. Ensiksi apuohjelmaan syötettiin toimialueen tunnus, jolla oli toimialueen laajuiset järjestelmänvalvojan oikeudet. Seuraavaksi valittiin konfiguroitavaksi palveluksi ”Certification Authority” -palvelu. Sertifikaattiauktoriteetin asennustyypiksi valittiin ”Enterprise CA.” Koska ympäristössä ei ole jo olemassa olevaa julkisen avaimen infrastruktuuria, valittiin sertifikaattiauktoriteetin tyypiksi ”Root CA.” Seu-

raavaksi asennusohjelma kysyi yksityisen avaimen luonnista. Koska olemassa olevaa yksityistä avainta ei ole, valittiin ”create a new private key” -vaihtoehto. Seuraavaksi asennusohjelma pyysi määrittelemään sertifikaattiauktoriteetin yksityisen avaimen kryptografia-asetukset. Kryptografiatoimittajaksi valittiin ”RSA#Microsoft Software Key Storage Provider,” avaimen pituudeksi 2048 bittiä ja tiivistefunktioksi SHA256. Seuraavaksi asennusohjelma pyysi syöttämään sertifikaattiauktoriteetin yleisen nimen ja luokitellun nimen päätteen, joka olivat taulukon 7 mukaiset.

Sertifikaattiauktoriteetin yleinen nimi	ilkkatest-TESTDC01-CA
Luokitellun nimen pääte	DC=ilkkatest,DC=local
Luokitellun nimen esikatselu	CN=ilkkatest-TESTDC01-CA,DC=ilkkatest,DC=local

Taulukko 7. testdc01.ilkkatest.local-sertifikaattiauktoriteetin nimiasetukset.

Seuraavaksi asennusohjelma pyysi määrittelemään sertifikaattiauktoriteetin luomien sertifikaattien voimassaoloajan. Asetus jätettiin oletusarvoon, joka tarkottaa sitä, että sertifikaattiauktoriteetin luomat sertifikaatit ovat voimassa viiden vuoden ajan. Seuraava askel prosessissa oli sertifikaattitietokannan ja sertifikaattilokitietokannan sijainnin määrittely. Kyseiset asetukset jätettiin oletusarvoihinsa. Viimeinen askel prosessissa oli tarkastaa yhteenvedossa esitetyt asetukset ja viimeistellä prosessi painamalla ”Configure”-painiketta. Sama prosessi toistettiin lopuksi myös toisella toimialueen hallintapalvelimella.

Seuraava osa sertifikaattiauktoriteetin käyttöönottoprosessia oli sertifikaattiauktoriteettien konekohtaisten sertifikaattien vienti tiedostoon ja niiden asentaminen sertifikaatteja vaativien palvelimien ”Trusted Root Certification Authorities” -säilöön. Prosessi aloitettiin avaamalla toimialueen hallintapalvelimella Microsoftin hallintakonsoli -ohjelma (*mmc.exe.*) Seuraavaksi hallintakonsoliin liitettiin sertifikaattien hallinta-apuohjelma, joka osoitettiin hallitsemaan paikallisen tietokoneen sertifikaatteja. Seuraavaksi apuohjelmassa navigoitiin ”Trusted Root Certification Authorities” -välilehdelle, klikattiin sertifikaattiauktoriteetin omaa sertifikaattia ja valittiin ”Export” -valinta. Sertifikaatin muodoksi valittiin DER-enkoodattu binäärimuoto X.509 ja sertifikaatti tallennettiin palvelimen kovalevylle CER -tiedostomuotoon.

Kyseinen tiedosto kopioitiin sitten toimitushallintapalvelimelle, jossa Microsoftin hallintakonsoli -ohjelma avattiin ja siihen lisättiin sertifikaatinhallinta-apuohjelma. Apuohjelman käyttöliittymässä navigoitiin palvelimen ”Trusted Root Certification Authorities” -säilöön ja

valittiin ”Import”-vaihtoehto. Avautuvaan ikkunaan syötettiin ladatun CER-tiedoston sijainti, tuotavaksi säilöksi valittiin ”Trusted Root Certification Authorities” -säilö ja tuonti viimeisteltiin painamalla ”Finish”-painiketta. Toimitushallintapalvelin oli tämän jälkeen valmis hyväksymään sertifikaattiauktoriteetin luomat sertifikaatit.

6.10 SSL-sertifikaatin luonti

Seuraava askel käyttöönottoprosessia oli luoda SSL-sertifikaatti toimitushallintapalvelimelle, jotta StoreFront-palvelu voitiin vaihtaa HTTPS-tilaan. Sertifikaattipyynnön luonti tapahtui avaamalla toimitushallintapalvelimella ”Internet Information Services (IIS) Manager” -ohjelma. IIS Manager -ohjelman käyttöliittymästä valittiin itse toimitushallintapalvelin ja sitten ”Server Certificates” -vaihtoehto. Avautuvasta näkymästä valittiin ”Create Certificate Request…” -valinta joka avasi ikkunan, johon taulukon 8 sisältämät sertifikaattipyynnön tiedot syötettiin.

Yleinen nimi	testdec01.ilkkatest.local
Organisaatio	Ilkka
Organisaatioyksikkö	IT
Kaupunki	Oulu
Alue	Oulu
Maa	FI

Taulukko 8. testdec01.ilkkatest.local -palvelimen sertifikaattipyynnön tiedot.

Seuraavalla sivulla pyydettiin kryptografiapalvelun toimittajan ja avaimen pituuden tiedot. Kryptografiapalvelun toimittajaksi syötettiin ”Microsoft RSA SChannel Cryptographic Provider” ja avaimen pituudeksi 2048 bittiä. Lopuksi sertifikaattipyyntö tallennettiin tekstitiedostona palvelimen kovalevylle. Tekstitiedosto avattiin ja sen sisältö kopioitiin leikepöydälle. Seuraavaksi verkkoselaimeen syötettiin osoite https://10.0.0.102/certsrv/, joka on ensisijaisen toimialueen ohjauspalvelimen sertifikaattipalvelun osoite.

Sertifikaattipalvelusta valittiin ”Request a certificate” -vaihtoehto, seuraavasta näkymästä ”advanced certificate request” -vaihtoehto ja lopulta ”Submit a certificate request using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-

64-encoded PKCS #7 file.” Avautuvaan lomakkeeseen syötettiin “Saved Request” -kohtaan tekstitiedostosta kopioitu teksti, “Certificate Template” -kohtaan vaihtoehto ”Web Server” ja ”Attributes” -kohta jätettiin tyhjäksi. Lopuksi painettiin Submit-painiketta. Lopuksi valmis sertifikaatti ladattiin palvelusta DER-enkoodatussa muodossa.

Seuraavaksi IIS Manager -ohjelman ”Server Certificates” -näkymästä valittiin vaihtoehto ”Complete Certificate Request…” Avautuvaan ikkunaan syötettiin ladatun sertifikaattitiedoston sijainti, annettiin sille nimeksi TESTDEC01 ja tallennettiin se palvelimen henkilökohtaiseen sertifikaattisäilöön.

6.11 Citrix Self-Service Password Reset -ratkaisun käyttöönotto

Ensimmäinen tässä opinnäytetyössä kokeiltu ratkaisu oli Citrix Self-Service Password Reset -ratkaisu. Ratkaisun käyttöönotto aloitettiin luomalla Windows Server 2016 -virtuaalikone, jolle asetettiin neljä gigatavua keskusmuistia, yksi prosessoriydin ja 40 gigatavua kovalevytilaa. Citrix ei ole asettanut SSPR-ratkaisulle järjestelmän suorituskyvyn minimivaatimuksia [38]. Käyttöjärjestelmän asennuksen jälkeen virtuaalikone nimettiin uudelleen, sille annettiin staattinen IP-osoite ja se liitettiin toimialueeseen. Virtuaalikoneen verkkoasetukset on lueteltu taulukossa 9.

	testsspr.ilkkatest.local
IP-osoite	10.0.0.106
Aliverkon peite	255.255.255.0
Oletusyhdyskäytävä	10.0.0.1
Ensisijaisen nimipalvelimen osoite	10.0.0.102
Toissijaisen nimipalvelimen osoite	10.0.0.103

Taulukko 9. Citrix SSPR-palvelimen verkkoasetukset.

