
**AUTOMATISOITU KÄYTTÄJÄHALLINTO,
KÄYTTÄJÄN INTERAKTION KAUTTA**



Ammattikorkeakoulun opinnäytetyö

Tietotekniikan koulutusohjelma

Riihimäen yksikkö syksy 2014

Jesse Mertanen



RIIHIMÄKI
Tietotekniikka
Ohjelmointi

Tekijä	Jesse Mertanen	Vuosi 2014
Työn nimi	Automatisoitu käyttäjähallinto, käyttäjän interaktion kautta	

TIIVISTELMÄ

Työn määrä Tietotekniikan palvelukeskuksessa eli tipakkeessa kasvaa huomattavasti nopeammin kuin työntekijöiden määrä. Tipakkeen palvelualueena ovat kolme kuntaa ja näiden kuntien loppukäyttäjät. Nykyinen rakenne ja toimintakulttuuri eivät millään kannata enää pitkään, mutta toisaalta nykytilanne ei toistaiseksi salli suuria organisaatiomuutoksia.

Tässä opinnäytetyössä keskityttiin automatisointiin Microsoftin System Center Orchestratorin avulla, lyhyemmin Orchestrator, sekä sivuttiin Orchestratorin linkityksiä muihin järjestelmiin. Pääpaino oli Orchestratorin runbookissa, jota kutsutaan web-porttaalin kautta sähköisellä käyttäjätunnuslomakkeella. Runbook antaa komentoja Active directorylle ja tätä kautta esimiesten on mahdollista jatkossa luoda ja poistaa käyttäjätunnuksia ilman, että välissä tarvitaan tietotekniikan palvelukeskuksen henkilökuntaa. Tavoitteena oli helpottaa Service deskin työkuormaa ja toisaalta nopeuttaa tunnuskäsittelyä loppukäyttäjän näkökulmasta.

Työn teoriaosuudessa kuvataan palvelin- ja järjestelmäarkkitehtuuria sekä lyhyesti oheisjärjestelmät.

Testausosuudessa kuvataan, miten testausta tehtiin ja minkälaisia haasteita kohdattiin sekä sitä miten ne ratkaistiin.

Työn tuloksena saatiin vahvaa näyttöä automatiikan hyödyistä rutiinimaisissa töissä. Lopputuloksena oli, että työn kuormitus tasoittui ja jatkossa vastaavanlaisia automatiikoita tullaan hyödyntämään huomattavasti enemmän.

Avainsanat Automatiikka, orchestrator, active directory, service manager, runbook

Sivut 17 s. + liitteet XX s.

Riihimäki
Degree Programme in Information technology
Programming technology

Author	Jesse Mertanen	Year 2014
Subject of Bachelor's thesis	Automatic user account management, via user interaction	

ABSTRACT

The amount of work in an ITC service center is rapidly increasing more than the number of workers able to do the work. The customers are three municipalities and their end-users. The current construction and working culture cannot last long, but on the other hand, the current situation will not allow big changes in the organizational structure.

This thesis focuses on automation with Orchestrator, and touch on links to other systems. The main focus is in Orchestrator's runbooks, which are triggered via the Web-portal using an electronic user ID form. Runbook commands an Active directory and this is how superiors can create or delete user accounts, without needing the ITC service center. The goal was to lighten the Service desk's amount of work and speed up end users user account handling.

The server architecture and system architecture are described in theoretical part. Also the links to other supporting systems are described.

The practical part describes how the testing was done and the challenges and which solutions were found.

The results of this work were strong evidence of the benefits of automation in routine jobs. The end result was balancing the amount of work and this kind of automation will be exploited in the future much more.

Keywords Automatic, orchestrator, active directory, service manager, runbook

Pages 17 p. + appendices XX p.

SISÄLLYS

1	JOHDANTO	1
2	TYÖN LÄHTÖKOHDAT	1
2.1	Työn toimeksiantaja	2
2.2	Työn tavoitteet	2
3	ARKKITEHTUURI.....	2
3.1	Palvelinarkkitehtuuri	2
3.2	Järjestelmäarkkitehtuuri	3
3.2.1	Yleiskuva	4
3.2.2	Orchestrator	4
3.2.3	Service Manager	6
3.2.4	Active Directory	6
3.2.5	Microsoft Exchange	6
4	TOTEUTUS.....	7
4.1	Service Managerin määrittelyt	8
4.2	Orchestratorin määrittelyt.....	11
4.2.1	Orchestratorin liitännät	12
4.2.2	Runbookkien luominen.....	12
5	TESTAUS	13
5.1	Virheenkäsitteilyrutiini	14
6	YHTEENVETO	15

LÄHTEET

LIITTEET



SANASTO

AD	Active directory. Microsoftin versio LDAP aktiivihakemistopalvelusta.
Affected user	Palvelupyynnössä oleva tietokenttä, josta näkee kuka palvelupyynnön on tehnyt.
Microsoft Exchange	Sähköpostijärjestelmä, jolla loppukäyttäjälle tuotetaan kalenteri- ja sähköpostipalvelua.
Connector	Konnektori, jolla voidaan luoda järjestelmien välisiä yhteyksiä.
Library	Service Managerin kirjasto, jonne on tallennettu Service Managerin tietoartikkelit, runbook -tiedot ja palvelukatalogi.
Orchestrator	Automaatioiden tekemiseen tarkoitettu graafinen työkalu.
Palvelupyyntö	ITIL:n mukainen palvelupyyntö on käyttäjän pyyntö saada jokin asia suoritetuksi. Service managerissa palvelupyyntöön kirjataan esitetty pyyntö ja siihen liittyvät tiedot.
Runbook	Orchestratorin osa, jossa määritellään suoritettavat toiminnot graafisen käyttöliittymän avulla.
SCSM	System Center Service Manager. Microsoftin tuote ITIL-pohjaiselle timentointijärjestelmälle.
Service catalog	Palvelukatalogi, jossa sijaitsee Service Managerin palvelutuotteet.
Sharepoint	Web -sivustojen luomiseen ja julkaisemiseen tarkoitettu Microsoftin tuote.

