HAAGA-HELIA
ammattikorkeakoulu

Valmistelu käyttäjätunnushallinnan automatisoinnille Microsoft System Center 2012:n avulla

Kimmo Vilhunen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2014

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

11.12.2014

Tekijä(t)
Kimmo Vilhunen

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Valmistelu käyttäjätunnushallinnan automatisoinnille Microsoft System Center 2012:n avulla

Sivu- ja liitesivumäärä
34 + 2

Opinnäytetyön otsikko englanniksi
Preparing the automation of user account management with Microsoft System Center 2012

Helsingin kaupungilla on käytössään selainkäyttöinen tunnushallintatyökalu, jonka kaupungin aktiivihakemistoa ylläpitävä toimittaja tarjoaa. Julkishallinnon kilpailuttamisvelvoitteen myötä on tunnistettu, että mikäli toimittaja vaihtuu, työkalun käyttöoikeus lakkaa.

Opinnäytetyössä selvitettiin voidaanko tällä hetkellä oleva käyttäjätunnushallinnan työkalu korvata Microsoft System Centerin Service Managerin ja Orchestratorin toiminnallisuuksilla. Lisäksi selvitettiin mahdollisuuksia lisätä automaatiota. Ohjelmistojen ja itsepalveluportaalin asennukset ja alkukonfiguroinnit on rajattu pois työn laajuudesta.

Työn teoriaosuudessa käsitellään palvelunhallintaa ITIL:in ja Microsoft Operations Frameworkin (MOF) näkökulmista, joihin myös Service Manager vahvasti nojaa. Lisäksi esitellään Service Managerin ja Orchestratorin ominaisuuksia, toimintaa ja tärkeimpiä käsitteitä.

Tuotoksena syntyi proof of concept –tyyppinen versio tunnushallintaportaalista, jossa palvelupyynnön tiedoista muodostettiin käyttäjätunnus ja luotiin se runbook-työnkulun avulla aktiivihakemistoon. Aiempien testien perusteella oli todettu, että Service Managerin omaa itsepalveluportaalia ei haluta käyttää. Itsepalveluportaalina käytettiin Ciresonin kehittämää portaaliratkaisua.

Johtopäätöksenä Service Managerin ja Orchestratorin toiminnallisuuksilla voidaan toteuttaa tunnushallinnan toiminnallisuudet, joissa on suurin volyymi (mm. uuden tunnuksen luominen ja käyttäjän salasanan palauttaminen). Nykyisin käytössä olevan työkalun monipuolista hakutoiminnallisuutta ei voida portaaliin toteuttaa. Haut on käytännössä toteutettava yksittäisinä palveluina, jotka muodostavat tarvittavat raportit dokumenttina. Service Managerissa ei voida arkistoida tietoja pitkiä aikoja, joten käyttöoikeuksien jäljitettävyysvaatimus edellyttää erillistä lokiratkaisua.

Asiasanat
palvelunhallinta, ITIL, käyttäjätunnus, Service Manager

HAAGA-HELIA
University of Applied Sciences

Abstract

11.12.2014

Author(s)
Kimmo Vilhunen

Degree programme
Information Technology

Report/thesis title
Preparing the automation of user account management with Microsoft System Center 2012

Number of pages and appendix pages
34 + 2

City of Helsinki is currently using a web browser based tool to manage user accounts and other active directory objects. The tool is provided by the AD provider. As public administration is required by law to invite to tender, a concern has risen that the license to use the tool will cease if the AD provider is changed.

The main objective of this thesis was to find out if the current tool can be replaced with the functionalities of the Microsoft System Center Service Manager and Orchestrator. Another objective was to find possibilities to increase automation in the user account management process. Installations and out-of-the-box configurations of the software and the self-service portal were left outside the scope of this thesis.

The theory section covers service management from the points of view of ITIL and Microsoft Operations Framework. These are strongly implemented in Service Manager processes. Furthermore, the theory section covers functionalities of Service Manager and Orchestrator and some of the most important concepts of the products.

The actual product was a proof-of-concept type of version of the user account management portal. As a service request is sent, a user account is automatically formed from the information of the request and the runbook creates the account into the active directory. On the basis of the results of earlier testing it was decided that the native portal of Service Manager will not be used. Instead, the self-service portal Cireson has developed will be used.

In conclusion, the functionalities of Service Manager and Orchestrator can handle the user cases with the highest volume, such as creating a new user or resetting a user password. However, it is not possible to create as versatile search and reporting functionalities as the current tool provides. They have to be implemented as single services that form a document, based on in advance defined criteria. It is also not possible to store information for a long period of time in Service Manager. In order to trace user account requests as policy and regulation dictates, a separate solution for logging is required.

Keywords
service management, ITIL, user account, Service Manager

Sisällys

1 Johdanto 1
2 Palvelunhallinta 2
2.1 Palvelunhallinta ITIL:ssä 2
2.2 Menettelytavat, periaatteet ja peruskäsitteet ITIL:ssä 3
2.3 Microsoft Operations Framework ja sen suhde ITIL:iin 4
2.4 Microsoft System Center 2012 Service Manager 6
2.4.1 Service Managerin kehitys 6
2.4.2 Service Managerin käsitteitä 8
2.4.3 Service Managerin prosessit 9
2.4.4 Service Managerin muokkaaminen 10
2.4.5 Palveluluettelo 12
2.5 Orchestrator 12
2.5.1 Orkestrointi, ITIL ja MOF 13
2.5.2 Orchestratorin käsitteitä 13
3 Helsingin kaupungin käyttäjätunnushallinnan automatisoinnin valmistelu 15
3.1 Kaupunginkanslian ict-toiminto 16
3.2 Suunnitelma 16
3.3 Toteutus 17
3.3.1 Hallintapakettien määrittely 18
3.3.2 Palvelutarjouksen luominen 20
3.3.3 Runbookien määrittely 21
3.3.4 Service Managerin konfigurointi 25
3.3.5 Muut toiminnot 29
3.4 Tuotos 30
4 Pohdinta 31
Lähteet 34
Liitteet 35
Liite 1. Alkuperäinen tehtäväluettelo projektisuunnitelmasta 35

1 Johdanto

Helsingin kaupunki on hankkinut aktiivihakemistopalvelun (AD) ylläpidon kolmannelta osapuolelta, joka on tarjonnut käyttäjätunnushallintaan selainkäyttöisen sovelluksen. Julkishallinnolla on hankinnoissaan kilpailuttamisvelvoite. On tunnistettu, että mikäli AD:n ylläpito siirtyy toiselle toimittajalle, käytössä olevan sovelluksen käyttöoikeus lakkaa.

Kaupungilla on olemassa olevat lisenssit Microsoft System Center -tuoteperheeseen, joten opinnäytetyössä halutaan selvittää, voiko käyttäjätunnushallinnan toiminnallisuudet toteuttaa kyseisen tuoteperheen Service Manager- ja Orchestrator-tuotteilla ja automaatioastetta nostaa. Service Manager on service desk -toiminnon toiminnanohjausjärjestelmä, sisältäen mm. häiriönhallinnan, palvelupyyntöjen tiketöinnin ja itsepalveluportaalin. Orchestrator on työnkulkujen ja automaatioiden luomiseen tarkoitettu työkalu. Opinnäytetyön tavoitteena on toteuttaa käyttäjätunnushallintaan proof of concept -tyyppinen versio tunnushallinnasta. Ohjelmistojen asennukset on rajattu opinnäytetyön ulkopuolelle.

Tämän opinnäytetyön keskeisiä termejä ovat palvelunhallinta, ITIL ja käyttäjätunnus. ITIL on alun perin Iso-Britannialle tehty, kansainvälisesti käyttöönotettu it-palveluiden toteuttamista kuvaava kokoelma parhaita käytänteitä. Palvelunhallinta on yksi käyttäjille näkyvimpiä ITIL:n osa-alueita. Palvelunhallinta-termi avataan tarkemmin luvussa 2.

2 Palvelunhallinta

It-organisaatio vastaa sellaisten teknologiaresurssien tarjoamisesta, joita tarvitaan yrityksen tavoitteiden toteuttamiseen. Tällaisia resursseja ovat mm. sovellukset, tiedosto- ja tulostusresurssit, viestintä- ja ryhmätyövälineet, verkot, palvelimet, työasemat ja mobiililaitteet. Työntekijät odottavat, että työvälineet ovat luotettavia, turvallisia, stabiileja ja kustannustehokkaita. He myös tarvitsevat jonkun, johon ottaa yhteyttä tarvitessaan apua. (Meyler ym. 2014a, 11.)