Seuraavaksi toimialueelle luotiin kaksi käyttäjätiliä Citrix SSPR-ratkaisua varten. Ensimmäinen käyttäjätili, datanvälittäjätili, oli normaali toimialueen käyttäjätili, jolle myöhemmin delegoitiin keskussäilön luonnin yhteydessä käyttäjäoikeuksia. Toinen käyttäjätili oli SSPR-palvelun itsepalvelutili, joka myös oli normaali toimialueen käyttäjätili. Itsepalvelutilin luonnin jälkeen ”Active Directory Users and Computers” -ohjelmasta klikattiin oikealla

hiiren painikkeella toimialueen nimeä ja valittiin ”Delegate Control” -vaihtoehto. Avautuvasta apuohjelmasta itsepalvelutilille delegoitiin seuraavat käyttöoikeudet:

- Read lockoutTime
- Write lockoutTime
- Reset password
- Change password
- Read userAccountControl
- Write userAccountControl
- Read pwdLastSet
- Write pwdLastSet

Näillä käyttöoikeuksilla itsepalvelutilillä oli oikeudet vaihtaa normaalien käyttäjätunnusten salasanoja, mutta ei esimerkiksi toimialueen järjestelmänvalvojien salasanoja.

Seuraava askel SSPR-palvelun käyttöönotossa oli keskussäilön luonti. Keskussäilö on osa SSPR-palvelua, johon SSPR tallentaa erinäisiä käyttämiänsä tietoja, kuten käyttäjien salasananpalautuksessa käytettävät kysymykset ja vastaukset. Keskussäilö päätettiin luoda tässä ympäristössä käyttäen Windowsin omaa SMB-jakoa.

Keskussäilön luonti aloitettiin asentamalla SSPR-palvelimelle ”File Server” -rooli, joka onnistui ”Server Manager” -ohjelman ”Add Roles and Features” -toiminnon avulla. Roolin asentamisen jälkeen ”Server Manager” -ohjelmasta klikattiin ”File and Storage Services” -vaihtoehtoa. Avautuvasta näkymästä navigoitiin ”Shares”-välilehdelle, josta valittiin ”Tasks” ja ”New Share…” -vaihtoehdot. Avautuvasta ikkunasta valittiin ”SMB Share - Quick” -vaihtoehto. Seuraavalla sivulla valittiin tehtävän jaon sijainniksi C-asema ja juuripoluksi C:\Shares. Seuraavassa näkymässä apuohjelma kysyi luotavan SMB-jaon nimeä sekä polkua. Luotavalle SMB-jaolle annettiin nimeksi CITRIXSYNC$ ja jaon poluiksi muodoistuivat seuraavat:

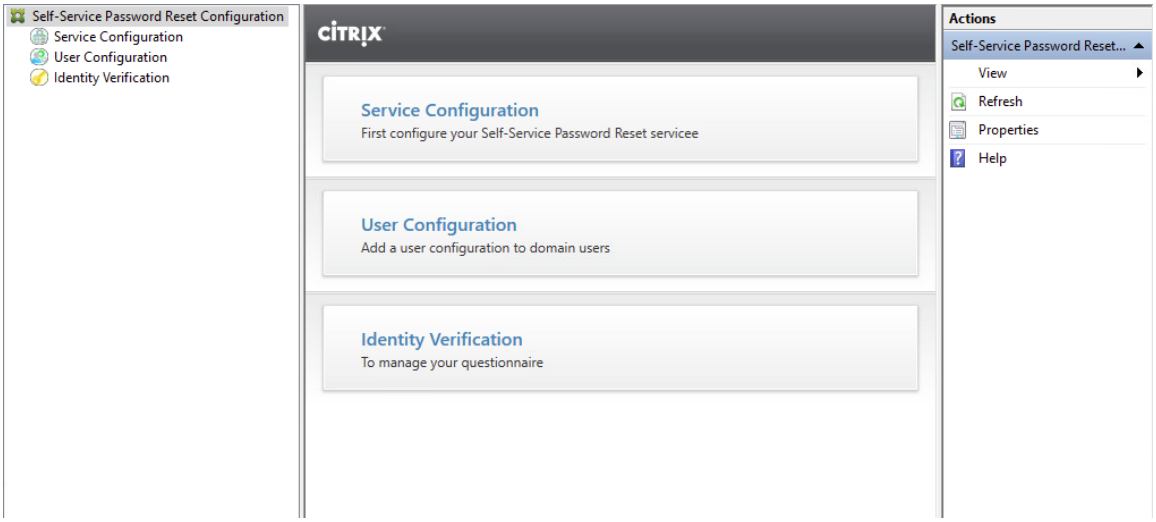
- Paikallinen polku: C:\Shares\CITRIXSYNC$
- Etäpolku: \\TestSSPR\CITRIXSYNC$

Seuraavalla sivulla apuohjelma antoi määritellä SMB-jaon lisäasetukset. ”Allow caching of share” -vaihtoehdosta otettiin valinta pois ja valittiin ”Encrypt data access” -vaihtoehto. Seuraavalla sivulla apuohjelma antoi mahdollisuuden muuttaa SMB-jaon käyttöoikeuksia. Tämä onnistui painamalla ”Customize permissions…” -painiketta. Avautuva ikkuna sisälsi SMB-jaon nykyiset käyttöoikeudet, joista ensiksi otettiin periytyminen poissa valitsemalla ”Disable inheritance” ja ”Convert inherited permissions into explicit permissions on this object” -vaihtoehdot. Tämän jälkeen SMB-jaosta poistettiin kaikki muut käyttöoikeudet paitsi ”CREATOR OWNER”, ”Local Administrators” ja ”SYSTEM”. Tämän jälkeen SMB-jakoon lisättiin aiemmin luotu datanvälittäjätili, jolle annettiin jakoon ”Full Control” -oikeudet. Lopuksi ”CREATOR OWNER” -käyttäjän oikeuksia vähennettiin ottamalla ”Full Control”, ”Delete subfolders and files”, “Change permissions” ja “Take ownership” -oikeudet pois. Tämän jälkeen navigoitiin ”Share”-välilehdelle, jossa datanvälittäjätilille, paikallisille järjestelmänvalvojille ja toimialueen järjestelmänvalvojille annettiin pääsy luotavaan jakoon ”Full Control” -oikeuksilla. Lopuksi viimeinen sivu näytti yhteenvedon valituista asetuksista ja SMB-jako luotiin painamalla ”Create” -painiketta. Keskussäilön luonti viimeisteltiin navigoimalla luotuun kansioon ja tekemällä kaksi kansiota: CentralStoreRoot ja People. Keskussäilö oli luotu onnistuneesti.

Keskussäilön luonnin jälkeen seuraavana oli vuorossa itse Citrix SSPR-ratkaisun asentaminen. Citrix SSPR-ratkaisun asennusprosessi aloitettiin asettamalla SSPR-palvelimelle Citrix XenApp 7.15 LTSR -ohjelmiston asennusohjelman sisältävä ISO-tiedosto. Asennusohjelma avattiin ja avautuvasta valikosta valittiin ”Self-Service Password Reset” -vaihtoehto. Avautuvasta asennusohjelmasta hyväksyttiin lisenssisopimus, valittiin SSPR-komponentti asennettavaksi ja annettiin asennusohjelman avata Windowsin palomuurista TCP-portti 443. Lopuksi asennusohjelma näytti yhteenvedon valituista asetuksista ja asennus aloitettiin valitsemalla Install-vaihtoehto.

Seuraava askel SSPR-palvelun käyttöönotossa oli SSL-sertifikaatin luonti ja asennus palvelimelle. Prosessi tapahtui samalla periaatteella kuin toimitushallintapalvelimen sertifikaatin luonti, joten sertifikaatin luontiprosessin kulkua ei tässä kappaleessa toisteta.

Seuraavaksi määriteltiin Citrix SSPR-ratkaisun asetukset avaamalla ”Citrix Self-Serivce Password Reset Configuration” -ohjelma, jonka päävalikon näkymää kuva 7 havainnollistaa.



Kuva 7. Citrix Self-Service Password Reset Configuration -ohjelman päävalikko.