1 JOHDANTO

It-alalla on huomattavan paljon rutiinitöitä, ylläpitotöitä ja näiden ohella pitäisi toimintaa myös suunnitella ja kehittää. Kuntien nykyinen taloudellinen tilanne on heikko eikä lisäresursseja tahdo saada edes hyvin perustelemalla, etenkin kun useissa kunnissa on juuri käyty yt-neuvotteluja. Opinnäytetyöni aihe on alkusysäys edellä mainittuihin haasteisiin Tietotekniikan palvelukeskuksessa eli tipakkeessa ja tarkoitus on ensin ottaa askel kohti automaattisempaa käyttäjähallintaa, jolla henkilöstön työkuormaa pyritään helpottamaan. Käytännössä päästään eroon manuaalisesta, ja sen takia virhealttiista tunnuskäsittelystä ja paperisista lomakkeista, jotka vielä ovat olleet asiakaskunnissa käytössä. Aiheen valintaan vaikutti myös vahva ohjelmointitaustani sekä mielenkiintoni Microsoftin julkaisemaan System Center Orchestrator -tuotteeseen, joka kokoaa skriptit ja prosessit graafisten kuorien sisälle.

Tavoitteena on saada aikaan esimiehille Service Managerin portaalin kautta toimiva web-lomake, jonka täyttämällä he saavat alaiselleen tunnuksen muutamassa minuutissa. Lisäksi tarkoitus on tuottaa sellainen virhekäsittely, että mikäli automatiikka ei saa tunnusta tuotettua, siirretään se Service Managerissa käsin tehtäväksi tapaukseksi. Lopullinen päämäärä on työnantajan näkökulmasta vapauttaa resursseja muihin työtehtäviin ja tätä kautta lisätä tehokkuutta, sekä toisaalta asiakkaan näkökulmasta helpottaa ja nopeuttaa tunnusten anomisprosessia.

Opinnäytetyön aihe on rajattu uuden tunnuksen ja sähköpostilaatikon tekemiseen. Kokonaisuudessa kuitenkin huomioidaan jatkokehitys, ja tarkoitus on lisätä toimintoja myöhemmin, kuten esimerkiksi lyncin aktivointi ja ryhmäjäsenyydet.

Henkilökohtaisina tavoitteina on osaamisen kartuttaminen ja vaikuttaminen työmäärien kohtuullistamiseen. Jatkossa haluaisin automatisoida enemmänkin rutiininomaisia tehtäviä ja tätä kautta helpottaa jatkuvasti vaativampaa ja haasteellista työympäristöä, jossa työn määrä kasvaa, mutta resurssit eivät.

2 TYÖN LÄHTÖKOHDAT

Työn toteuttaminen aloitettiin Tietotekniikan palvelukeskuksen johdolle tehdyn esityksen pohjalta. Ehdotuksen tavoitteena oli luoda Service managerin portaaliin sähköinen lomake, jonka kautta voi anoa käyttäjätunnuksia. Lomake on tarkoitettu esimiehille, korvaamaan käytössä olevan paperisen version. Lisäksi sähköiseen lomakkeeseen liitetään automatiikka, joka tekee tunnuksen perustietoineen valmiiksi. Tarkoituksena on hyödyntää Service Managerin ja Orchestratorin ominaisuuksia. (Mertanen, sähköpostiviesti 27.9.2013.)

2.1 Työn toimeksiantaja

Työn toimeksiantajana toimii Tietotekniikan palvelukeskus eli Tipake, joka on Keravan liikelaitos. Tipakkeella on oma johtokunta, joka päättää Tipakkeen asioista. Tipake palvelee tällä hetkellä kolmea asiakaskuntaa: Kerava, Järvenpää ja Mäntsälä. Käyttäjätunnuksia näissä on yhteensä noin 7000 ja työntekijöitä on 30, joista tunnuksia käsittelee kaksi Service deskin työntekijää. Työaika tunnuksien tekemiseen menee noin 45–55 tuntia kuukaudessa.

2.2 Työn tavoitteet

Opinnäytetyön tavoitteena on tuottaa ja testata automatisoitu käyttäjähallinto, jossa esimiesasemassa oleva loppukäyttäjä voi tuottaa alaiselleen käyttäjätunnuksen.

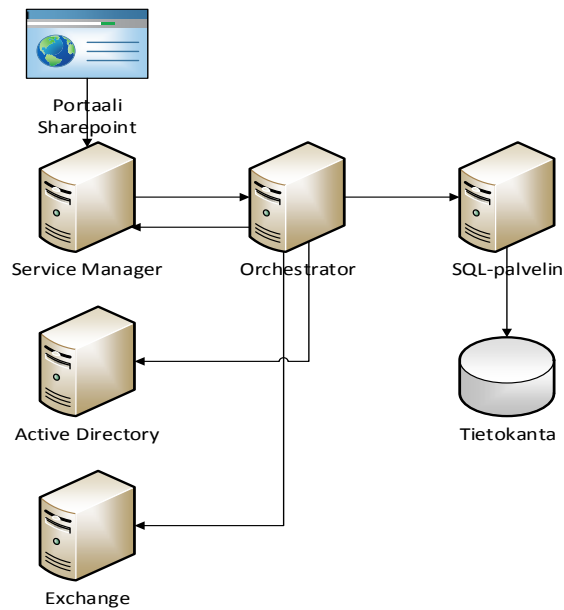
Automatiikka rakennetaan Orchestratorin runbookilla, sekä hyödynnetään olemassa olevaa Service Manager -järjestelmää, jonka tarkempi kuvaus on luvussa 3.2.3. Pää tavoitteena on saada tuotettua käyttöön otettava järjestelmä, jota on mahdollista jatkokehittää ja laajentaa kasvavia tarpeita vastaavaksi.

3 ARKKITEHTUURI

Tipakkeella on VmWaren vCenter -palvelinympäristö, jonka alustana on Dell M1000E DRAC -korttipalvelinkehikko, ja levyjärjestelmänä on Dell Equal Logic. Virtuaalipalvelimien hallintaan ja konfigurointiin käytetään selainpohjaista VmWaren Vsphere -clienttia. Kokonaisuus (liite 1) sijaitsee Keravan konesalissa, johon Tipakkeella on valokuituyhteydet.

3.1 Palvelinarkkitehtuuri

Tähän projektiin liittyviä palvelimia (kuva 1) on hieman laskentatavasta riippuen 3-8. Service Manager on toteutettu käytännössä neljän palvelimen päälle, joista yksi on tietokantapalvelin. Orchestrator on toteutettu kahden palvelimen päälle, joista yksi on sama tietokantapalvelin kuin Service Managerilla. Portaalia varten on sharepoint palvelu, joka on toteutettu kolmen palvelimen päälle. Näiden lisäksi on yhteyksiä muihin järjestelmiin riippuen automatiikasta, mm. Active directory ja Microsoft Exchange.