Ei riitä, että nämä resurssit hankitaan niitä tarvitseville. Hankinnat täytyy ennakoida ja suunnitella ja miettiä niiden tukiresurssit. It:n palvelunhallinta on konsepti, jolla järjestetään ja tarjotaan it-kyvykkyydet käyttäjille palveluina. Palvelunhallinnan keskiössä on palvelun käyttäjän näkemys siitä, mitä it tarjoaa yritykselle. Näkökulma eroaa merkittävästi teknologialähtöisestä lähestymistavasta tietohallintoon. (Meyler ym. 2014a, 12.)

Käytännössä it-palvelunhallinta toteutetaan sarjana erikoistuneita prosesseja, joiden avulla it-palvelut tuotetaan ja tuetaan. Prosessit eivät ota kantaa teknologiaan, ja ne jakavat strategiat ja tavoitteet muiden prosessinkehitysjärjestelmien kanssa, kuten Total Quality Management (TQM) ja Six Sigma. It-palvelunhallintaprosessien tavoitteena on vahvistaa it-työn tehokkuutta ja vaikuttavuutta sekä korostaa sen yhdenmukaisuutta liiketoiminnan toiminnallisuus-, suorituskyky- ja kustannusrakennetarpeiden kanssa. (Meyler ym. 2014, 12.)

2.1 Palvelunhallinta ITIL:ssä

Information Technology Infrastructure Libraryn (ITIL:n) mukaan palvelupyyntö on yleistermi erityyppisille vaatimuksille, joita käyttäjät asettavat it-organisaatiolle. Monet pyynnöt ovat usein pieniä muutoksia, joihin sisältyy vain pieniä riskejä ja joita tehdään usein. Tällaisia pyyntöjä ovat esimerkiksi salasanojen muutospyynnöt tai ohjelmistojen asennuspyynnöt. Tällaisten pyyntöjen laajuuden ja luonteen vuoksi ne kannattaa hoitaa mieluummin erillisinä prosesseina. Muutoin ne voivat tukkia häiriön- ja muutoksenhallintaprosesseja. Toimivalla palvelunhallinnalla voidaan parantaa käyttäjien tyytyväisyyttä saamiinsa palveluihin, ja sillä voidaan suoraan vaikuttaa millaisen vaikutelman it-organisaatio antaa yritykselle. (TSO 2011, 86–87.)

Ammattimainen ja tehokas palvelupyyntöjen käsittely lisää käyttäjätyytyväisyyttä. Palvelupyyntöjen käsittelyn avulla voidaan tarjota palvelukanava, josta käyttäjät voivat saada standardoituja palveluita, joihin on jo ennalta määritelty hyväksyntäketjut. Käyttäjät saavat

paremmin tietoa palveluiden saatavuudesta ja menettelytavoista, joilla palveluita voi saada. (TSO 2011, 87.)

Palvelupyynnön täyttämiseen tarvittava prosessi vaihtelee sen mukaan, mitä pyydetään, mutta se voidaan yleensä purkaa sarjaksi suoritettavia aktiviteetteja. Aktiviteetit on hyvä dokumentoida ja taltioida palveluhallinnassa käytettävään tietokantaan. (TSO 2011, 87.)

Joissain organisaatioissa palvelupyynnöt käsitellään häiriönhallintaprosessilla ja sen työkaluilla, jolloin palvelupyyntö on tietyntyyppinen tapahtuma. Varsinaiset palvelupyynnöt erotetaan häiriöistä luokittelun avulla. Ajatuksellisesti näillä on kuitenkin eroa: häiriötapahtuma on yleensä suunnittelematon tapahtuma, kun taas palvelupyyntö voidaan suunnitella ennalta. (TSO 2011, 87.)

Organisaatioissa, joissa on runsaasti käsiteltäviä palvelupyyntöjä, joiden täyttämiseen käytetään erikoistuneita menetelmiä, voi olla hyödyllistä käsitellä palvelupyynnöt erillisessä työjonossa. Samalla pyynnöt saa hallittua erillisenä tietuetyyppinä. Suorastaan välttämätöntä tämä on silloin, kun raportoinnissa on tarpeellista erottaa tarkemmin häiriötapahtumat pyynnöistä tai kun organisaatio päättää laajentaa palvelupisteen toimintaa myös varsinaisen it:n ulkopuolelle. (TSO 2011, 87.)

Palvelunhallinta tuottaa organisaatiolle lisäarvoa tarjoamalla henkilöstölle pääsyn standardoituihin palveluihin, joiden avulla henkilöstö voi parantaa tuottavuutta tai yrityksen palveluiden ja tuotteiden laatua. Samalla olemassa olevien palveluiden saatavuuteen liittyvä byrokratia vähenee, mikä pienentää palveluiden tarjoamisen kustannuksia. Palvelupyyntöjen keskittäminen voi lisäksi mahdollistaa pyydettyjen palvelujen paremman kontrollin, mikä auttaa pienentämään kustannuksia keskitetyillä neuvotteluilla tavarantoimittajien kanssa. Myös it-tuen järjestämisen kustannukset vähenevät. (TSO 2011, 87.)

2.2 Menettelytavat, periaatteet ja peruskäsitteet ITIL:ssä

Palvelupyyntöjen täyttämiseen liittyy useita menettelytapoja. Pyynnön täyttämisessä tulee käyttää ennalta määritettyä prosessia, joka sisältää tarvittavat toiminnot, toimijat ja tavoiteajat. Näin varmistetaan pyyntöjen täyttäminen yhtenäisellä ja tehokkaalla tavalla. Toimintatapa edellyttää, että erityyppiset palvelupyynnöt tunnistetaan etukäteen ja niiden työnkulut mietitään jo palvelua suunniteltaessa. (TSO 2011, 88.)

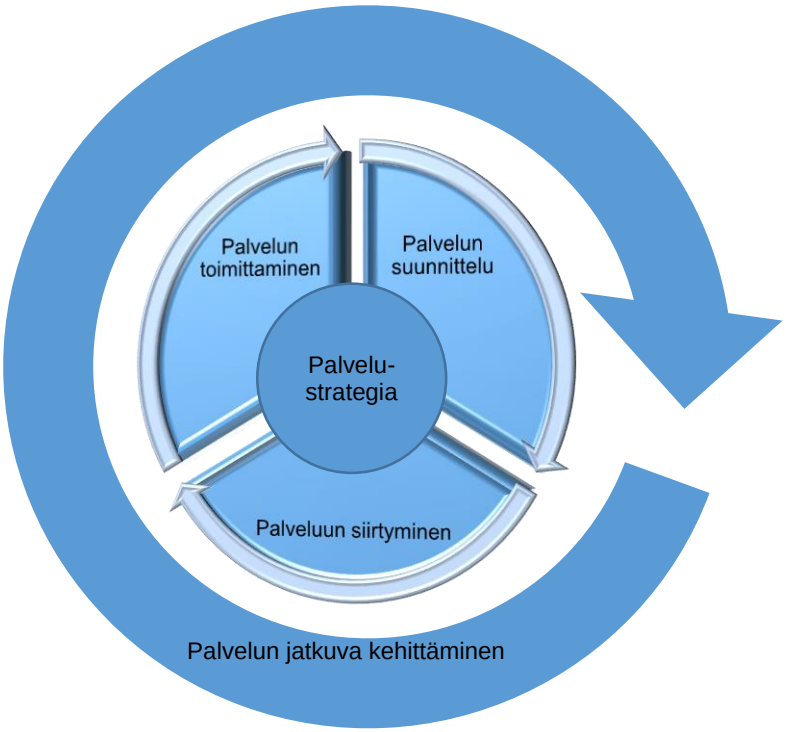
Palvelupyyntöjen omistajuuden tulee sijaita keskitetyssä toiminnossa, kuten service desk -palvelupisteessä. Keskitetyn toiminnon tehtävänä on usein myös suorittaa käyttäjän

pyyntö. Käyttäjällä on vain yksi yhteydenottopiste, josta hän voi palvelun pyytää ja josta hän saa tietoa pyynnön etenemisestä. (TSO 2011, 88.)

Kaikki pyynnöt tulee rekisteröidä ja priorisoida, ja niiden elinkaarta tulee hallita yhdessä järjestelmässä. Tämä tukee yhdenmukaista ja toistettavaa palvelupyyntöjen käsittelyä. Samalla pyyntöjen katoamisen riski pienenee. Kaikilla pyynnöillä tulee olla valtuutus ennen kuin niitä aletaan täyttää. Tällä varmistetaan, että resursseja käytetään tehokkaasti ja vain valtuutetuille pyynnöille. Näin pyynnöt saadaan kytkettyä pääsynhallinnan aktiviteetteihin ja tietoturvapolitiikkaan. (TSO 2011, 88.)