Asetusten määrittäminen aloitettiin valitsemalla ”Service Configuration” -välilehti ja välilehdeltä ”New Service Configuration” -vaihtoehto. Avautuva apuohjelma kysyi keskussäilön sijaintia, johon syötettiin arvoksi \\TESTSSPR.ilkkatest.local\CITRIXSYNC$. Seuraavalla välilehdellä apuohjelma kysyi, mitä toimialueita kyseinen SSPR-ratkaisu tulee hallitsemaan. Toimialueeksi asetettiin ilkkatest.local ja painettiin Properties-painiketta. Avautuvaan ikkunaan syötettiin luodun datanvälittäjätilin sekä itsepalvelutilin kirjautumistiedot ja painettiin OK. Seuraavalla sivulla viimeisteltiin asetusten määrittäminen valitsemalla Finish-vaihtoehto ja apuohjelma loi SSPR-ratkaisun määritellyillä asetuksilla.

Seuraava askel SSPR-ratkaisun käyttöönotossa oli määritellä, mitä kohderyhmiä SSPR-ratkaisu palvelee. Kohderyhmä oli mahdollista määritellä käyttäjätasolla, käyttäjäryhmätasolla ja hallintoyksikkötasolla. Käyttäjien ja kohderyhmien määrittely aloitettiin navigoimalla ”Citrix Self-Service Password Reset Configuration” -ohjelman ”User Configuration” -välilehdelle ja valitsemalla ”New User Configuration” -vaihtoehto. Avautuvassa ikkunassa oli kaksi kenttää: ”User LDAP path” ja ”Active Directory Group”. Ensimmäiseen kenttään syötettiin seuraavat LDAP-polut:

- LDAP://ilkkatest.local/CN=Users,DC=ilkkatest,DC=local
- LDAP://ilkkatest.local/OU=SSPR,DC=ilkkatest,DC=local

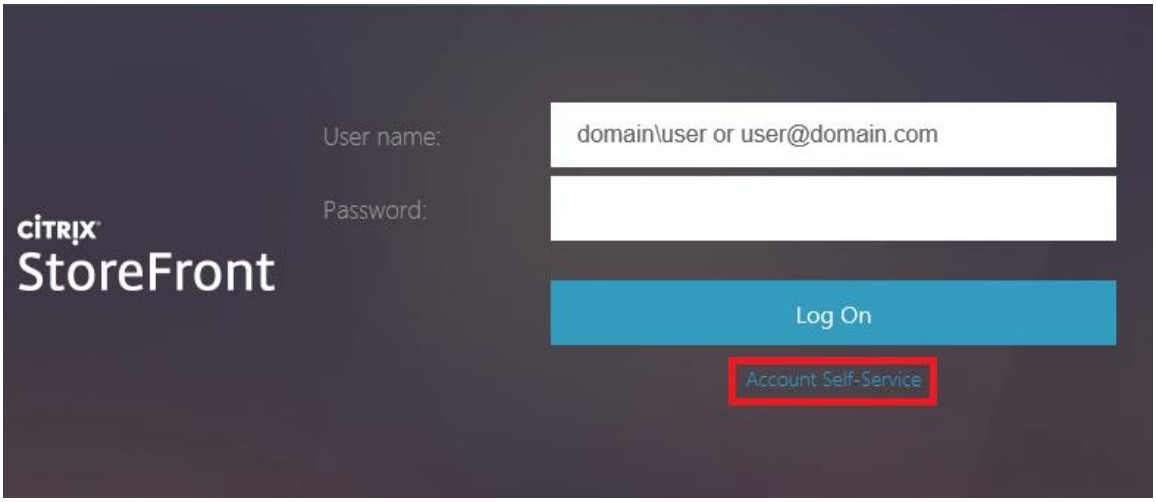
Toiseen kenttään syötettiin SSPR-ratkaisun palvelemaksi käyttäjäryhmäksi ”ILKKATEST\Domain Users”. Nämä asetukset takasivat sen, että SSPR-ratkaisu oli käytössä kaikilla toimialueen käyttäjätileillä, jotka sijaitsivat Active Directoryn Users-säilössä tai SSPR-organisaatioyksikössä. Seuraavalla sivulla apuohjelma kysyi lisenssipalvelimen

osoitetta, johon syötettiin arvoksi testdec01.ilkkatest.local ja portiksi valittiin oletusarvo. Viimeisellä sivulla apuohjelma kysyi, mitä Citrix SSPR-ratkaisun ominaisuuksista otetaan käyttöön. Sekä käyttäjätilien palautus että salasanojen vaihto otettiin käyttöön. Viimeinen kenttä pyysi määrittelemään palvelun osoitteen, jolle annettiin arvoksi https://testsspr.ilkkatest.local/MPMService ja portiksi 443. Lopuksi käyttöönotto viimeisteltiin painamalla Create-painiketta.

Viimeinen askel Citrix SSPR-palvelun käyttöönotossa oli ottaa SSPR käyttöön StoreFront-palvelussa. Ensin käyttöön otettu StoreFront-palvelu täytyi vaihtaa HTTPS-tilaan, sillä SSPR-palvelu tukee ainoastaan HTTPS-tilassa olevia StoreFront-palveluita. Tämä tapahtui avaamalla toimitushallintapalvelimelta ”Citrix Studio” -ohjelma, josta mentiin ”StoreFront” ja ”Server Group” -välilehdille. Kyseiseltä välilehdeltä valittiin ”Change Base URL” -vaihtoehto ja StoreFrontin uudeksi osoitteeksi asetettiin https://testdec01.ilkkatest.local/. Kyseisen toimenpiteen jälkeen StoreFront-palvelu oli HTTPS-tilassa.

Seuraavaksi Citrix Studiossa navigoitiin ”StoreFront” ja ”Stores” -välilehdille, jossa aiemmin luotua Store-palvelua klikattiin hiiren oikealla painikkeella ja valittiin ”Manage Authentication Methods” -vaihtoehto. Avautuvasta ikkunasta valittiin ”User name and password” -vaihtoehto, jonka jälkeen valinnan oikealla puolella olevaa hammasratasikonia klikattiin ja avautuvasta valikosta valittiin ”Manage Password Options” -vaihtoehto. Avautuneeseen ikkunaan asetettiin valinta ”Allow users to change passwords” -valinnan valintaruutuun sekä ”At any time” -valintaruutuun. Valinnat hyväksyttiin painamalla OK-painiketta sekä avautuneesta ikkunasta että ”Manage Authentication Methods” -ikkunasta. Näin käyttäjät pystyivät vaihtamaan Active Directory -käyttäjätiliensä salasanan Citrix Receiverin verkkokäyttöliittymän kautta.

Seuraavaksi ”Manage Authentication Methods” -ikkuna avattiin uudelleen, hammasratasikonia klikattiin uudelleen ja valittiin ”Configure Account Self-Service” -vaihtoehto. Avautuvaan ikkunaan asetettiin ”Citrix SSPR” arvoksi ja klikattiin Configure-painiketta. Avautuneeseen ikkunaan asetettiin valinta sekä ”Enable password reset” että ”Allow account unlock” -valintaruutuihin ja ”SSPR Account Service URL” -kohtaan asetettiin arvoksi https://testsspr.ilkkatest.local/MPMService. Valinnat viimeisteltiin painamalla OK-painiketta kaikkiin kolmeen avattuun ikkunaan. Citrix SSPR-palvelu oli valmis käytettäväksi. Citrix SSPR-palvelun käyttöönoton jälkeen Citrix StoreFront-palvelun kirjautumisnäkymään ilmestyi ”Account Self-Service” -vaihtoehto, jonka avulla käyttäjä pystyi palauttamaan salasanansa sekä poistamaan lukitusta käyttäjätilistään lukituksen. Kuva 8 havainnollistaa tätä muutosta.



Kuva 8. Citrix StoreFront -kirjautumisnäkymä. Account Self-Service -vaihtoehto korostettuna.

Käyttöönoton jälkeen kirjautunut käyttäjä näki Receiver-näkymässään uuden Tasks-välilehden. Kyseiseltä välilehdeltä käyttäjä pystyi vastaamaan järjestelmänvalvojan asettamiin turvakysymyksiin. Turvakysymyksiin vastattuaan käyttäjä pystyi valitsemaan ”Account Self-Service” -vaihtoehdon StoreFrontin kirjautumisnäkymästä ja vaihtamaan unohtuneen salasanan vastaamalla oikein turvakysymyksiin. Järjestelmänvalvoja pystyi muuttamaan turvakysymyksiä ”Citrix Self-Service Password Reset Configuration” -ohjelman ”Identity Verification” -välilehdeltä.