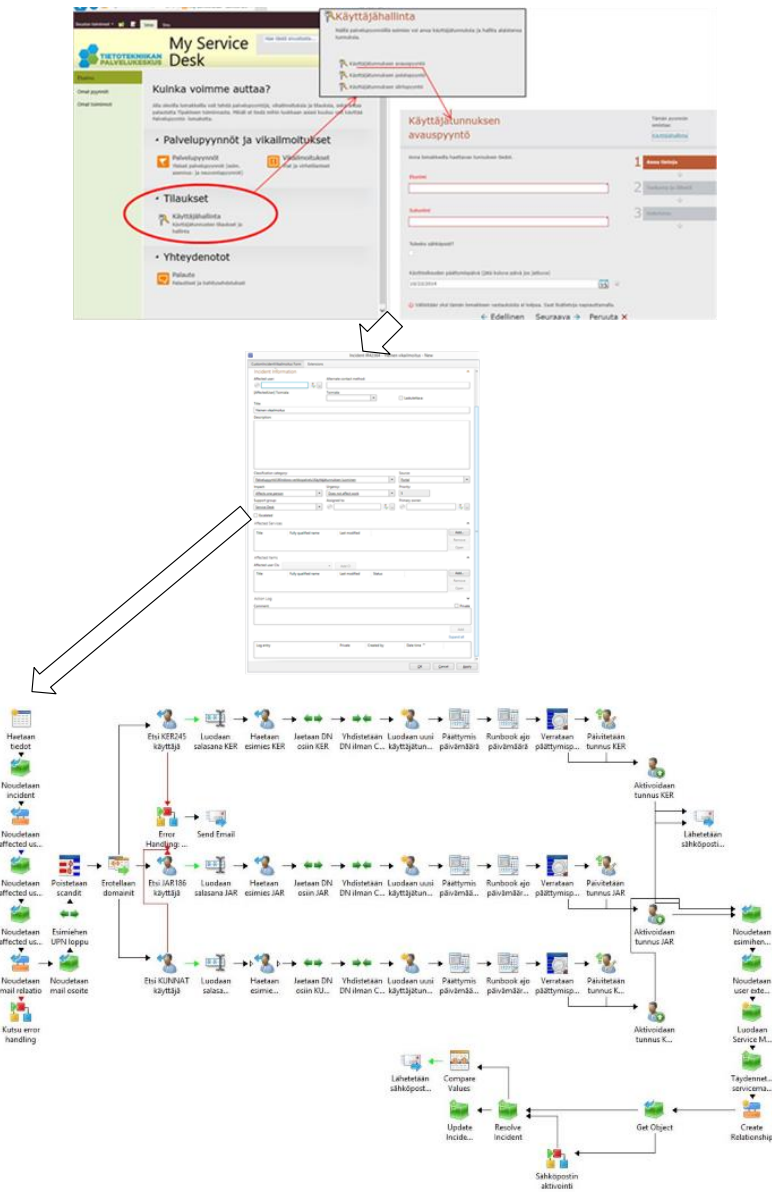


Kuva 1. Palvelinarkkitehtuuri.

3.2 Järjestelmäarkkitehtuuri

Kokonaisuus on esitelty kuvassa 2, jossa ylimpänä on sharepointin päälle rakennettu web -lomake. Lomakkeelle syötetyt tiedot viedään Service Managerin palvelupyynnöön, joka näkyy kuvassa keskellä. Palvelupyynnö aktivoi Orchestratorin runbookin, joka kuvassa on alimmaisena. Annettujen tietojen pohjalta runbook tekee käyttäjälle tunnuksen, täydentää palvelupyynnön tietokenttiä ja ilmoittaa sähköpostilla käyttäjälle uuden tunnuksen ja salasanan, sekä lopuksi sulkee palvelupyynnön.

3.2.1 Yleiskuva



Kuva 2. Kokonaiskuvassa web-portaali, palvelupyyntö ja runbook.

Käyttäjä saa prosessin etenemisestä tietoa web -portaalin kautta, mutta ilman virhetilanteita automatiikka luo tunnuksen muutamassa minuutissa.

Virhetilanteen sattuessa käyttäjä saa tiedon, että tapahtui virhe ja palvelupyyntö on siirretty manuaaliseen käsittelyyn. Käytännössä tämä tarkoittaa sitä, että palvelupyyntö menee asiantuntijalle, joka tarkistaa virheen ja tekee tunnuksen käsin.

3.2.2 Orchestrator

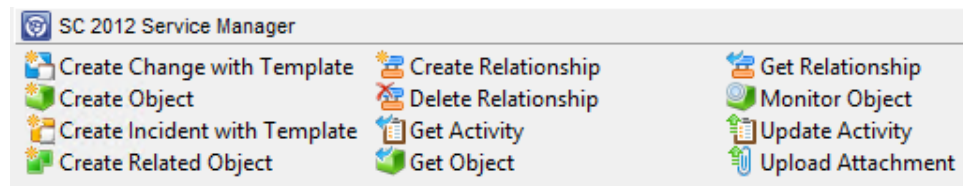
Microsoftin System Center Orchestrator on automaatioiden tekemiseen tarkoitettu graafinen toiminnanohjaustyökalu, johon on keskitetty tärkeimmät ohjelmointi- ja automaatiotyökalut integrointia ja järjestelmien ohjaamista varten. Orchestratorin tarkoituksena on erilaisten prosessien ja

työnkulkujen ohjaaminen ja koordinointi. (Orchestrator Capabilities. 2014.)

Orchestrator kokoaa kaikki yleiset työkalut yhteen, kuten skriptit, liitännät muihin järjestelmiin ja perustiedostonkäsittelyt. Näin kokonaisuudesta tulee yksi hallittava järjestelmä, ja kaikki automaatio voidaan pitää yhdessä paikassa sen sijaan, että se olisi jaettu eri palvelimille ja eri tiedostosijainteihin.

Jotta Orchestratorilla voidaan rakentaa runbook, tarvitaan käyttöön erilaisia työkaluja. Orchestratorin sisällä näitä kutsutaan integration packeiksi ja valmiiksi tehtyjä työkaluja voi helposti ladata Microsoftin omilta sivuilta. Service managerin hallintaa varten lasimme ja asensimme System Center Integration Pack for System Center 2012 Service Manager -paketin. Integraatiopaketin käyttöönotto tapahtuu Orchestratorin Deployment Manager -työkalussa. Microsoftilta löytyy paljon valmiita paketteja eri tarkoituksiin, jotka voi myös ottaa käyttöön Deployment Manager -työkalulla.

Kun tarvittu integraatiopaketti on asennettu, tapahtuu itse työn toteutus Orchestratorin runbook designer -työkalussa. Asennettujen pakettien sisältämät toiminnot löytyvät työkalun oikeasta reunasta. Kuvassa 3 on Service managerin toimintoja, jotka integraatiopaketista asennettiin.