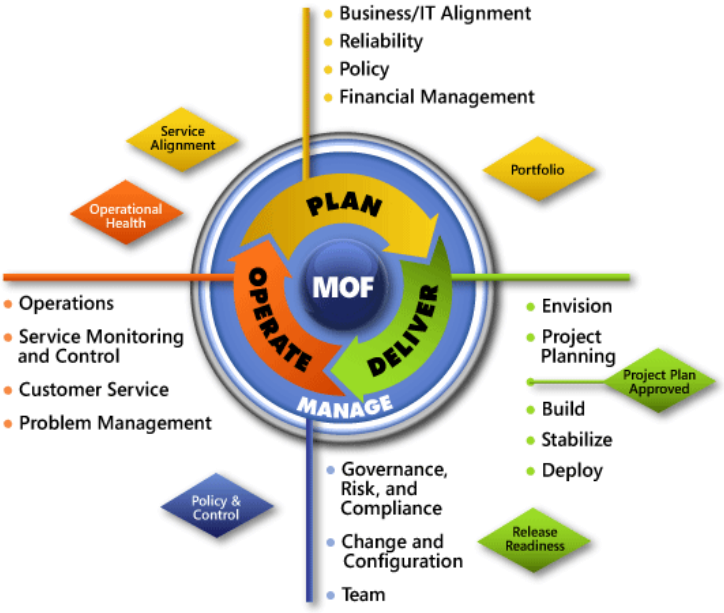
2.3 Microsoft Operations Framework ja sen suhde ITIL:iin

Microsoft Operations Framework (MOF) on Microsoftin kehittämä viitekehys it-palveluiden tuottamiseen. Se kehitettiin alun perin tarjoamaan it-ammattilaisille Microsoftin alustojen hallintaan tarvittavia tietoja ja prosesseja sekä mahdollistamaan järjestelmien korkean tason luotettavuus ja turvallisuus. (van Bon & Dyer 2009, 11.)



Kuvio 1. ITIL:n komponentit (Meyler ym. 2014a, 54)

ITIL:ssä palvelun elinkaaren keskiössä on palvelustrategia (service strategy). Palvelun suunnittelu (service design), palveluun siirtyminen (service transition) ja palvelun toimittaminen (service operation) -komponentit jalkauttavat tätä strategiaa syklisesti (kuvio 1). Palvelun jatkuva kehittäminen -komponentti (continual service improvement) koskee kaikkia syklin vaiheita. (Meyler ym. 2014a, 54.)



Kuvio 2. MOF:n komponentit (van Bon & Dyer 2009, 12)

MOF:ssa palvelun elinkaari muodostuu kolmesta vaiheesta: suunnitteluvaiheesta (plan phase), toimitusvaiheesta (deliver phase) ja tuotantovaiheesta (operate phase). Vaiheiden perustana on hallintakerros, jonka prosesseja sovelletaan palvelun elinkaaren kaikissa vaiheissa (kuvio 2). (van Bon & Dyer 2009, 11.)

Sekä ITIL:ssä että MOF:ssa palvelunhallinnan lähtökohtana on palvelun elinkaari. Molemmissa käytetään prosesseja ja toimintoja. Niiden painotuksissa on kuitenkin eroa. ITIL:ssä monia komponentteja kuvataan prosesseina ja aktiviteetteina, joissa on vain vähän toimintoja. Ero on kuitenkin pienempi kuin miltä alkuun voi näyttää, sillä ITIL:n käsitteellä prosessi kuvataan monia asioita, jotka ovat itse asiassa toimintoja. Suurin ero on, että ITIL keskittyy siihen mitä tehdään, kun taas MOF kattaa sen lisäksi myös miten tehdään. (van Bon & Dyer 2009, 13.)

MOF:ssa palvelunhallintatoiminnon asiakaspalvelu – käytännössä service desk -tiimi – on asiakkaan kontaktipiste kysymyksille ja it-tarpeille. Kuten muutkin tiimit, se voi olla keskitetty, hajautettu tai virtuaalinen. Tiimi toimii yksikkönä, jonka tehtävänä on varmistaa laa-

dukas asiakaspalvelu. MOF:ssa on määritetty terminologia erityyppisille yhteydenottosyille. Terminologiassa on erotettu olemassa olevan palvelun tilaaminen palvelun toteuttamispyynnöksi ja kokonaan uuden palvelun tai ominaisuuden pyytäminen uudeksi palvelupyynnöksi. Kuten ITIL:ssä, myös MOF:n mukaan pyyntö luokitellaan, priorisoidaan ja taltioidaan. (Microsoft 2008, 2–5.)

2.4 Microsoft System Center 2012 Service Manager

System Center 2012 Service Manager on it-palvelunhallinnan ITIL:iin ja MOF:iin pohjautuvien parhaiden käytänteiden käyttöönottoon ja automatisointiin tarkoitettu alusta. Siihen on valmiiksi sisäänrakennettu prosessit häiriönhallintaan, ongelmanratkaisuun, muutoshallintaan, palvelupyyntöjen toteuttamiseen, julkaisunhallintaan, tietämyksenhallintaan ja kokoonpanotietojen hallintaan. Mukana on palveluluettelo, erilaisia mittaristonäkymiä ja raportointi. (Meyler ym. 2014a, 3.)

Service Manager sisältää kokoonpanon hallintatietokannan ja sisäisen prosessimoottorin. Nämä mahdollistavat it-toiminnon tuottamisen palveluna. Service Manager kerää tietoja ja kytkeytyy System Center -tuoteperheen Orchestratoriin, Virtual Machine Manageriin, Operations Manageriin ja Configuration Manageriin sekä aktiivihakemistoon (AD). (Meyler ym. 2014a, 3.)

Toiminnallisella tasolla Service Manager voidaan nähdä ohjelmistoratkaisuna, joka tukee MOF:ssa ja ITIL:ssä määriteltyjä prosesseja. Tekniseltä kannalta katsottuna Service Manager on työnkulkujen hallintajärjestelmä samaan tapaan kuin System Center Operations Manager tai Orchestrator, joihin on MOF-prosessit sisäänrakennettu työnkuluiksi. Työnkulkuja voi laajentaa omien liiketoimintaprosessien mukaisesta, sillä Service Manager tukee laajennoksia kustomoitujen hallintapakettien kautta. (Meyler ym. 2014a, 37.)

2.4.1 Service Managerin kehitys

Microsoft aloitti vuonna 2007 uuden tuotteen kehittämisen koodinimellä Service Desk. Sen tavoitteena oli tarjota MOF-prosesseja tukevia toiminnallisuuksia. Lisäksi sen oli tarkoitus toimia yhdessä muiden Microsoftin tarjoamien it-hallintatuotteiden kanssa. Julkaisu oli suunniteltu vuoden 2008 jälkimmäiselle puoliskolle. (Meyler ym. 2014a, 37.)

Tuote pohjautui Office SharePoint Server 2007 Enterprisen ja SQL Server 2005:n yhdistelmälle. Kehityksen ja testauksen aikana Microsoft totesi, että tuotteen suorituskyky ja skaalautuvuus eivät täyttäneet vaatimuksia. Vuoden 2008 alkupuolella yhtiö päätti julkai-

sun siirtämisestä vuoteen 2010. Samalla Microsoft päätti käyttää System Center Operations Manageria nykyisin Service Managerina tunnetun tuotteen pohjana. Ensimmäinen julkaisu tapahtui kesäkuussa 2010 nimellä System Center Service Manager 2010. (Meyler ym. 2014a, 38.)

Ensimmäisessä versiossa oli toiminnallisuudet häiriönhallintaan, ongelmanratkaisuun ja muutoksenhallintaan. Tuote sisälsi kokoonpanotietokannan, jonka sisältö kerättiin automaattisesti aktiivihakemistosta, System Center Configuration Managerista ja Operations Managerista yhdistimien avulla. Service Manager 2010:een sisältyi itsepalveluportaali, jonka avulla loppukäyttäjät pystyivät tekemään häiriöilmoituksia ja muutospyyntöjä sekä tarkistamaan niiden tilanteen web-sivulta. Portaaliin sisältyi myös analyytikon näkymä muutospyyntöjen tarkasteluun ja hyväksymiseen sekä manuaalisten aktiviteettien suorittamiseen. (Meyler ym. 2014a, 38.)