6.12 SQL-palvelimen luonti

Seuraava tässä työssä kokeiltu ratkaisu, PWM, vaati tietojen tallennusta varten tietokannan. Ennen kyseisen palvelun käyttöönottoa kyseistä palvelua varten luotiin SQL-palvelin. SQL-palvelimelle annettiin neljä gigatavua keskusmuistia, yksi prosessoriydin sekä 40 gigatavua kovalevytilaa. Käyttöjärjestelmän asennuksen jälkeen virtuaalikone nimettiin uudelleen, sille annettiin staattinen IP-osoite ja se liitettiin toimialueeseen. Taulukko 9 havainnollistaa virtuaalikoneen verkkoasetuksia.

	testsql.ilkkatest.local
IP-osoite	10.0.0.105
Aliverkon peite	255.255.255.0
Oletusyhdyskäytävä	10.0.0.1
Ensisijaisen nimipalvelimen osoite	10.0.0.102
Toissijaisen nimipalvelimen osoite	10.0.0.103

Taulukko 9. SQL-palvelimen verkkoasetukset.

Seuraavaksi palvelimelle asennettiin ”Microsoft SQL Server 2017 Express” -ohjelmisto. Ohjelmisto asennettiin palvelimelle käyttäen oletusasetuksia, lukuun ottamatta instanssin nimeä, jolle annettiin nimeksi TESTPWM. Ohjelmiston asennuksen jälkeen palvelimelle ladattiin ja asennettiin ”SQL Server Management Studio 17.6” -ohjelma. Asennuksen jälkeen SQL-palvelimelle kirjauduttiin sisään kyseisellä ohjelmalla ja luotiin tietokanta nimellä PWM. Seuraavaksi avattiin Windowsin palveluidenhallintaohjelma (*services.msc*), josta etsittiin ”SQL Server Browser” -palvelu, joka otettiin käyttöön ja asetettiin käynnistymään automaattisesti. Lopuksi avattiin ”SQL Server Configuration Manager” -ohjelma, josta navigoitiin ”SQL Server Network Configuration” -välilehdelle ja seuraavaksi ”Protocols for TESTPWM” -välilehdelle. Välilehdellä klikattiin hiiren oikealla painikkeella ”TCP/IP”-valintaa ja otettiin se käyttöön. Lopuksi SQL-palvelin käynnistettiin uudelleen.

6.13 PWM-palvelun käyttöönotto

PWM-ratkaisun käyttöönotto aloitettiin luomalla Windows Server 2016 -virtuaalikone, jolle asetettiin neljä gigatavua keskusmuistia, yksi prosessoriydin ja 40 gigatavua kovalevytilaa. Käyttöjärjestelmän asennuksen jälkeen virtuaalikone nimettiin uudelleen, sille annettiin staattinen IP-osoite ja se liitettiin toimialueeseen. Taulukko 10 havainnollistaa virtuaalikoneen verkkoasetuksia.

	testpwm.ilkkatest.local
IP-osoite	10.0.0.108
Aliverkon peite	255.255.255.0
Oletusyhdyskäytävä	10.0.0.1
Ensisijaisen nimipalvelimen osoite	10.0.0.102
Toissijaisen nimipalvelimen osoite	10.0.0.103

Taulukko 10. PWM-palvelimen verkkoasetukset.

Tämän jälkeen Windowsin palomuurista avattiin TCP-portti 80 PWM-käyttöönottoa varten. Palvelimelle luotiin myös SSL-sertifikaatti samalla periaatteella kuin toimitushallintapalvelimelle aiemmin tämän työn aikana. Toimialueelle luotiin myös PWM-itsepalvelutili samalla periaatteella ja asetuksilla kuin Citrix SSPR-palvelua varten luotu käyttäjätili. Active Directoryyn luotiin myös PWM:ää varten käyttäjäryhmä, jolle annettiin nimi ”PWM Admins”. Käyttäjäryhmälle delegoitiin ”Read all user information” -oikeus ja kyseiseen ryhmään lisättiin PWM-itsepalvelutili sekä toimialueen ”Domain Admins” -ryhmä. PWM:ää varten luotiin myös testikäyttäjä nimeltä pwmtest, joka on normaali toimialueen käyttäjätili. PWM kokeilee säännöllisin väliajoin toimenpiteitä kyseitä käyttäjätiliä kohtaan varmistaakseen oman toiminnallisuutensa. Testikäyttäjä ei ole pakollinen, mutta se otettiin tässä kokoonpanossa käyttöön.

PWM:n asennusprosessi alkoi PWM:n vaatimien ohjelmien asennuksella. Ensimmäinen ohjelma oli Oraclen kehittämä ”Java SE Runtime Environment 8” -ohjelma. Ohjelmasta ladattiin 64-bittinen 8u172-versio. Kyseinen ohjelma asennettiin oletusarvoilla. Seuraava askel asennusprosessissa oli Apache Software Foundationin kehittämän Tomcat-ohjelman lataus ja asennus. Ohjelmasta ladattiin 64-bittinen 8.0.33-versio. Kyseinen ohjelma asennettiin myös oletusarvoilla ja asennuksen jälkeen Windowsin palomuurista avattiin TCP-portit 8005, 8080 ja 8009. Lopuksi Windowsista avattiin palveluidenhallintaohjelma (*services.msc*), jossa Tomcatin palvelu asetettiin käynnistymään automaattisesti.

Seuraavaksi PWM:n verkkosivuilta ladattiin kyseisen ohjelman 1.8.0-versio, joka oli pakattuna WAR-muotoiseen arkistoon. Arkiston tiedostopääte uudelleenimettiin WAR-päätteestä JAR-päätteeseen, jolloin WinRAR-ohjelma kykeni purkamaan sen ongelmitta. Purettu arkisto kopioitiin Tomcatin webapps-kansioon, joka tässä kokoonpanossa sijaitsi polussa C:\Program Files\Apache Software Foundation\Tomcat 8.0\webapps. Tiedostojen

kopioinnin jälkeen navigoitiin polkuun C:\Program Files\Apache Software Foundation\Tomcat 8.0\webapps\pwm\WEB-INF ja muokattiin ”web.xml”-tiedostoa lisäten seuraavat linjat:

```
<param-name>applicationPath</param-name>
<param-value>webapps\pwm\WEB-INF</param-value>
```

Seuraavaksi Javalle tuli tuoda toimialueen ohjauspalvelimien sertifikaatit. Java käyttää erillistä sertifikaattitietokantaa kuin Windows, joten vaikka ohjauspalvelimien sertifikaatit asennettiin palvelimelle SSL-sertifikaatin luonnin yhteydessä, tämä askel tuli silti tehdä. Toimialueen ohjauspalvelimien sertifikaatit tuotiin Javan ”keytool”-apuohjelmalla Javan sertifikaattitietokantaan.