Kuva 3. Service managerin toiminnot runbook designerissa.

Asennettavien integraatiopakettien lisäksi Orchestratorissa on oletuksena toimintoja, joilla voi tuoda esimerkiksi parametreja runbookiin tai ajastaa runbookin käynnistymään tiettyyn aikaan.

Käyttäjätunnusautomaatikassa on hyödynnetty parametreja. Tällöin runbookin ensimmäiseksi toiminnoksi laitetaan Initialize Data -toiminto, jonka nimen voi tosin muuttaa kuvaavammaksi. Toimintojen väliin tulee nuoli, joka vedetään ensimmäisestä toiminnosta seuraavaan. Tämä kertoo ohjelmalle miten toiminnosta toiseen edetään. Yhdestä toiminnosta voi lähteä nuolia useisiin toimintoihin ja toisaalta yhteen toimintoon voidaan tulla useasta toiminnosta, aina kuitenkin siten, että runbookilla on vain yksi alku.

Toimintojen välissä oleviin nuoliin voidaan määritellä ehtoja, jotka perustuvat aikaisempiin toimintoihin. Käyttäjätunnusautomaatikassa tätä on hyödynnetty siten, että kun samalla runbookilla tehdään kolmeen kuntaan tunnuksia, niin esimiehen toimialueesta määritellään ehdoksi kunta ja tämän perusteella toiminto ohjautuu kyseistä kuntaa koskevaan prosessiin. Tämä on esitelty luvussa 4.2.2.

3.2.3 Service Manager

System Center Service Manager on Microsoftin tuote, jolla hallitaan It - palveluiden tarjontaa. Service Manager pohjautuu Information Technology Infrastructure Libraryyn eli ITIL:iin. ITIL on käytännössä kokoelma käytäntöjä IT-palveluiden hallintaan ja johtamiseen. (Key Element Guide ITIL Service Operation. 2012, 1-4.)

Service Managerissa on valmiit prosessit vikailmoituksille, palvelupyynnöille, muutoshallinnalle ja ongelmanhallinnalle (Service Manager. 2014). Tietotekniikan palvelukeskuksessa on käytössä nämä kaikki, mutta Service Managerin tarjoamien tapojen kohdalla olemme hieman muokanneet olemassa olevaa järjestelmää. Käytännössä pääosa toiminnoista on rakennettu suoraan vikailmoitusprosessien alle ja eriytetty toisistaan luokituilla. Tähän toteutukseen on päädytty pääosin siksi, että vikailmoituslomake on Service Managerissa ainoa, jolla voi seurata tapauksen käsittelyyn käytettyä aikaa.

Vikailmoituksia varten Service Managerissa on lomake, johon tallennetaan vikailmoitusta koskevat tiedot. Vikailmoituksia voi tulla Tietotekniikan palvelukeskuksen service deskille sähköpostilla, portaalin kautta tai puhelimitse. Sähköpostin ja portaalin kautta tuleisiin ilmoituksiin ei tarvitse täydentää kuin toimialue, luokittelu eli vian yleiskuvaus, kiireellisyys, toimialue ja kenelle tapaus ohjataan käsiteltäväksi. Puhelimitse tuleva ilmoitus vaatii lisäksi ilmoittajan, vian otsikon ja tarkemman vian kuvauksen.

Käyttäjätunnusautomaattikan osalta kaikki tiedot ja ilmoituksen käsittelyvaiheet luomisesta ratkaisuun täytetään automaattisesti. Ainoastaan silloin kun automaattikassa tapahtuu virhe, joudutaan osa tiedoista käsittelemään manuaalisesti, hieman riippuen missä kohdassa automaattikkaa virhe on tullut. Virheenkäsittelystä on kerrottu tarkemmin luvussa 5.1.

3.2.4 Active Directory

Active directory lyhyemmin AD on Microsoftin Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu. Käyttäjätilien lisäksi AD sisältää tiedot toimialueessa olevista konetileistä ja muista verkon resursseista. Lisäksi AD:n kautta voidaan määritellä suojauspolitiikkoja ja ryhmäkäytäntöjä. (Active Directory overview. 2005.)

3.2.5 Microsoft Exchange

Microsoftin Exchange tarjoaa käyttäjille sähköposti- ja kalenteripalveluita. Käyttäjällä pitää olla tili AD:ssa tai se voidaan postilaatikon luonnin yhteydessä luoda AD:hen. (Introduction to Installing and Managing Microsoft Exchange Server 2007. 2007, 1.)

4 TOTEUTUS

Automatisoidun käyttäjähallinnon rakentaminen päätettiin aloittaa yhteistyössä konsultin kanssa siten, että samalla saadaan koulutusta Orchestratoriin ja toisaalta perustaitoja, jotta jatkossa voidaan toteutuksia tehdä itse. Tipakkeesta varattiin toteutukseen kaksi henkilöä, joilla oli osaamista myös service managerista. Ennen varsinaista käyttäjähallinnon automaatiikkaa täytyi ensin luoda yhteydet Active directoryyn, Microsoft Exchangeen ja Service Manageriin.

Toteutuksen lähtökohtana oli muodostaa web -lomakkeen täyttämisen jälkeen palvelupyyntö (kuva 4), johon kaikki tieto tallentuisi jatkokäsittelyä varten.

The screenshot shows a web-based form for creating a new incident. The title is "Incident IR42364 - Yleinen vikailmoitus - New". The form is divided into several sections:

- Incident Information:** Includes fields for "Affected user" (with a user selection icon), "Alternate contact method", "Title" (containing "Yleinen vikailmoitus"), and a large "Description" text area.
- Classification and Details:** Includes "Classification category" (set to "Palvelupyynnöt/Windows-verkkopalvelu/Käyttäjätunnuksen luominen"), "Source" (set to "Portal"), "Impact" (set to "Affects one person"), "Urgency" (set to "Does not affect work"), "Priority" (set to "5"), and "Support group" (set to "Service Desk").
- Assignment:** Includes "Assigned to" and "Primary owner" fields with user selection icons, and an "Escalated" checkbox.
- Affected Services and Items:** Two table-like sections with columns for "Title", "Fully qualified name", "Last modified", and "Status". Each section has "Add...", "Remove", and "Open" buttons.
- Action Log:** Includes a "Comment" text area with a "Private" checkbox and an "Add" button.
- Log Entry Table:** A table with columns for "Log entry", "Private", "Created by", and "Date time".

At the bottom of the form are "OK", "Cancel", and "Apply" buttons.