Microsoft julkaisi joulukuussa 2010 tuotteelle ensimmäisen huoltopäivityksen, joka sisälsi yli 500 bugikorjausta, lisäsi tuettujen kielten määrää ja tuen SQL Server 2008 R2 -tietokantapalvelimelle. Päivitys ei kuitenkaan tuonut tuotteeseen uusia toiminnallisuuksia. (Meyler ym. 2014a, 38.)

Seuraavasta versiosta piti alun perin tulla Service Manager 2010 Release 2 (R2), mutta Microsoft päätti yhdenmukaistaa koko System Center -tuoteperheen nimeämiskäytännöt ja julkaisurytmin. Version nimeksi tuli Service Manager 2012 ja toiminnallisuuksiin lisättiin palvelupyyntöjen toteuttaminen sekä julkaisunhallinta. Versiossa myös mahdollistettiin Orchestrator-integraatio. Näin palvelupyyntötoiminnallisuus pystyi käynnistämään Orchestratorin runbook-työnkulkuja. (Meyler ym. 2014a, 39.)

Hieman Windows Server 2012:n jälkeen Microsoft julkaisi System Center 2012:lle ensimmäisen huoltopäivityksen, joka ensisijaisesti lisäsi tuen uudelle palvelinkäyttöjärjestelmälle ja Windows 8:lle. Integraatiota Operations Managerin kanssa parannettiin päivityksessä ja lisättiin tuki SQL 2012:lle. (Meyler ym. 2014a, 39.)

System Center 2012 R2 julkaistiin lokakuussa 2013 (Microsoft 2013). Versio keskittyy yksityisen pilvialustan hallintaan liittyviin toiminnallisuuksiin ja usean päätelaitteen ympäristöihin. Service Managerin osalta versio sisältää pieniä korjauksia vakauteen ja suorituskykyyn. Versiossa on myös tuki Windows Server 2012 R2:lle ja Windows 8.1:lle. Uusia toiminnallisuuksia Service Manageriin versiossa ei ole mukana. (Meyler ym. 2014a, 39.)

Huoltopäivitysten välillä Microsoft julkaisee pienempiä korjauspaketteja, jotka sisältävät päivityksiä yksittäisiin System Center -tuotteisiin. Korjauspaketti 2:sta alkaen Microsoft on alkanut julkaista korjauspaketteja Service Manageriin ja muihin System Center -tuotteisiin neljännesvuosittain. Näin tuoteperheen toiminnallisuuksia, vakautta ja suorituskykyä voidaan parantaa säännöllisellä julkaisurytmillä. (Meyler ym. 2014a, 39.)

2.4.2 Service Managerin käsitteitä

Kokoonpanotietokanta (configuration management database) on Service Managerin tietokanta, joka sisältää kaikki kokoonpanonimikkeet, työnimikkeet ja tietämysnimikkeet. Se sisältää myös Service Managerin konfigurointiin liittyvät asetukset. (Meyler ym. 2014a, 41.)

Kokoonpanonimikkeet (configuration item, CI) ovat Service Manageriin yhdistimillä tuotuja tai manuaalisesti lisättyjä objekteja, esimerkiksi tietokoneita, ohjelmistoja, käyttäjiä ja AD-ryhmiä. Työnimikkeet (work item) ovat Service Managerin toiminnallisuuksiin liittyviä objekteja, kuten luotuja häiriöilmoituksia, muutospyyntöjä tai palvelupyyntöjä. Tietoartikkelit (knowledge articles) sisältävät työnimikkeisiin liittyvää teknistä dokumentaatiota. (Meyler ym. 2014a, 41.)

Kokoonpano- ja työnimikkeillä sekä tietoartikkeleilla voi olla suhteita toisiinsa. Esimerkiksi kokoonpanonimikkeeseen voi liittyä tietoartikkeli tai työnimike. Kokoonpanonimikkeen tiedoista näkee vaikkapa sen, millaisia häiriöilmoituksia kyseiseen nimikkeeseen liittyy. (Meyler ym. 2014a, 41.)

Hallintapaketit (management packs) ovat xml-tiedostoja, joissa määritellään Service Managerin käyttämät tietomallit ja objektit. Hallintapakettien avulla voidaan muokata muun muassa Service Managerin työnkulkuja, ryhmiä, jonoja, tehtäviä, lomakkeita, yhdistimiä ja konsoli-ikkunaa. Hallintapaketit voidaan suojata muutoksilta sinetöimällä ne salausavaimella. Vain sinetöimättömiä hallintapaketteja voi muokata. Hallintapaketteja käsitellään tarkemmin luvussa 2.4.4 Service Managerin muokkaaminen. (Meyler ym. 2014a, 44.)

Jonoja (queue) käytetään työnimikkeiden ryhmittelyyn erilaisin kriteerein. Jonot ovat pakollisia silloin, kun halutaan hyödyntää Service Managerin palvelutason hallintaominaisuuksia. Kun luodaan palvelutasotavoite, kyseiselle palvelutasolle on määritettävä jono. Jonojen avulla voidaan myös antaa työnimikkeiden käsittelyyn erilaisia oikeuksia. (Meyler ym. 2014a, 47.)

Yhdistimet (connectors) ovat komponentteja, jotka hoitavat Service Managerin tiedonsiirtoa. Service Manager sisältää valmiiksi yhdistimet aktiivihakemistoon, Operations Manageriin, Configuration Manageriin, Orchestratoriin sekä Virtual Machine Manageriin. Muihin järjestelmiin yhdistämistä varten tietoa voidaan tuoda csv-muotoisena csv-yhdistimen kautta. Näiden kautta voidaan tuoda Service Manageriin kokoonpanonimikkeitä. Mukana on myös Exchange-yhdistin, jonka avulla voidaan sähköposti ohjata suoraan Service Manageriin. Sillä ei siis tuoda järjestelmän piiriin kokoonpanonimikkeitä kuten muilla yhdistimillä. (Meyler ym. 2014a, 48.)

Runbookit ovat Orchestratorilla tehtyjä työnkulkuja. Niiden avulla voidaan automatisoida toimintoja, ja ne voidaan käynnistää työnimikkeistä. (Meyler ym. 2014a, 48.)

2.4.3 Service Managerin prosessit

System Center -tuoteperhe on ensisijaisesti tarkoitettu teknologian hallintaan. Service Manager poikkeaa tästä linjasta, sillä se on työn hallintaan tarkoitettu ohjelmisto. Jotta siitä voi saada kaiken irti, on ymmärrettävä myös it-alan tehtävät, joita sillä on tarkoitus hallita. (Meyler ym. 2014a, 53.)

Service Managerin prosessit pohjautuvat MOF:ssa ja ITIL:ssä määritettyihin prosesseihin. Palvelunhallinnan osalta Palvelupyyntöprosessi (service request fulfillment) tarjoaa mekanismin pyyntöjen hallintaan. Prosessin tarkoituksena on tarjota käyttäjälle kätevä, keskitetty pääsy tietoon ja palveluihin sekä täyttää pyynnöt tehokkaasti ja yhdenmukaisesti. (Meyler ym. 2014a, 66.)

Palvelupyyntöjen täyttäminen koostuu kolmesta aktiviteetista. Pyynnön saapuessa se talletioidaan ja luokitellaan. Sen jälkeen varmistetaan hyväksyntä, mikäli sellainen tarvitaan, ja täytetään pyyntö. Lopuksi vielä pyyntö merkitään valmiiksi ja suljetaan. (Meyler ym. 2014a, 67.)

Service Managerin mukana tulee SharePoint-pohjainen itsepalveluportaali, jonka avulla käyttäjät voivat tehdä palvelupyyntöjä ja häiriöilmoituksia, tarkistaa niiden tilannetietoja ja lisätä kommenttejaan. Itsepalveluportaalin käytölle on edellytyksenä palveluluettelo, johon konfiguroidaan ja järjestetään tarjottavat palvelut. Palveluluettelo paketoi häiriöilmoitukset ja palvelupyynnöt pyyntötarjouksiksi, joihin voidaan määritellä käyttäjältä kysyttävät asiat. Pyyntötarjoukset voidaan ryhmitellä kustomoiduiksi palvelutarjouksiksi ja palvelutarjoukset kustomoituihin kategorioihin. (Meyler ym. 2014a, 67.)

Cireson-niminen yritys on tehnyt Service Manageriin HTML5-pohjaisen web-käyttöliittymän, joka toimii kaikilla päätelaitteilla. Cireson on myös kehittänyt itsepalveluportaalin, joka korvaa täysin Service Managerin portaalin. Toisin kuin Service Managerin natiiviportaali, Ciresonin portaali ei vaadi alleen SharePointia. (Meyler ym. 2014a, 624.)