Seuraava osa PWM-palvelun käyttöönottoprosessia oli asetusten konfigurointi. Tämä tapahtui avaamalla nettiselain ja menemällä osoitteeseen http://localhost:8080/pwm/config/ConfigManager. Avautuvasta näkymästä valittiin ”Start Configuration Guide” -vaihtoehto. Ensimmäiseksi valittiin, haluttiinko anonyymejä käyttäjätietoja lähettää PWM:n kehittäjille. Koska kyseinen kokoonpano oli kokeiluympäristö, kyseinen vaihtoehto voitiin sallia. Seuraavaksi apuohjelma kysyi, mitä LDAP-pohjaa käytetään. Tähän kohtaan asetettiin arvoksi ”Microsoft Active Directory”. Seuraavaksi apuohjelmaan syötettiin LDAP-palvelimen tiedot, jotka olivat seuraavat:

- LDAP-palvelimen osoite: testdc01.ilkkatest.local
- Portti: 636
- TLS: Käytössä

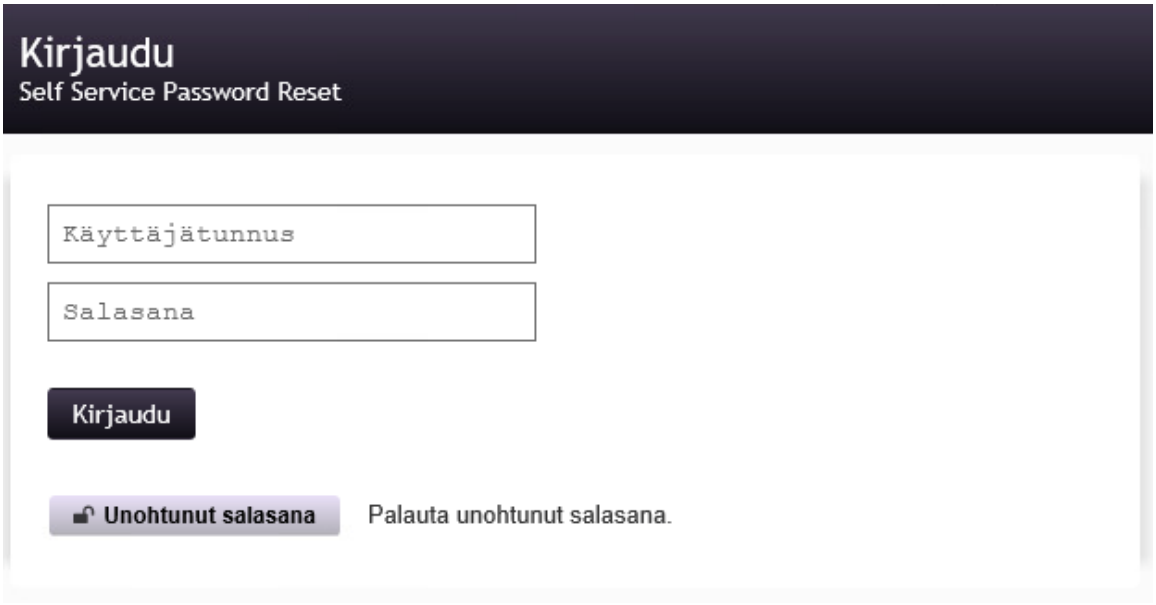
Asennusohjelmasta valittiin sertifikaatinhallintatavaksi ”use application to manage certificates and import certificates”. Seuraavaksi asennusohjelma pyysi syöttämään PWM-itsepalvelutilin sijainnin ja salasanan, käyttäjäsäilön sijainnin ja järjestelmänvalvojaryhmän sijainnin. Seuraavat arvot syötettiin:

- PWM-itsepalvelutilin sijainti: CN=PWM Proxy User,OU=PWM,DC=ilkkatest,DC=local
- Käyttäjäsäilön sijainti: DC=ilkkatest,DC=local
- Järjestelmänvalvojaryhmän sijainti:CN=PWM Admins,OU=PWM,DC=ilkkatest,DC=local

Seuraavaksi asennusohjelma kysyi, mihin PWM:n käyttämä data tallennetaan. Asennusohjelmassa oli kolme vaihtoehtoa: tallentaminen LDAP:iin, tallentaminen ulkoiseen tietokantaan ja tallentaminen paikalliseen tietokantaan. Paikalliseen tietokantaan tallentamista ei suositeltu, joten tallennuspaikaksi valittiin ulkoinen tietokanta eli aiemmin tässä työssä luodun SQL-palvelimen tietokanta. Koska PWM on Java-pohjainen sovellus, tietokantaan yhdistäminen tapahtuu Java Database Connectivity (JDBC) -ohjelmointirajapinnan kautta. Tätä ominaisuutta varten Microsoftin sivuilta ladattiin JDBC-ajurin versio 4.2. Ajuri ladattiin .TAR.GZ-muodossa ja purettiin PWM-palvelimen työpöydälle. Puretusta kansiorakenteesta navigoitiin sqljdbc_4.2.8112.200_enu/sqljdbc_4.2/enu/jre8 -kansioon, josta valittiin sqljdbc42.jar tiedosto käytettäväksi JDBC-ajuriksi PWM:n tietokantayhteyteen. Sen jälkeen tietokantayhteysasetuksiin määriteltiin seuraavat asetukset:

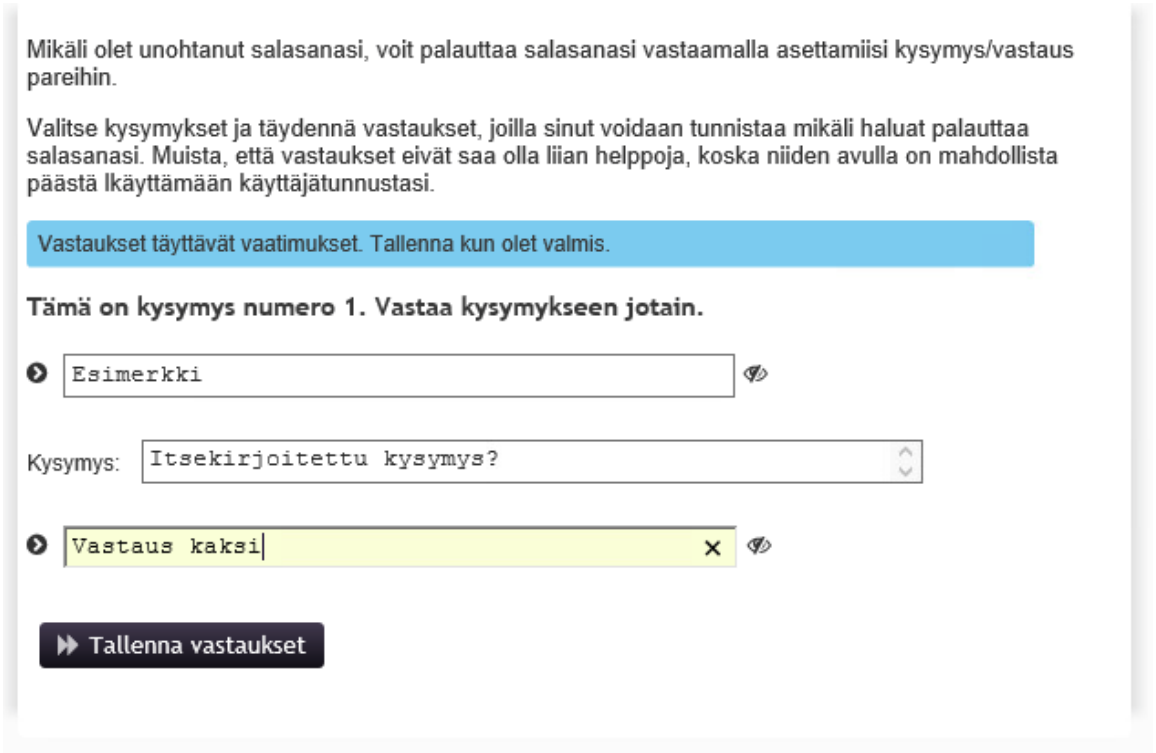
- Database class: com.microsoft.sqlserver.jdbc.SQLServerDriver
- Database connection string: jdbc:sqlserver://testsql.ilkkatest.local;instanceName=testpwm;databaseName=PWM
- Vendor: Other

Kyseiselle sivulle syötettiin myös tietokantakirjautumiseen käytettävän käyttäjätilin käyttäjätunnus ja salasana. Seuraavaksi asennusohjelma pyysi mahdollisen testikäyttäjän tietoja. Koska kyseinen käyttäjä luotiin aiemmin, otettiin kyseinen ominaisuus käyttöön ja syötettiin seuraavat sijaintitiedot: CN=PWM Test,OU=PWM,DC=ilkkatest,DC=local. Seuraavaksi asennusohjelma pyysi määrittelemään salasananpalautuskysymykset. PWM:ssä on jo valmiiksi usealle kielelle käännettyjä kysymyksiä, mutta kokeilun vuoksi ne poistettiin ja kirjoitettiin suomenkieliset palautuskysymykset. Yhteen kysymyksistä asetettiin arvoksi [user defined], joka tarkoittaa sitä, että käyttäjä itse keksii turvakysymyksen. Lopuksi asennusohjelma pyysi määrittelemään PWM-palvelun sivun verkko-osoitteen. Tähän asetettiin arvoksi http://testpwm.ilkkatest.local:8080/pwm. Lopuksi asennusohjelma näytti yhteenvedon valituista asetuksista, jotka otettiin käyttöön painamalla ”Save Configuration” -painiketta. PWM-palvelu oli nyt onnistuneesti otettu käyttöön. Kuva 9 havainnollistaa PWM-palvelun kirjautumisnäkymää.