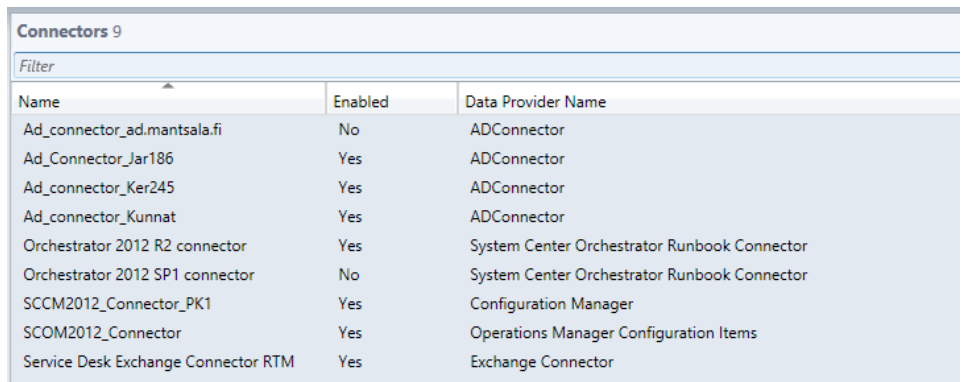
Kuva 4. Service Managerin palvelupyynnö.

Affected user tarkoittaa tapauksen ilmoittajaa, eli tässä tapauksessa esimiestä. Affected user -kenttään tallentuu tieto käyttäjän käyttäjätunnuksesta. Kun tunnus luodaan Active directoryyn, kyseinen esimiestieto kirjataan luodun tunnuksen manager -kenttään. Alempana palvelupyynnössä näkyy kommenttikenttä, johon kirjataan sekä asiakkaalle näkyviä kommentteja tapauksen etenemisestä että tarvittaessa yksityisiä kommentteja, kuten automatiikan mahdollisesti tuottamia virheilmoituksia.

4.1 Service Managerin määrittelyt

Kokonaisuutta varten, Service manageriin on luotu liitännät (kuva 5). Käyttäjäautomatiikkaa varten liitäntä tarvitaan vain Orchestratoriin, koska

Service Managerilla ei ole tarkoitus kuin käynnistää Orchestratorin runbook.

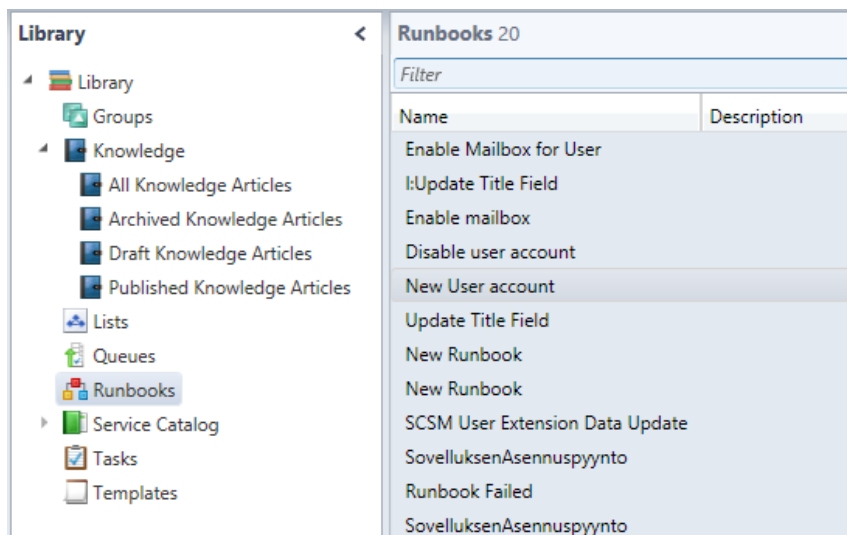


The screenshot shows a table titled 'Connectors 9' with a filter bar. The table has three columns: Name, Enabled, and Data Provider Name. The data rows are as follows:

Name	Enabled	Data Provider Name
Ad_connector_ad.mantsala.fi	No	ADConnector
Ad_Connector_Jar186	Yes	ADConnector
Ad_connector_Ker245	Yes	ADConnector
Ad_connector_Kunnat	Yes	ADConnector
Orchestrator 2012 R2 connector	Yes	System Center Orchestrator Runbook Connector
Orchestrator 2012 SP1 connector	No	System Center Orchestrator Runbook Connector
SCCM2012_Connector_PK1	Yes	Configuration Manager
SCOM2012_Connector	Yes	Operations Manager Configuration Items
Service Desk Exchange Connector RTM	Yes	Exchange Connector

Kuva 5. Service managerin liitännät.

Orchestratorin liitäntä on kuvassa 5 nimellä *Orchestrator 2012 R2 connector*. Liitäntän luomisen jälkeen, voidaan Service Managerin kirjastoon määrittellä runbook. Runbook täytyy ensin olla luotuna, jotta se voidaan ottaa käyttöön Service Managerissa (kuva 6).



The screenshot shows the Service Manager interface. On the left is the 'Library' pane with a tree view containing: Library, Groups, Knowledge (with sub-items: All Knowledge Articles, Archived Knowledge Articles, Draft Knowledge Articles, Published Knowledge Articles), Lists, Queues, Runbooks, Service Catalog, Tasks, and Templates. On the right is the 'Runbooks 20' pane with a filter bar and a list of runbooks:

Name	Description
Enable Mailbox for User	
!Update Title Field	
Enable mailbox	
Disable user account	
New User account	
Update Title Field	
New Runbook	
New Runbook	
SCSM User Extension Data Update	
SovelluksenAsennuspyynto	
Runbook Failed	
SovelluksenAsennuspyynto	

Kuva 6. Runbookin määrittely Service Managerissa.

Portaaliin täytyy luoda tunnuspyyntöä varten web-lomake, mikä tapahtuu myös Library osiossa, kohdassa Service Catalog. Tähän määritellään lomakkeella annettavat tiedot. Web -lomake haluttiin pitää mahdollisimman selkeänä ja käytännössä siinä kysytään tällä hetkellä vain etunimi ja sukunimi, sekä optiona annetaan sähköpostilaatikon luominen ja tarvittaessa tunnuksen voimassaoloaika.

Edit Request Offering

General

User Prompts

Configure Prom...

Map Prompts

Knowledge Artic...

Publish

History

Description, shown on the request offering page:
Lomakkeella pyydetään uutta käyttäjätunnusta

Template name:
Custom / Incident / New AD User Select template

Management pack:
Custom / Incident / New AD User New...
Last modified: 28.5.2014 12:41:16

^ User Prompts

Enter the prompts or information text

Form instructions:
Anna lomakkeella haettavan tunnuksen tiedot.