2.4.4 Service Managerin muokkaaminen

Microsoft on tehnyt Service Managerista helposti erilaisiin tarpeisiin muokattavan. Yhtiö myös tarjoaa tyypillisten kustomointien tekoon tarvittavat työkalut. Laajempia, ohjelmointia vaativia muokkauksia varten Service Manager tarjoaa tunnettuja teknologioita hyödyntävän alustan. Service Managerissa on hyödynnetty System Center Operations Managerin modulaarista alustaa, minkä vuoksi se on muokattavissa kaikilla alueilla datakerroksesta työnkulkujen kautta esityskerrokseen saakka. (Meyler ym. 2014a, 686.)

Hallintapaketit ovat xml-tiedostoja, joissa määritellään tietomallit sekä erilaiset objektit, kuten konsolin näkymät, ryhmät, jonot, yhdistimet jne. Hallintapaketin rakenne sisältää eri hallintapakettien väliset suhteet ja hallintapaketin sisältämien resurssien väliset suhteet. Hallintapaketin sinetöinti mahdollistaa sen, että sen sisältöön voidaan viitata toisista hallintapaketeista. (Meyler ym. 2014a, 688.)

Jotta jotain objektia voidaan käsitellä kokoonpanotietokannassa, se täytyy kuvata tietomalissa (data model). Tietomalli koostuu luokkatyypeistä (class type) ja niiden välisistä suhteista (relationship). Uusia luokkatyyppejä luomalla tai olemassa olevia luokkatyyppejä laajentamalla voidaan kokoonpanotietokantaan tuoda sellaisia tietoja ja muita objekteja, joita siellä ei ennestään ole. Objektin ominaisuudet kuvataan käyttäen yhtä tai useampaa luokkatyyppiä. Kullekin ominaisuudelle voidaan määritellä parametreja, esimerkiksi tietotyyppi sekä minini- ja maksimipituus. Näiden parametrien avulla voidaan huolehtia tiedon laadusta. (Meyler ym. 2014a, 690.)

Peritty luokkatyyppi (derived class type) perii kaikki ominaisuudet ja suhteet emoluokkatyypiltä (parent class type). Lähes kaikilla luokkatyypeillä on yhteisiä ominaisuuksia muiden luokkatyyppien kanssa, joten uutta luokkaa luotaessa tai olemassa olevaa laajennettaessa onkin pohdittava, mitä luokkaa käyttää pohjaluokkana (base class). (Meyler ym. 2014a, 691.)

Tietomallin määrityksen jälkeen määritellään tarvittaessa suhteet muihin objekteihin. Suhteen määrityksessä määritellään lähde- ja kohdeluokkatyypit sekä näiden kardinaliteetit.

Kardinaliteetilla tarkoitetaan minimi- ja maksimiarvoja, joiden avulla rajoitetaan eri objektien suhteita toisiinsa. Käytetään esimerkkinä suhdetta, jossa lähdeluokkatyyppinä on työnimike ja kohdeluokkatyyppinä käyttäjä, johon kyseinen työnimike vaikuttaa. Kardinaliteetti minimiarvolla 0 ja maksimiarvolla 1 tarkoittaa sitä, että työnimikkeelle voidaan liittää joko ei yhtään tai korkeintaan yksi käyttäjä, johon nimike vaikuttaa. Kardinaaliteetin arvot 2 ja siitä ylöspäin tarkoittavat rajoittamatonta. (Meyler ym. 2014a, 691–692.)

Suhteita on neljää tyyppiä. Viittaus (reference) on yksinkertaisin: se on kahden objektin välinen yhteys. Kohteella ja lähteellä ei ole muuta riippuvuutta keskenään. Toisen objektin poistaminen poistaa vain yhteyden objektien väliltä. Lähde ja kohde voivat olla mitä tahansa luokkatyyppiä. Sisältö (containment) pohjautuu viittaus-tyyppiin, joten se sisältää kyseisen tyypin ominaisuudet. Lisäksi jos käyttäjällä on oikeus hallinnoida lähdettä, hän automaattisesti saa oikeuden hallinnoida kohdetta. Esimerkiksi jos käyttäjällä on oikeus käsitellä jonoa, hänellä on automaattisesti myös oikeus käsitellä jonon sisällä olevia työnimikkeitä. Jäsenyys (membership) -tyyppi pohjautuu sisältö-tyyppiin ja siis perii kaikki sen ominaisuudet. Lisäksi suhteen kohteella on riippuvuus suhteen lähteeseen: jos lähde poistetaan, myös kohde poistetaan automaattisesti. Jos esimerkiksi työnimikkeeseen liittyy tiedostoliite, mikäli työnimike poistetaan tietokannasta, myös liite poistuu. Isännöinti (hosting) on tyyppi, joka perii jäsenyys-tyypin ominaisuudet (ja siis sisältää samalla viittaus- ja sisältö-tyyppien ominaisuudet). Lisäksi tyyppi sisältää kolme omaa ominaisuutta: Ensinnä kohdeluokka on määriteltävä tyypiksi hosted, mikä tarkoittaa sitä, että kohdetta ei voi olla olemassa ilman isäntää. Toiseksi isännöitävät instanssit jakavat identiteettinsä isännän kanssa – toisin sanoen samalla viittausavaimella voi olla useampia isännöitäviä instansseja, kunhan ne ovat eri isäntien alla. Kolmanneksi suhteen kohde voi olla suhteessa vain yhteen isännöityyn suhteeseen. (Meyler ym. 2014a, 693–695.)

Yhdistelmäluokat (combination class) yhdistelevät tietoa useista objekteista ja esittävät informaation yhtenä objektina. Eräs yhdistelmäluokan käyttötarkoitus onkin tarjota mekanismi, jonka avulla voidaan käyttöliittymässä näyttää toisiinsa liittyviä objekteja samalla lomakkeella. Yhdistelmäluokkia käytetään myös, kun kokoonpanokannasta haetaan tietoa monimutkaisilla kyselyillä. Yhdistelmäluokkia käytetään esimerkiksi Service Managerin käyttöliittymän näkymissä. (Meyler ym. 2014a, 695–696.)

Service Managerin tietosisältöä laajennettaessa siis määritellään tietomalli. Service Manager Authoring Tool -työkalulla luodaan hallintapaketti, johon määritellään joko uusi luokka tai haetaan pohjaksi valmis luokka, jota laajennetaan. Tähän uuteen luokkaan määritellään tarvittavat ominaisuudet eli uudet tietosisällöt ja niiden tietotyypit sekä suhteet muihin hallintapaketteihin tai objekteihin. (Meyler ym. 2014a, 724–736.)

2.4.5 Palveluluettelo

Palveluluettelo on ITIL v3:ssa määritetty käytäntö it-palvelunhallintaan. Palveluluettelo koostuu palvelutarjouksista (service offering), joiden alla on kyseiseen palvelutarjoukseen liittyvät pyyntötarjoukset (request offering). Pyyntötarjouksia luodessa voidaan hyödyntää mallipohjia tai luoda omia malleja. Mallipohjat kannattaa luoda ennen kuin pyyntötarjouksia aletaan luoda. (Meyler ym. 2014a, 308–311.) Koska runbook-työnkulut kytketään mallipohjalle aktiviteeteiksi, kannattaa runbookit puolestaan luoda ennen mallipohjia.

Pyyntötarjoukselle määritetään käyttäjältä kysyttävät kysymykset. Mikäli kysymykseen liittyy lisämäärityksiä, esimerkiksi muotovaatimuksia tai kyselyasetuksia, ne määritetään. Lopuksi kysyttävät kysymykset kytketään pyyntötarjouksen käytettävissä oleviin kenttiin. Lopuksi pyyntötarjous julkaistaan. (Meyler ym. 2014a, 315–321.)

Pyyntötarjouksen luonnin jälkeen luodaan palvelutarjous, johon pyyntötarjous liitetään ja palvelutarjous julkaistaan. Tämän jälkeen palvelutarjous on käytettävissä itsepalveluportaalissa. (Meyler ym. 2014a, 329.)

2.5 Orchestrator

Orchestrator oli alun perin Opalis Software, Inc. -nimisen yrityksen tuote Opalis Integration Server (OIS). Opalis oli johtavassa asemassa it-prosessien automatisoinnissa ja runbook-automatisoinnissa. Microsoft osti yrityksen joulukuussa 2009. Marraskuussa 2010 Microsoft julkaisi viimeisen OIS-nimeä kantaneen version ja System Center 2012 -julkaisusta alkaen tuote nimettiin System Center Orchestratoriksi. (Meyler ym. 2014b, 1.)