Kuva 9. PWM-palvelun kirjautumisnäkymä oletusteemalla.

Käyttäjä pystyi kirjautumaan toimialueen tunnuksillaan sisälle PWM-palveluun. Ensimmäisellä sisäänkirjautumiskerralla PWM pyysi käyttäjää määrittelemään turvakysymyksiinsä vastaukset. Kuva 10 havainnollistaa käyttäjän näkemää näkymää.



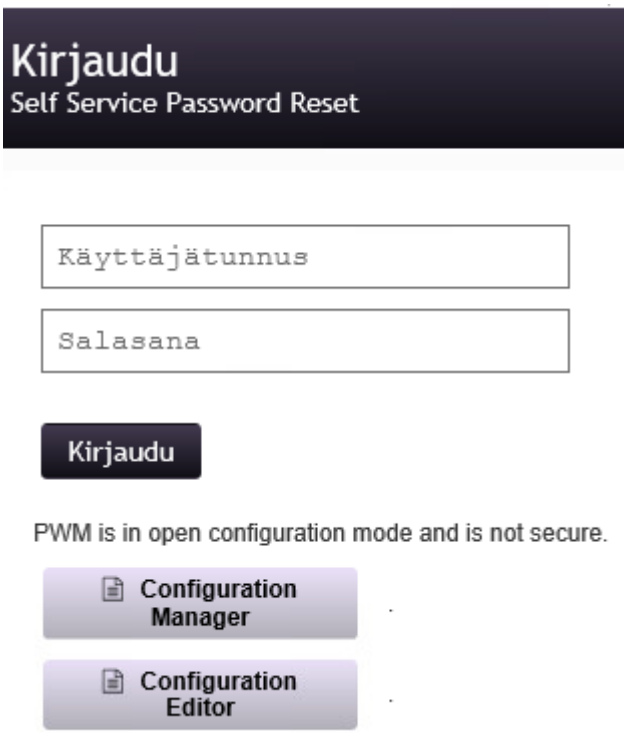
Kuva 10. PWM-palvelun turvakysymysten määritys. Vastaukset näkyvillä selvyyden vuoksi.

Unohtunut salasana voitiin vaihtaa valitsemalla PWM-palvelun kirjautumisruudusta ”Unohtunut salasana” -vaihtoehto. Seuraavaksi ohjelma pyysi käyttäjän käyttäjätunnusta, jonka jälkeen ohjelma esitti käyttäjälle hänen määrittelemänsä turvakysymykset. Kysymyksiin oikeiden vastauksien syöttämisen jälkeen ohjelma antoi mahdollisuuden vaihtaa unohtunut salasana uuteen.

PWM-palvelu voitiin asettaa konfiguraatiotilaan navigoimalla PWM:n WEB-INF-kansioon ja muuttamalla PwmConfiguration.xml-tiedostoa. Tiedostosta seuraavan linjan totuusarvoa muuttamalla oli mahdollista asettaa PWM-palvelu konfiguraatiotilaan:

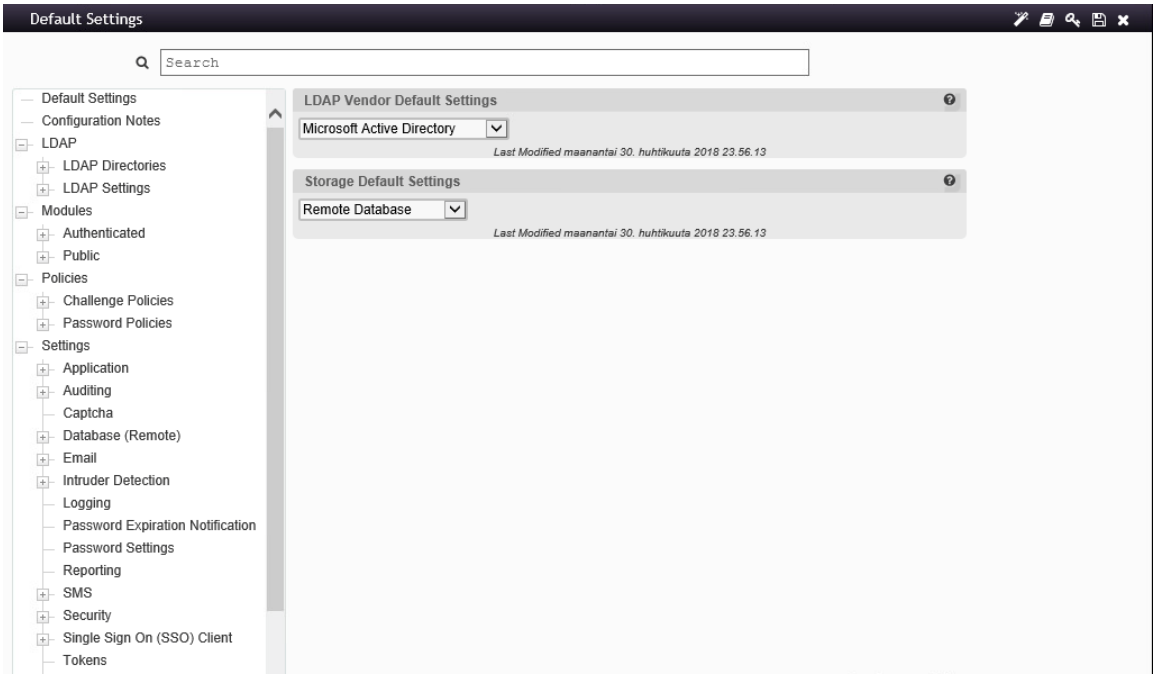
<property key=”configIsEditable” modifyTime=”muutosaika”>*false*</property>

Muuttamalla kyseisen totuusarvon *true*-arvoon PWM otti käyttöön konfiguraatiotilan ja palvelun kirjautumisnäkymä muuttui erilaiseksi. Muuttunut kirjautumisnäkymä on havainnollistettu kuvassa 11.



Kuva 11. PWM-palvelun kirjautumisnäkymä konfiguraatiotilassa.

Painamalla ”Configuration Manager” tai ”Configuration Editor” -painikkeita sivu pyysi asentamisvaiheessa määritellyn salasanan, jonka jälkeen PWM:n asetuksia pystyi tarkastelemaan ja muuttamaan. PWM-palvelun konfiguraatiotilan näkymä on esitelty kuvassa 12.



Kuva 12. PWM-palvelun Configuration Editor -näkymä.

PWM-palvelu voitiin muuttaa turvakysymys-vastauspari -autentikaatiotilasta muihin autentikaatiotiloihin navigoimalla Modules-valikosta Public-valikkoon, josta valittiin Forgotten Password -vaihtoehto, sitten Profiles-vaihtoehto, Sitten Default-vaihtoehto ja lopulta Definition-vaihtoehto. Avautuvalta sivulta valittiin Verification Methods -vaihtoehto. Kyseisestä asetusruudusta asetettiin Challenge/Response answers -vaihtoehto Not Used -tilaan ja LDAP Attributes -vaihtoehto Required-tilaan. Seuraavaksi Required LDAP Attributes -kohtaan lisättiin LDAP-attribuutti telephoneNumber. Nämä asetukset varmistivat sen, että salasananpalautusprosessi pyysi käyttäjälle Active Directoryssä asetettua puhelinnumeroa. Puhelinnumeron syöttämisen jälkeen salasananpalautusprosessi tarjosi saman salasananvaihtomahdollisuuden kuin turvakysymys-vastausparin syöttämisen jälkeen aiemmin. Kyseiseltä sivulta oli myös mahdollista asettaa PWM-palvelun käyttämäksi autentikaatiotavaksi muun muassa kaksitahoinen autentikaatio, SMS-autentikaatio ja sähköpostiautentikaatio.