Enter prompts or information text

	User Prompts or Information	Response Type	Prompt Type
1	Etunimi	Required	Text
2	Sukunimi	Required	Text
3	Tuleeko sähköposti?	Optional	True/False
4	Käyttöoikeuden päättymispäivä (jätä kuluva päivä jos ja...)	Optional	Date

! You can configure the prompts above on the next wizard pages.

^ Configure Prompts

Configure user prompts

Select a prompt and click Configure below to constrain valid input for the prompt.

	User Prompts or Information	Prompt Output
1	Etunimi	1: String (string)
2	Sukunimi	1: String (string)
3	Tuleeko sähköposti?	1: True / False (bool)
4	Käyttöoikeuden päättymispäivä (jätä kuluva päivä jos ja...)	1: Date (datetime)

✓ All prompts configured

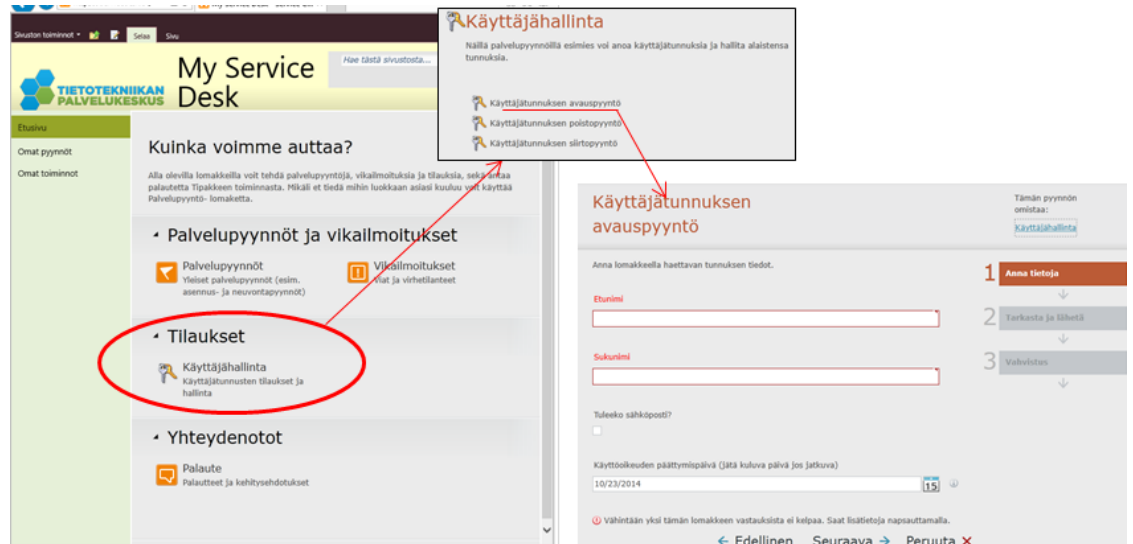
OK Cancel

Kuva 7. Lomakkeen määrittelyt.

Service Managerissa määriteltiin web-lomakkeella täytettävät kentät (kuva 7). Web-lomakkeelle annetut tiedot tallentuvat Service Managerin palvelupyntöön, josta runbookin automatiikka käy tiedot lukemassa.

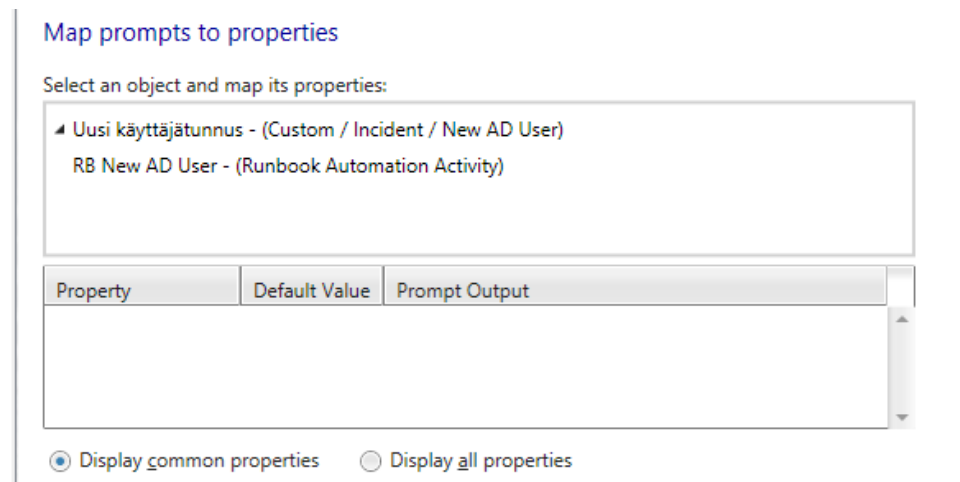
4.2 Orchestratorin määrittelyt

Automatiikka vaatii toimiakseen liitännät myös Orchestratoriin sekä itse runbookin, jossa automatiikka sijaitsee. Lisäksi tarvitaan käyttäjän web-lomakkeelle (kuva 8) antamat tiedot. Luvun 4 alussa käsiteltiin tietojen tallentuminen palvelupyynnöön, josta runbookilla toteutetun automatiikan on ne tarkoitus lukea. Tätä toimintoa varten runbookille annetaan kutsu-misvaiheessa parametrina palvelupyynnön yksilöllinen tunnus.



Kuva 8. Web-portaalin lomake.

Tämän jälkeen kokonaisuuden ohjaus siirtyy Service Managerin määrittelyjen (kuva 9) mukaisesti Orchestratorille, jossa aktivoituu tietty runbook. Runbookin (liite 2) tehtävä on ohjata tunnuksen luomisprosessia ja tehdä palvelupyynnöön merkintöjä pyynnön etenemisestä sekä päivittää palvelupyynnön statusta.



Kuva 9. Runbookin kutsuminen Service Managerista.

4.2.1 Orchestratorin liitännät

Kaiken ytimessä on Active directory, jossa kaikki käyttäjätilit sijaitsevat. Active directory on kuvattu tarkemmin luvussa 3.2.4. Tätä liitännää tarvitaan uutta tunnusta luotaessa sekä tietojen keräämistä varten. Liitännän kautta Orchestrator osaa käskyttää Active directoryä (Active Directory Integration Pack for System Center 2012 - Orchestrator. 2013).

Käyttäjätilin luomisen jälkeen on mahdollista, että tunnuksesta halutaan myös sähköpostiosoite. Sähköpostia varten täytyy luoda liitäntä myös Microsoft Exchange -palvelimeen. (Exchange Admin Integration Pack for Orchestrator in System Center 2012 SP1. 2013.)