Liiketoimintaprosessien automatisoinnissa haetaan hyötyjä yrityksen ydintoiminnalle. Esimerkkinä voi toimia prosessi, jossa päivittäin haetaan web-sivustolle rekisteröityneet henkilöt. Näistä muodostetaan csv-tiedosto, joka lähetetään tiedon laadusta vastaavalle työntekijälle. Tarkistuksen jälkeen tiedot viedään yrityksen asiakkuudenhallintajärjestelmään. (Meyler ym. 2014b, 8.)

It-prosessien automatisoinnilla pyritään puolestaan virtaviivaistamaan rutiininomaisia it-operaatioita, joihin yleensä liittyy manuaalisia vaiheita. Tästä esimerkkinä voi toimia virtuaalikoneiden luonti, sovellusten käyttöönotto ja asetusmuutokset. (Meyler ym. 2014b, 8.)

2.5.1 Orkestrointi, ITIL ja MOF

ITIL-prosessien käyttöönotto on hyvä tilaisuus tarkastella, miten orkestrointi (orchestration) voi tuottaa hyötyjä. Usein it-tiimit organisoidaan vastuualueiden ja osaamisalueiden pohjalta: tietokannat omana tiiminään, virtualisointi omanaan, verkot omanaan. Tiimit ovat siiloutuneita. Orkestroinnilla varmistetaan, että komplekseissa prosesseissa siiloissa suoritettavat tehtävät tehdään oikea-aikaisesti. (Meyler ym. 2014b, 12–13.)

Prosesseja inventoidessa voidaan tunnistaa sellaiset tekniset operaatiot, joita suoritetaan säännöllisesti. MOF on melko lähellä ITIL:iä: molemmissa kuvataan it-palvelunhallinnan parhaita käytänteitä. Microsoft on itse valinnut ITIL:n omien it-operaatioidensa standardiksi sen kuvailevan lähestymistavan vuoksi. Yhtiö kuitenkin suunnitteli MOF:n ohjaavammaksi helpottaakseen Microsoftin omien teknologioiden suunnittelua ja käyttöönottoa. Voidaankin sanoa, että MOF laajentaa ITIL:iä sisältämällä opastusta ja parhaita käytänteitä Microsoftin omien kokemusten pohjalta. (Meyler ym. 2014b, 8–9.)

2.5.2 Orchestratorin käsitteitä

Integraatiopaketti (integration pack) on kokoelma johonkin tuotteeseen tai teknologiaan liittyviä aktiviteettejä. Joissain tapauksissa integraatiopaketti voi sisältää myös yhdistimiä ulkoisiin järjestelmiin. (Meyler ym. 2014b, 67.)

Aktiviteetti (activity) on tehtävä, joka suorittaa spesifin toiminnon. Aktiviteetille voidaan määrittää ominaisuuksia. Esimerkiksi Suorita ohjelma -aktiviteeti suorittaa jonkin ohjelman tai komennon, ja sille voidaan määrittää parametreja ominaisuuksia muokkaamalla. Aktiviteettien välillä on älykäs linkki, jolle voidaan määrittää ehtoja. Orchestrator sisältää suoraan noin 70 aktiviteettia sisäänrakennettuna. (Meyler ym. 2014b, 67.)

Runbook on työnkulku, joka koostuu yhdestä tai useammasta toiminnosta eli aktiviteetistä. Aktiviteettien välillä on älykäs linkki. Orchestrator-ympäristössä voi rakentaa useita runbookeja ja runbookit voivat kutsua toisiaan. Runbookeja voi myös viedä ja tuoda Orchestrator-ympäristöstä toiseen. Runbookin suoritus tapahtuu runbook-palvelimella. (Meyler ym. 2014b, 68.)

Dataväylä (data bus) on avainasemassa runbookin suorituksessa. Dataväylä kuljettaa tietoja aktiviteettien välillä runbookissa. Dataväylä kuljettaa tietoja myös runbookien välillä, kun ne kutsuvat toisiaan. Dataväylää säilytetään sen runbook-palvelimen muistissa, joka runbookia suorittaa. Kun runbookin suoritus on valmis, kaikki kyseiseen runbookiin liittyvä tieto tyhjennetään dataväylältä. Mikäli tietoja tarvitaan myöhemmin, runbook-työnkulun on

suoritettava aktiviteetti, joka tallentaa tiedon johonkin pysyvämpään säilytyspaikkaan, esimerkiksi tietokantaan tai tiedostoon. Dataväylä ei voi myöskään jakaa tietoja sellaisten runbookien välillä, joita ei ole käynnistetty samassa prosessissa. (Meyler ym. 2014b, 69.)

Yhdistimillä (connectors) kytkeydytään ulkoisiin järjestelmiin, esimerkiksi aktiivihakemistoon (AD) tai Exchange-sähköpostipalvelimeen. Kullakin yhteydellä on oma yhdistin. Jos esimerkiksi on muodostettava yhteys neljään eri aktiivihakemistoon, kullekin täytyy konfiguroida oma yhdistimensä. (Meyler ym. 2014b, 71.)

3 Helsingin kaupungin käyttäjätunnushallinnan automatisoinnin valmistelu

System Center -ympäristö Helsingin kaupungilla oli jo valmiina. Projektissa asennettiin Cireson-itsepalveluportaali testausta varten, mutta ohjelmistoasennukset, itsepalveluportaali mukaan lukien, on rajattu opinnäytetyön ulkopuolelle.

Helsingin kaupungin ympäristö on laaja. Kaupungilla on 33 virastoa ja liikelaitosta, henkilöstöä on noin 40 000, työasemia 22 000 ja erilaisia tietojärjestelmiä useita satoja. Työasemaympäristö on Windows-pohjainen ja palvelinympäristö moninaisempi.

Helsingin kaupungin aktiivihakemiston (AD) tekninen ylläpito on ostettu toimittajalta. AD on kaupunkitasoisesti yhteinen. Kullakin virastolla ja liikelaitoksella on AD:ssa oma organisaatioyksikkönsä (OU), joka sisältää viraston käyttäjä- ja tietokoneobjektit ja jota ne itse ylläpitävät. AD:n toimittaja on tarjonnut tietojen ylläpitoon selainkäyttöisen työkalun. Service Manager on tarjottu kaupunkitasoisena järjestelmänä. Se on kuitenkin käytössä vain kolmessa virastossa.

Vuoden 2014 alussa on aloittanut toimintansa ICT-palvelukeskus, jonka vastuualueeseen kuuluu AD:n ylläpito asiakasvirastojensa osalta. Käynnistysvuonna asiakasvirastoja olivat kaupunginkanslia, varhaiskasvatusvirasto sekä sosiaali- ja terveysvirasto. Henkilöstömäärältään virastoissa työskentelee lähes puolet koko Helsingin kaupungin henkilöstöstä (Helsingin kaupunginkanslia 2014). ICT-palvelukeskus on päättänyt liittyä kaupungin Service Manager -järjestelmän käyttäjäksi.

Koko Helsingin kaupungin kattavaa kartoitusta virastokohtaisista toimintatavoista ei tehty. Kaupunginkansliassa on tehty sähköinen InfoPath-lomake, jonka lähiesimies täyttää. Lomake lähtee sähköpostina tietohallintoon, henkilöstöhallintoon ja kulunvalvontaan. Tunnuksen luontia varten tietohallinto tulostaa lomakkeen pdf-muotoon ja tallentaa Service Manageriin pyynnön. Pyynnön tallennuksen jälkeen tietohallinto naputtelee tiedot käsin selainkäyttöiseen tunnushallintatyökaluun, joka varsinaisesti luo tunnuksen.

Sosiaali- ja terveysvirastossa puolestaan lähiesimies tai sihteeri tilaa tunnuksen Word-muotoisella lomakkeella tietohallinnolta, joka taas käsin naputtelee tiedot tunnushallintaan. Pelkästään sosiaali- ja terveysvirastossa tunnushallinnan toimenpiteisiin käytetään päivittäin 2,5 henkilötyöpäivää.

Nykyisessä tunnushallintatyökalussa on myös hakuominaisuus, jolla voidaan hakea AD:n tiedoista käyttäjiä, ryhmiä ja konetilejä ja käsitellä hakutuloksen listauksesta suoraan kyseisiä objekteja. Hakutuloksen saa myös vietyä Excel-muotoon jatkokäsittelyä varten. Hakuja käytetään AD-tietojen ylläpitoon, esimerkiksi käyttäjätunnusten poistamiseen käyttäjän työsuhteen päätyttyä, ja vanhentuneiden konetilien poistamiseen.