Asetusten muuttamisen jälkeen PWM-palvelun Configuration Editor -näkymästä pääsi pois painamalla oikeassa yläkulmassa sijaitsevaa disketin kuvaa. Tämä avasi ikkunan, joka näytti yhteenvedon muutetuista asetuksista. Jos muutokset hyväksyttiin, PWM tallensi ne ja käynnisti itsensä uudelleen. Lopuksi PWM-palvelu voitiin ottaa konfiguraatiotilasta pois muokkaamalla PwmConfiguration.xml-tiedostoa ja asettamalla totuusarvoksi jälleen *false*. Kyseisen muutoksen jälkeen PWM palasi normaaliin käyttötilaan ja oli valmis palvelemaan käyttäjiä.

7 Johtopäätökset

Kokeiluympäristön pystyttämisen ja siihen Citrix SSPR- ja PWM-ratkaisujen onnistuneen käyttöönoton jälkeen kyseiset ratkaisut esiteltiin toimeksiantajalle. Palaute Citrix SSPR -ratkaisusta vastasi odotuksia: kyseinen ratkaisu oli liian suppea toiminnoiltaan ja yhteensopimattomuus Citrix NetScalerin kanssa teki tuotteesta sopimattoman käyttöympäristöön. Citrix SSPR -ratkaisun käyttöönotto oli kuitenkin tarpeellinen seikka, sillä se tarjosi vertailukohdan Citrixin oman SSPR-ratkaisun ja PWM-ratkaisun kanssa.

Myös PWM-ratkaisun esittelystä saatu palaute oli odotusten mukainen: toimeksiantaja totesi ratkaisun sopivan erinomaisesti omaan ympäristöönsä. Erityisesti LDAP-attribuuttien perusteella autentikointi, SMS-moduulin lisäyksen mahdollisuus ja salasananvaihtopalvelun toteuttaminen tekstiviestipalveluna olivat toimeksiantajan mielestä erinomaisia ominaisuuksia. Toimeksiantaja arvosti myös sitä, että PWM antaa mahdollisuuden säilöä dataa Active Directoryn omaan LDAP-tietokantaan. Myös se seikka, että PWM-ratkaisu voidaan ottaa käyttöön Linux-pohjaisille palvelimille, oli toimeksiantajan mieleen.

PWM voidaan upottaa NetScalerin käyttöliittymään lisäämällä PWM-palveluun johtava hyperlinkki NetScalerin kirjautumissivulle. NetScaler-yhteensopivuusseikka voidaan myös kiertää kokonaan, jos PWM-palveluun lisätään SMS-moduuli ja palvelu muutetaan tekstiviestipohjaiseksi. Toimeksiantaja olikin erittäin kiinnostunut tästä mahdollisuudesta ja päätti ottaa ratkaisun sisäiseen jatkokehitykseen.

Vaikka Shaun Vermaakin SSPR-ratkaisu ja HyperSocket Password Self-Service -palveluiden käyttöönotto epäonnistui kohtuullisessa ajassa teknisistä syistä, se ei lopputuloksen kannalta ollut haitaksi. Shaun Vermaakin ratkaisu olisi alkutilassaan ollut liian suppea käyttöympäristöä varten sekä paljon hankalampi jatkokehittää verrattuna PWM-ratkaisuun. HyperSocket Password Self-Service -ratkaisun ilmaisversio oli erittäin paljon suppeampi verrattuna PWM-ratkaisuun, eikä maksullinen versio olisi luultavasti sopinut kohdeympäristöön yhtä hyvin kuin PWM.

Kaiken kaikkiaan opinnäytetyö oli erittäin onnistunut. Opiskelija sai mahdollisuuden pystyttää tuotantoympäristöä vastaavan Citrix XenApp 7.15 LTSR -ympäristön sekä sai kokemusta erinäisten SSPR-ratkaisujen käyttöönotosta. Toimeksiantaja sai jatkokehitystä varten ympäristöönsä erinomaisesti sopivan SSPR-ratkaisun, jota toimeksiantajan on yksinkertaista räätälöidä omaa käyttöympäristöänsä varten. Toimeksiantaja sai myös kattavan dokumentaation kyseisen ratkaisun käyttöönotosta.

Lähteet

[1] Kauppalehti. *Oulun DataCenter Oy.* Viitattu 7.5.2018. https://www.kauppalehti.fi/yritykset/yritys/oulun+datacenter+oy/25425953

[2] Asiakastieto.fi. *Oulun DataCenter Oy*. Viitattu 7.5.2018. https://www.asiakastieto.fi/yritykset/fi/oulun-datacenter-oy/25425953/taloustiedot

[3] BusinessOulu. (24. helmikuu 2016) *Oulun DataCenter Oy kasvaa ja vahvistaa organisaatiotaan*. Viitattu 7.5.2018. https://www.businessoulu.com/fi/uutiset/oulun-datacenter-oy-kasvaa-ja-vahvistaa-organisaatiotaan.html

[4] Oulun DataCenter Oy. *Oulun DataCenter Oy:n konesali- ja pilvipalvelut*. Viitattu 7.5.2018. http://www.ouludc.fi/palvelut

[5] Oulun DataCenter Oy. *Alusta – Futursoft Oy.* Viitattu 7.5.2018. http://www.ouludc.fi/referenssit/alusta_-_futursoft_oy

[6] Citrix. (11. toukokuu 2016) *Concepts and components*. Viitattu 4.5.2018. https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-6/xad-architecture-article/xad-core-concepts.html

[7] Oulun DataCenter Oy. *ODC Laitetila.* Viitattu 7.5.2018. http://www.ouludc.fi/palvelut/odc_laitetila

[8] Oulun DataCenter Oy. *ODC Kapasiteetti.* Viitattu 7.5.2018. http://www.ouludc.fi/palvelut/odc_kapasiteetti

[9] Oulun DataCenter Oy. *ODC Jatkuvuus.* Viitattu 7.5.2018. http://www.ouludc.fi/palvelut/odc_jatkuvuus

[10] Peter Mell & Timothy Grance. (2011, syyskuu). *SP 800-145, The NIST Definition of Cloud Computing*. Viitattu 24.1.2018. https://csrc.nist.gov/publications/detail/sp/800-145/final

[11] Salmio, P. (2012). *Pilvipalvelut*. Opinnäytetyö. Turun ammattikorkeakoulu. http://urn.fi/URN:NBN:fi:amk-201205025762

[12] Reiner, B., & Siegel, E. (2001). *Application service providers: an alternative approach to PACS implementation*. Journal of Digital Imaging, 14(1), 1–8. http://doi.org/10.1007/s10278-001-0017-9

[13] Clare Hopping. (4. heinäkuu 2017). *Everything you need to know about Citrix*. Viitattu 29.1.2018. http://www.itpro.co.uk/saas/28932/everything-you-need-to-know-about-citrix-1

[14] SuccessStory. *Citrix Systems SuccessStory*. Viitattu 29.1.2018. https://successstory.com/companies/citrix-systems

[15] Datanyze. *Virtualization Market Share Report | Competitor Analysis in Datanyze Universe | VMware, Microsoft Hyper-V, VMware vSphere | Datanyze*. Viitattu 21.5.2018. https://www.datanyze.com/market-share/virtualization/Datanyze%20Universe

[16] Bas van Kaam. (29.3.2017). *A walk down memorylane – The Citrus… I mean, Citrix ICA and Microsoft RDP early days…* Viitattu 29.1.2018. http://www.basvankaam.com/2017/03/29/a-lesson-in-history-the-citrix-ica-and-microsoft-rdp-early-days/

[17] Citrix. (2009) *Citrix 20th Anniversary*. Viitattu 29.1.2018. https://www.citrix.com/content/dam/citrix/en_us/documents/go/citrix_timeline.pdf

[18] Greg Shields. (2. huhtikuu 2014). *Citrix Products Evolve, but Name Changes Obscure Unification*. Viitattu 29.1.2018. https://redmondmag.com/articles/2014/04/01/citrix-products-evolve.aspx

[19] Brian Madden. (18.7.2007) *Independent Computing Architecture (ICA) - Citrix MetaFrame XP*. Viitattu 29.1.2018. http://www.brianmadden.com/feature/Independent-Computing-Architecture-ICA-Citrix-MetaFrame-XP