Järjestelmän käyttöliittymä on rakennettu Service Manager -tuotteen omilla ominaisuuksilla sharepointin päälle. Lisäksi Service Managerissa on kaikkien tapausten tiedot, joten tarvitaan vielä liitäntä Service Manageriin. (System Center Integration Pack for System Center 2012 Service Manager. 2013.)

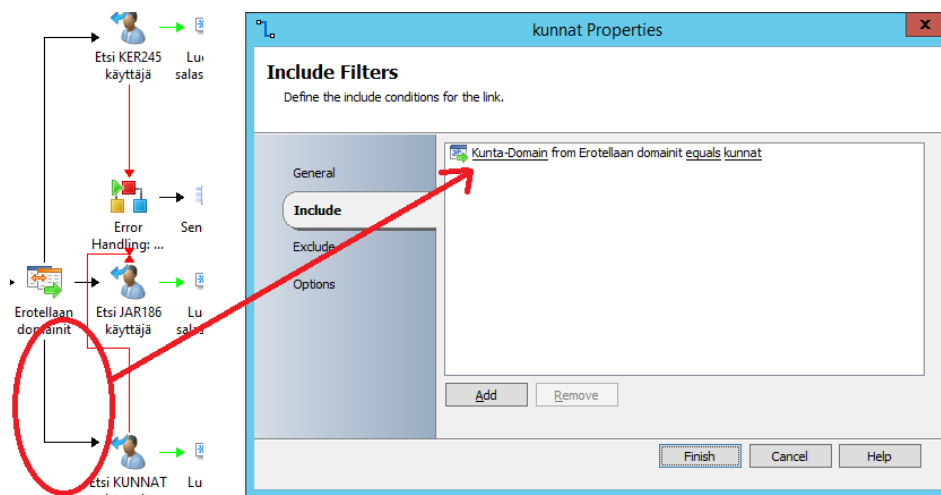
4.2.2 Runbookkien luominen

Service Manager välittää palvelupyynnön yksilöllisen tunnuksen parametrina runbookille (liite 2). Ensimmäisessä vaiheessa automatiikka kerää tietoja muodostuneesta palvelupyynnöstä ja pyynnön ilmoittajasta. Näitä tietoja hyödynnetään prosessin edetessä.

Työkalu on suunniteltu esimiehille, jotta he voivat alaisilleen tehdä nopeasti tunnusia. Näin ollen lähes kaikki alaiselle luotavan tunnuksen tiedoista kopioidaan esimiehen tiedoista, kuten esimerkiksi toimialue ja kustannuspaikka. Lisäksi luotuun tunnukseen tallennetaan esimiestieto, joka Active directoryn puolella näkyy manager -kentässä.

Jokainen asiakaskunta on tällä hetkellä omassa toimialueessa, ja tässä vaiheessa oletettiin, että esimiehen alainen on samassa kunnassa kuin esimieskin. Näin ollen ensin katsotaan esimiehen käyttäjätiedoista mihin toimialueeseen hänen tunnuksensa on tehty ja tämän jälkeen tarkistetaan kyseisestä toimialueesta, ettei sieltä löydy samanmuotoista tunnusta.

Runbookin sisällä kullekin toimialueelle on oma tunnuskäsittelynsä ja esimiehen toimialue (kuva 10) määrittelee mikä näistä valitaan. Prosessi muodostaa satunnaisen salasanan, tutkii esimiehen käyttäjätunnuksen sijainnin Active directoryssa ja hakee esimiehen tiedoista kustannuspaikan. Näiden tietojen pohjalta uusi käyttäjätunnus luodaan samaan sijaintiin ja samalle kustannuspaikalle. Lisäksi käyttäjätunnuksen määrittellään manager -kenttään esimiehen tiedot. Tämä määrittely perustuu siihen, että jatkossa voidaan tutkia mitkä tunnukset ovat kenenkin esimiehen alaisia.



Kuva 10. Esimiehen domain -tieto ohjaa automatiikan oikeaan tunnus käsittelyyn.

Tunnuksen luomisen jälkeen katsotaan palvelupyynnöstä, tehdäänkö käyttäjälle sähköposti ja asetetaanko tunnukselle voimassaoloaika. Lopuksi tunnus aktivoidaan ja lähetetään esimiehelle sähköpostilla käyttäjätunnus ja salasana. Tämän jälkeen päivitetään palvelupyynnön, mitä tunnukselle on tehty ja lopuksi merkitään palvelupyynnön tehdyksi.

5 TESTAUS

Testauksessa oli useita vaiheita. Aluksi testasimme automatiikan toimintaa luomalla itse tunnuksia ja myöhemmässä vaiheessa valitsimme loppukäyttäjistä halukkaita pilotoimaan lomakkeen toimintaa.

Loppukäyttäjistä ensimmäinen pilotointiryhmä oli Keravan kaupungin terveyskeskus, jolla oli tarve saada tunnukset nopeasti esim. keikkalääkäreille. Automatiikasta kiinnostui myös Järvenpään terveyskeskus samasta syystä, sekä myöhemmin Järvenpään Resina, joka tekee Järvenpäässä sijaisvälitystä. Tarpeissa korostui juuri se, että tunnus täytyi saada nopeasti.

Eniten virhetilanteita tuli, kun tunnusta yritettiin luoda henkilölle, jolla oli jo tunnus. Yhtenä pilottiryhmänä oli Järvenpään Resina, jossa automatiikkaa testanneet henkilöt eivät olleet varsinaisesti sijaisten esimiehiä, vaan välittivät sijaisia eri pisteisiin Järvenpäässä. Tällöin tunnusta oli saattanut hakea sijaisen työnjohdollinen esimies vanhalla tavalla, sekä sijaisvälityksen työntekijä automatiikan avulla. Tällöin käyttäjätunnusautomatiikan runbook pysähtyi virheeseen, kun se yritti luoda samanmuotoista tunnusta active directoryyn, joka siellä jo oli.

Vastaava kuin edellä kuvattu virhetilanne tuli myös siitä, että järjestelmässä oli olemassa jo samanniminen henkilö, vaikkei hän sama henkilö ollutkaan. Molemmissa tapauksissa oli sama ratkaisu eli runbookiin lisättiin toiminto, joka haki active directorystä tunnusta, joka sinne oli tarkoitus luoda. Mikäli tuloksia oli nolla, niin jatkettiin eteenpäin, mutta mikäli tulos oli enemmän kuin nolla, ohjattiin runbook virheenkäsittelyrutiiniin, josta kerron tarkemmin luvussa 5.1.