3.1 Kaupunginkanslian ict-toiminto

Opinnäytetyön toimeksiantajalla, kaupunginkanslialla, on keskitetty ict-toiminto, jonka vastuualueelle häiriöidenhallinta ja erilaiset it-palvelut, kuten ohjelmisto- ja laiteasennukset ja käyttäjätunnushallinta, kuuluvat. ITIL:n käytänteiden mukaisesti pyynnöt taltioidaan ja priorisoidaan Service Manageriin. Käytössä on kuitenkin vain häiriöidenhallinta-työjono. Tämän vuoksi sen tunnistaminen, että häiriöt eskaloituvat ongelmiksi, vaikeutuu ja työjonosta tulee hankalasti hallittava. Toimintatapana on, että kertaalleen tiketöidystä häiriöstä ei laadita uutta tikettiä uusien ilmoitusten myötä. Työjonon suuruus on kuitenkin jonkin verran aiheuttanut tuplatiketöintiä, kun aiempia samasta asiasta ilmoitettuja tikettejä ei ole havaittu.

Käyttäjille halutaan tarjota enemmän sähköisiä itsepalveluja. Yhdestä ja samasta paikasta hän löytäisi tilauslomakkeen niin ohjelmistoasennukselle kuin rikkoutuneen tilalle hankittavalle hiirelle. Tämä edellyttää, että käyttäjille on tarjota paikka, josta itsepalvelutoiminnot saa, ja että käyttöön saadaan palvelunhallinta-työjono. Samalla saadaan erotettua suunnitellut palvelupyyntötapahtumat ja suunnittelemattomat häiriötapahtumat omiin työjonoihinsa, ongelmatilanteiden laajuus helpommin havaittavaksi ja raportoinnin laatua parannettua.

3.2 Suunnitelma

Tavoitteena oli selvittää, ovatko nykyisen tunnushallintatyökalun toiminnallisuudet toteutettavissa System Center 2012 Service Managerin ja Orchestratorin avulla. Lisäksi tavoitteena oli selvittää, onko automaation astetta mahdollista nostaa nykyisestä. Erityisesti haluttiin mahdollistaa se, että esimies tai hänen valtuuttamansa voi sähköisesti tilata käyttäjätunnuksen, jolloin se luodaan automaattisesti ja tunnukselle kytketään automaattisesti tietyt organisaation perusteella myönnettävät AD-suojausryhmät ja jakeluluettelot. Opinnäytteen ulkopuolelle rajattiin ohjelmistojen asennukset.

Alkuperäisessä suunnitelmassa oli mukana Exchange-postilaatikon ja Lync-oikeuksien tilaaminen. Mukana oli myös virheenhallinta ja lokien määrittely. Alkuperäisen suunnitelman tehtäväluettelo on liitteenä 1.

3.3 Toteutus

Projektin lähtökohtana oli selvittää mahdollisuudet korvata tunnushallintatyökalu Service Managerin avulla. Käyttötapausten tunnistamisessa hyödynnettiin siis nykyisen työkalun toiminnallisuuksia. Tarkasteltavia käyttötapauksia olivat:

- Luo uusi käyttäjätunnus työntekijälle.
- Luo uusi yhteiskäyttötunnus.
- Luo uusi koulutustunnus.
- Luo uusi vierailijatunnus.
- Luo uusi yhteiskäyttöpostilaatikko.
- Luo uusi AD-ryhmä.
- Luo uusi konetili.
- Palauta käyttäjän salasana.
- Muokkaa käyttäjän ryhmäjäsenyyksiä.
- Muokkaa käyttäjän tietoja.
- Etsi käyttäjiä.
- Etsi AD-ryhmiä.
- Etsi konetilejä.

Seuraavissa kappaleissa on kuvattu toteutettuihin käyttötapauksiin liittyvä toteutus.

Työntekijän tunnus muodostetaan käyttäjän sukunimen viidestä ensimmäisestä ja etunimen kahdesta ensimmäisestä merkistä. Mikäli AD:ssa on jo samanniminen tunnus, merkkijonon perässä käytetään juoksevaa numerointia. Lisäksi tarvitaan runsaasti muita tietoja, joita hyödynnetään muissa järjestelmissä. Tiedot viedään aktiivihakemistoon, josta muut järjestelmät ne lukevat. Sähköpostiosoite on muodossa etunimi.sukunimi@hel.fi. Samannimisten henkilöiden kohdalla etu- ja sukunimen välissä käytetään henkilön toisen nimen ensimmäistä kirjainta.

Yhteiskäyttötunnuksia käytetään esimerkiksi kokoustilojen työasemissa sekä yhteiskäyttöisissä sähköpostitileissä ja koulutustunnuksia puolestaan koulutuksissa. Vierailijatunnukset on tarkoitettu kaupungin ulkopuolisten käyttöön, esimerkiksi palvelutoimittajan käyttöön. Tunnistamisen ja ylläpidon helpottamiseksi yhteiskäyttötunnukset alkavat merkkijonolla ”yht-”, yhteiskäyttöisiin sähköpostitileihin liittyvät tunnukset merkkijonolla ”pyht-”, koulutustunnukset merkkijonolla ”kou-” ja vierailijatunnukset merkkijonolla ”ext-”.

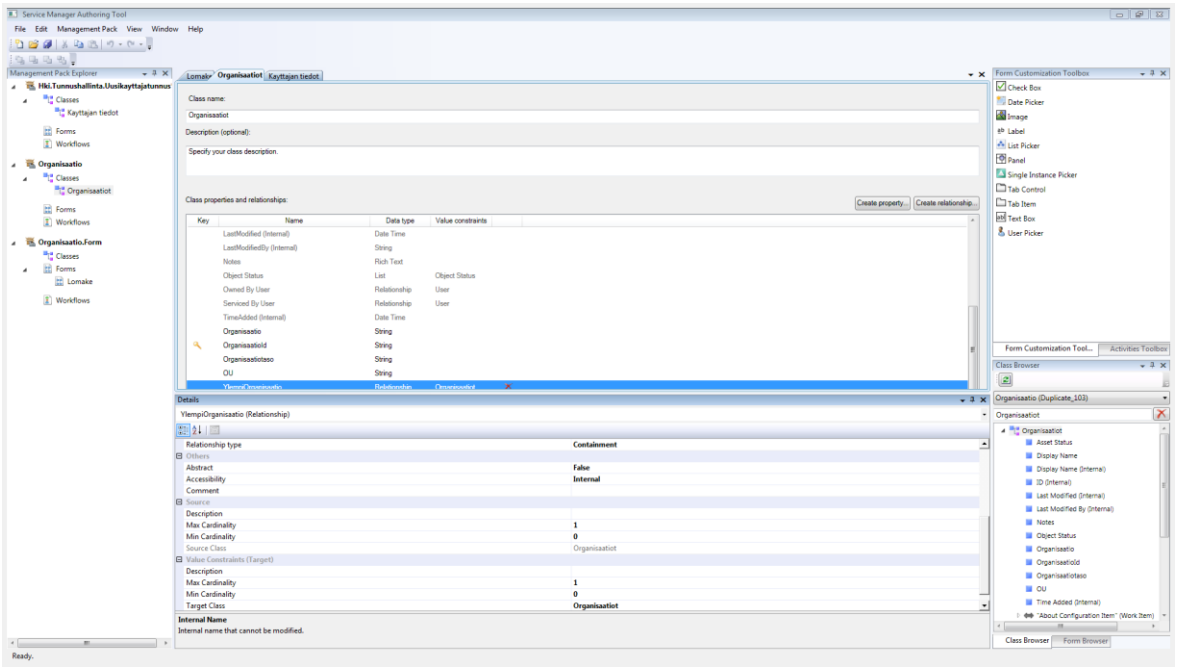
Aiempien testien pohjalta Service Managerin natiiviportaali ei ole osoittautunut kovin käyttäjäystävälliseksi. Esimerkiksi kysyttäviä tietokenttiä mahtuu sivulle vain viisi. Cireson on kehittänyt portaalin, joka korvaa täysin Service Managerin oman itsepalveluportaalin. Työn aluksi päätettiin testata tunnushallinnan toiminnallisuudet Ciresonin portaalilla ja tällä tavoin saada kokemuksia siitä, voiko portaalin ottaa Helsingin käyttöön.