[20] Pawel Serwan. (24.9.2014). *Dive into Citrix ICA protocol*. Viitattu 29.1.2018. https://pawelserwan.wordpress.com/2014/09/24/dive-into-citrix-ica-protocol-part1/

[21] Citrix. (24. tammikuu 2018) *XenApp and XenDesktop Service*. Viitattu 21.5.2018. https://docs.citrix.com/en-us/xenapp-and-xendesktop/service.html

[22] Citrix. (22. toukokuu 2017) *Active Directory*. Viitattu 21.5.2018. https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-14/technical-overview/active-directory.html

[23] Xen Project. *About Us*. Viitattu 21.5.2018. https://www.xenproject.org/about-us.html

[24] Citrix. Citrix *XenServer*. Viitattu 21.5.2018. https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-xenserver-industry-leading-open-source-platform-for-cost-effective-cloud-server-and-desktop-virtualization.pdf

[25] Citrix. (16. toukokuu 2017) *SSPR Not Working in StoreFront 3.7*. Viitattu 21.5.2018. https://support.citrix.com/article/CTX219595

[26] Citrix. (26. helmikuu 2018) *Self-Service Password Reset 1.1.x*. Viitattu 21.5.2018. https://docs.citrix.com/en-us/self-service-password-reset/current-release.html

[27] The PWM Project. *PWM*. Viitattu 21.5.2018. https://github.com/pwm-project/pwm

[28] Shaun Vermaak. (14. tammikuu 2018) *Free/Open-Source Self-Service Password Reset tool for Active Directory*. Viitattu 21.5.2018. https://www.experts-exchange.com/articles/31477/Free-Open-Source-Self-Service-Password-Reset-tool-for-Active-Directory.html

[29] Hypersocket. *Password Self-Service*. Viitattu 21.5.2018. https://www.hypersocket.com/en/products/password-self-service

[30] PistolStar Inc. *Self Service Password Reset*. Viitattu 21.5.2018. https://www.portalguard.com/self-service-password-reset.html

[31] PistolStar Inc. *PortalGuard Pricing*. Viitattu 21.5.2018. https://www.portalguard.com/pricing.html

[32] Ayehu Software Technologies. *Active Directory Password Reset*. Viitattu 21.5.2018. https://ayehu.com/resources/top-10-it-automation-processes/active-directory-password-reset-2/

[33] JiJi Technologies. *JiJi Self Service Password Reset*. Viitattu 21.5.2018. https://www.jijitechnologies.com/jiji-self-service-password-reset.aspx

[34] NetIQ. *Self Service Password Reset*. Viitattu 21.5.2018. https://www.netiq.com/products/self-service-password-reset/

[35] Citrix. (25. huhtikuu 2018) *System requirements*. Viitattu 3.5.2018. https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-15-ltsr/system-requirements.html

[36] Citrix. (1. maaliskuu 2018) *Prepare to install*. Viitattu 3.5.2018. https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-15-ltsr/install-configure/install-prepare.html

[37] Citrix. (3. toukokuu 2018) *How to allocate licenses on My Account*. Viitattu 4.5.2018. https://support.citrix.com/article/CTX126167

[38] Citrix. (26. helmikuu 2016) *System requirements*. Viitattu 6.5.2018. https://docs.citrix.com/en-us/self-service-password-reset/current-release/system-requirements.html

Liite 1: Citrix SSPR-ratkaisun SWOT-analyysi

Citrix SSPR

Vahvuudet	Heikkoudet
• Nopea käyttöönotto • Ei vaadi uudelleenkäynnistyksiä muille palvelimille • Ilmainen XenAppin kanssa • Integroitu StoreFrontiin, ei vaadi erillistä osoitetta	• Ei toimi nykyhetkellä NetScalerin kanssa • Ei lisäominaisuuksia • Suppeat mukautusmahdollisuudet
Mahdollisuudet	**Uhat**
• Citrix kehittää yhteensopivuutta NetScalerin kanssa	• Voi olla sekava käyttää, koska toimii pelkästään StoreFrontin kanssa

Liite 2: PWM-ratkaisun SWOT-analyysi

PWM

Vahvuudet	Heikkoudet
• Nopea käyttöönotto • Ei vaadi uudelleenkäynnistyksiä muille palvelimille • Avoimen lähdekoodin ratkaisu, ilmainen • Laajat mukautusmahdollisuudet • Lisäominaisuuksien integrointi mahdollista • Voidaan asentaa Linux-koneille	• Vaatii tietokantapalvelimen sekä itse PWM-palvelimen • Heikohko suomenkielinen käyttöliittymä
Mahdollisuudet	**Uhat**
• SMS-moduulin käyttöönotto • Suomenkielisen käyttöliittymän parantaminen • SSPR-palvelun osoitteen hyperlinkin lisäys NetScalerin käyttöliittymään	• Suppea tekninen tuki

Liite 3: Shaun Vermaakin avoimen lähdekoodin SSPR-ratkaisun SWOT-analyysi

Shaun Vermaakin avoimen lähdekoodin SSPR

Vahvuudet	Heikkoudet
• Hyvä alusta jatkokehitykselle	• Suppeat mukautusmahdollisuudet ilman ohjelmointitaitoja
Mahdollisuudet	**Uhat**
• C#-ohjelmoijan mahdollista kehittää ratkaisua pidemmälle	• Ei teknistä tukea • Jatkokehitys ei ole taattua

Liite 4: HyperSocket Access Managerin SWOT-analyysi

HyperSocket Access Manager

Vahvuudet	Heikkoudet
• Yksinkertainen käyttöönotto virtuaalilaitteen kautta • Ilmaisversiossa laajat ominaisuudet • Kattavat analytiikkatyökalut • Käyttäjäkohtainen lisensointi	• Ilmaisversiossa ainoana salasananpalautusmetodina turvakysymys-vastauspari
Mahdollisuudet	**Uhat**
• Maksullinen versio tuo kattavat lisäominaisuudet ratkaisuun	• Voi olla turhan suppea ilmaisversiona

Liite 5: PortalGuardin SWOT-analyysi

PortalGuard

Vahvuudet	Heikkoudet
• Kaksivaiheinen autentikaatio • Mobiilisovellus • Kattavat hallintatyökalut	• Kustannukset: 5000 dollaria + lisenssi 5000 dollaria/vuosi • Ei mahdollisuutta luoda omaa kokeiluympäristöä
Mahdollisuudet	**Uhat**
	• Liian järeä ratkaisu yksinkertaiseen käyttötarkoitukseen

Liite 6: Ayehu EyeSharen SWOT-analyysi

Ayehu EyeShare

Vahvuudet	Heikkoudet
• SMS-moduulia tukeva SSPR-ratkaisu • Automatisoitua salasananvaihtopalvelua on mahdollista räätälöidä ympäristön tarpeisiin	• Ratkaisu ei ole ilmainen
Mahdollisuudet	**Uhat**
• Kattava automaatiotyökalu, lisäkehitysmahdollisuudet suuret • Automaatiolle voi löytyä tuotantoympäristössä odottamattomiakin käyttökohteita	• Käyttöönoton hinta on tuntematon

Liite 7: JiJi Self Service Password Resetin SWOT-analyysi

JiJi Self Service Password Reset

Vahvuudet	Heikkoudet
• Outlook Web App -integraatio • Tukee SMS-autentikaatiota • Vanhentuneen salasanan etäresetointiominaisuus	• Hinta: 399 dollaria/500 käyttäjää • Hinta vielä korkeampi mitä enemmän ympäristössä on käyttäjiä
Mahdollisuudet	**Uhat**
	• Käyttöönoton hinta on tuntematon

Liite 8: NetIQ SSPR-ratkaisun SWOT-analyysi

NetIQ Self Service Password Reset

Vahvuudet	Heikkoudet
• Perustuu PWM-ratkaisuun • Toimitetaan virtuaalisena laitteena, nopea käyttöönotto • Kaupallisen tuotteen asiakastuki verrattuna PWM-ratkaisuun	• Maksullinen • Asiakastuki ei tarpeeksi suuri syy käyttää PWM:n sijasta
Mahdollisuudet	**Uhat**
• SMS-moduulin käyttöönotto • SSPR-palvelun osoitteen hyperlinkin lisäys NetScalerin käyttöliittymään	• Käyttöönoton hinta on tuntematon