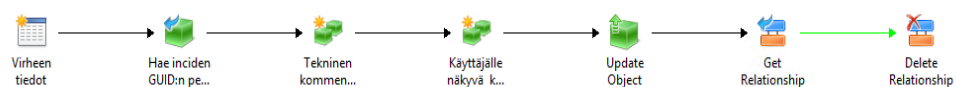
Huolimattomuusvirheiltäkään ei välttytty, sillä kolmen kunnan tunnukset ovat kolmessa eri toimialueessa ja runbookissa oli omat prosessinsa kunkin toimialueen tunnusten luomiselle. Järvenpään toimialueeseen oli kuitenkin tullut käyttäjätunnuksen hakuun vahingossa Keravan toimialueen tiedot. Niinpä tarkistus ohjautui virheenkäsittelyyn vain, jos Keravalta löytyi samanmuotoinen tunnus, kuin mitä Järvenpään oli luomassa. Tämän virheen kohdalla ratkaisu oli helppo, mutta virheen löytäminen vaikeaa.

Pilottiryhmästä löytyi myös yksi esimies, jolla ei ollut sähköpostilaatikoita. Tämän esimiehen kohdalla runbook pysähtyi virheilmoitukseen aina, kun se yritti lähettää esimiehelle sähköpostia. Käytännössä ongelma korjattiin luomalla kyseiselle henkilölle sähköpostilaatikko, mutta lisäksi runbookiin lisättiin toiminto, joka käy tarkistamassa, onko esimiehelle määritetty sähköpostiosoite ja mikäli on, niin käytetään sitä tietojen lähettämiseen, mikäli ei ole, mennään virheenkäsittelyrutiiniin.

5.1 Virheenkäsittelyrutiini

Ensimmäisen pilotoinnin yhteydessä huomattiin erilaisia "ongelmatilanteita", joiden osalta täytyi miettiä ratkaisumalleja. Ensimmäinen haaste johon törmäsimme, oli jo olemassa olevaan tunnuksen reagoiminen. Jotta mahdolliset virheet eivät pysäytä koko automatiikkaa, päätettiin rakentaa oma virheenkäsittelyrutiini, joka ohjaisi virheen sattua tapauksen manuaaliseen käsittelyyn.

Orchestratoriin tehtiin oma runbook, jota kutsutaan aina kun tapahtuu virhe. Kyseiseen palvelupyyntöön kirjataan merkintä tapahtuneesta virheestä käsittelijää varten, sekä lisäksi loppukäyttäjää varten tieto, että tapaus on siirtynyt manuaaliseen käsittelyyn.



Kuva 11. Virheenkäsittelyn runbook.

Virheen käsittely -funktiossa (kuva 11) annetaan parametrina Service Manager -järjestelmän luoma tapauksen id -tieto sekä tapaukseen kirjattavat virhetekstit. Tiedot päivitetään oikeaan palvelupyyntöön id-tiedon perusteella ja tämän jälkeen poistetaan palvelupyynnöstä suorittajatieto.

Suorittajatiedon poistaminen perustuu sovittuun tapaan, jolla Service Manager käsittelee palvelupyynnöitä. Kun palvelupyynnön käsittelijää ei ole määritetty, palvelupyyntö siirtyy järjestelmässä Service desk työntekijälle, joka ohjaa palvelupyynnön käsittelijälle.

6 YHTEENVETO

Opinnäytetyössäni kehitettiin Tietotekniikan palvelukeskuksen käyttäjätunnushallintaa automatisoimalla käyttäjätunnuksen anominen. Kokonaisuus toteutettiin tekemällä kunnille tarkoitettuun Service Managerin portaaliin web -lomake, jolla esimies voi luoda alaiselleen tunnuksen. Tavoitteena oli nopeuttaa sekä helpottaa prosessia asiakkaan näkökulmasta ja keventää työkuormaa service desk -työntekijän näkökulmasta. Henkilökohtaisena tavoitteena oli oman osaamisen lisääminen siten, että jatkossa vastaavia automatisointeja voidaan toteuttaa ilman ulkopuolista apua.

Pääosin työ eteni hyvin, mutta jonkin verran aikataulut venyivät johtuen muista työkiireistä sekä Orchestratorin päivityksen aiheuttamista jälkitöistä. Työn toimeksiantajan puolesta ei varsinaista aikataulua ollut, joten kokonaisuuden kannalta aikataulujen venymisellä ei ollut merkitystä.

Tavoitteet saavutettiin onnistuneesti ja saadun palautteen perusteella juuri palvelun nopeus oli testiryhmien mielestä heitä eniten hyödyttävä asia. Myös oma osaamiseni karttui ja olen kehittämässä erilaisiin tarpeisiin lisää automatisointeja Orchestratorilla.

LÄHTEET

Active Directory Integration Pack for System Center 2012 - Orchestrator. 2013. Microsoft. Technet.
Viitattu 31.10.2014.

<http://technet.microsoft.com/en-us/library/hh553474.aspx>

Active Directory overview. 2005. Microsoft. Technet.
Viitattu 30.10.2014.

<http://technet.microsoft.com/en-us/library/cc758436%28v=ws.10%29.aspx>

Exchange Admin Integration Pack for Orchestrator in System Center 2012 SP1. 2013. Microsoft. Technet.
Viitattu 31.10.2014.

<http://technet.microsoft.com/en-us/library/jj614529.aspx>

Introduction to Installing and Managing Microsoft Exchange Server 2007. 2007. Microsoft. Kurssimateriaali 5047a. Moduuli 1, sivu 1.

Key Element Guide ITIL Service Operation. 2012. Best management practice. Lontoo.

Mertanen, Jesse. 27.9.2013. Projektisuunnitelma - Käyttäjätunnuslomakkeen sähköistäminen. Vastaanottaja Ari Viljanen. Sähköpostiviesti. 27.9.2013.

Orchestrator Capabilities. 2014. Microsoft. Technet.
Viitattu 23.10.2014.

<http://technet.microsoft.com/en-us/library/hh420338.aspx>

Service Manager. 2014. Microsoft. Technet.
Viitattu 24.10.2014.

<http://technet.microsoft.com/en-us/library/hh305220.aspx>

So What Is Active Directory? 2014. Microsoft. Developer Network. Viitattu 22.9.2014.

<http://msdn.microsoft.com/en-us/library/aa746492%28v=vs.85%29.aspx>

System Center Integration Pack for System Center 2012 Service Manager. 2013. Microsoft. Technet.

Viitattu 22.9.2014.

<http://technet.microsoft.com/en-us/library/hh832008.aspx>

LIITTEET

Liite 1

Datacenterin laitteet (ei julkinen liite)

Liite 2

Uuden käyttäjän luomisen -runbook (ei julkinen liite)