Sosiaali- ja terveysvirastossa (Sote) on määritetty organisaation perusteella määräytyvien AD-suojausryhmien nimeämiskäytäntö. Kaupungin politiikan mukaan ryhmän nimen alussa tulee näkyä virastolyhenne. Soten nimeämiskäytäntö muodostuu vastaavasti organisaation lyhenteistä organisaatiohierarkian alimmalle tasolle asti.

3.3.1 Hallintapakettien määrittely

Ensin määriteltiin kussakin käyttötapauksessa tarvittavat tiedot tietomallia varten. Etenkin uutta työntekijäkäyttäjää luodessa tarvitaan runsaasti sellaisia tietoja, joille ei löydy luontevaa tallennuspaikkaa Service Managerissa. Näitä varten tietokentät on luotava Service Manageriin käyttäen Service Manager Authoring Tool -työkalua, jonka voi ladata Microsoftin kotisivuilta. Työkalun käyttöliittymä on esitetty kuviossa 3. Kaikkia työkaluja ei ole lokalisoitu suomeksi, joten yrittääkseni helpottaa lukemista alla olevassa kuvauksessa englanninkieliset työkalun tekstit ja komennot on kirjoitettu kursiivilla.

Luonti aloitettiin luomalla tyhjä hallintapaketti. Pohjaksi haettiin olemassa oleva *Service Request* -luokka *Class Browser* -ikkunassa kirjastosta *System Work Item Service Request Library*, joka haettiin Management Pack Explorer (MPE) -näkymään hiiren oikealla painikkeella napsauttamalla ja valitsemalla aukeavasta valikosta *View*. *Service Request* -luokka löytyi *Classes*-rakenteesta. Luokan nimeä napsauttamalla oikealla hiiren painikkeella luokkaa pääsi laajentamaan (*Extend class*). Koska Microsoftin tekemä palvelupyyntökirjasto on sinetöity hallintapaketti, valittiin tallennuspaikaksi juuri tehty uusi sinetöimätön hallintapaketti. Lopuksi lisättiin määritellyt tiedot ja niiden tietotyypit *Create property* -toiminnolla. Lopulliselle lomakkeelle tullut sähköpostiprofiilin valintaluettelo määriteltiin tässä vaiheessa käyttäen tietotyyppiä *List*. Tarvittavat suhteet muihin objekteihin periytyivät alkuperäisestä palvelupyyntöluokasta, joten niitä ei tarvinnut erikseen luoda.



Kuvio 3. Käyttäjän tiedot- ja organisaatioluokka sekä organisaatiotietojen syöttölomake luotiin Service Manager Authoring Tool -työkalulla

Organisaatiovalinta haluttiin asteittain tarkentuvaksi kyselyksi. Organisaatiotieto määritettiin tätä varten kokoonpanonimikkeiksi. Ensin luotiin tyhjä hallintapaketti. *Classes*-haarasta hiiren oikealla painikkeella napsauttamalla valittiin *Create configuration item class*. Hierarkkisuus saatiin aikaan muodostamalla *Containment*-tyyppinen suhde organisaatioyksiköstä hierarkiassa ylempänä sijaitsevaan organisaatioyksikköön ja määrittämällä kohderajoitukseksi (*Value Constraints*) kohdeluokaksi (*Target Class*) itse kyseinen luokka. Koska hallintapaketin suhdetta ei tarvita hallintapaketin ulkopuolella, *Accessibility*-ominaisuus määritettiin sisäiseksi (*internal*). Organisaatioyksikkö voi liittyä vain yhteen ylempään organisaatioyksikköön, joten kardinaliteetiksi määritettiin 1. Hallintapaketti tallennettiin, sinetöitiin ja suljettiin.

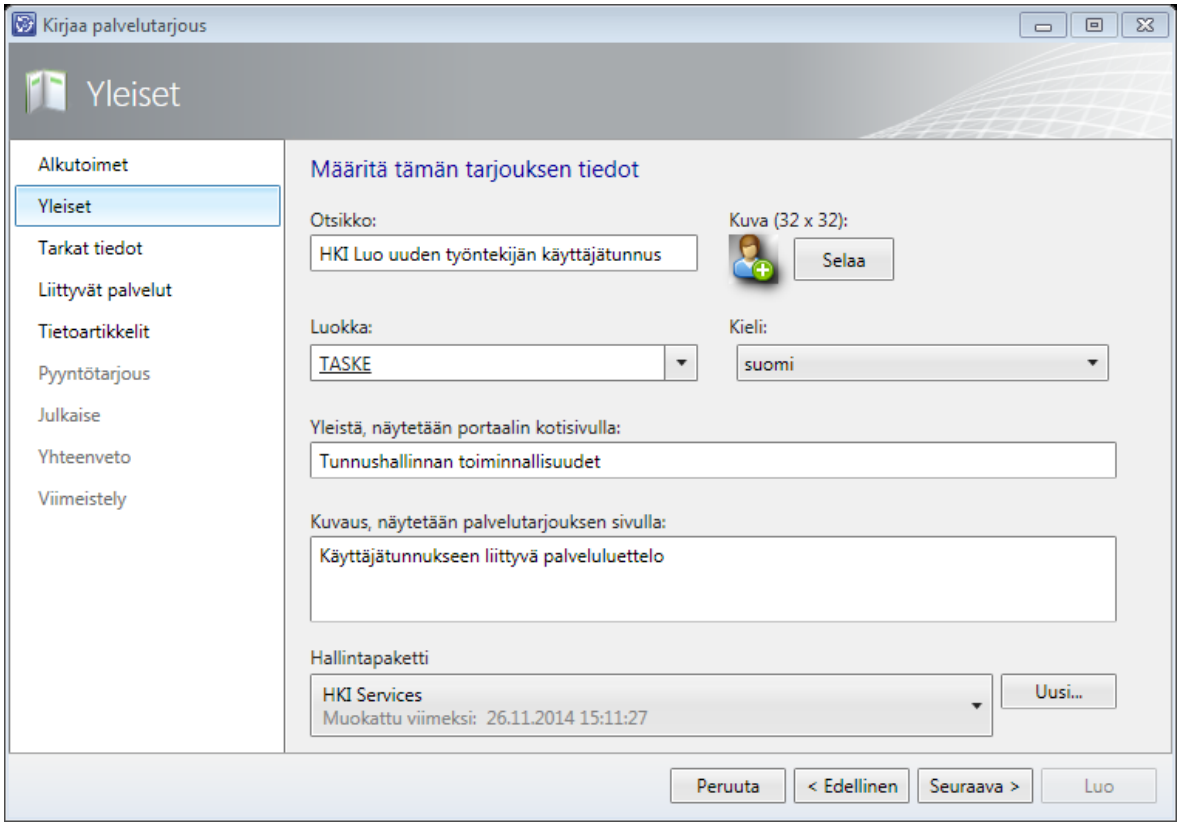
Kuvio 4. Organisaatiotiedon syöttölomake

Seuraavaksi luotiin organisaatiotiedoille kuvion 4 mukainen tietojen syöttölomake. Uuteen, tyhjään hallintapakettiin *Forms*-haarasta valittiin *Create*, jolloin näytölle tuotiin tyhjä lomake. Työkalupaletista tuotiin lomakkeelle *label*-tyyppiset kentät otsikoita varten ja *text box* -tyyppiset kentät tietojen syöttökenttiä varten. Ylemmän organisaation valinta tehtiin *single instance pickerin* avulla. Tämän jälkeen avattiin näytölle sinetöity hallintapaketti, johon organisaatioluokka luotiin. Sinetöidyn hallintapaketin avaaminen näkymään mahdollistaa sen, että tietojen syöttökentät voidaan yhdistää hallintapaketin kenttiin. Yhdistäminen tehdään *Binding path* -ominaisuuden avulla.

Sinetöityä hallintapakettia ei voi muokata eikä saada sinetöimättömäksi, joten hallintapaketeista tallennettiin sekä sinetöity että sinetöimätön, tarvittaessa muokattava versio. Sinetöintiin käytettävä salausavain oli luotu ennalta, joten sen luomista ei käsitellä tässä raportissa. Hallintapaketin sinetöinti tehtiin napsauttamalla hiiren oikealla painikkeella MPE-näkymässä hallintapaketin nimeä ja valitsemalla toiminto *Seal Management Pack*. Hieman yllättäen toimintoa ei löydy ohjelman valikoista.

3.3.2 Palvelutarjouksen luominen

Sinetöidyt hallintapaketit tuotiin Service Manageriin Hallinta-työtilan (workspace) Hallintapaketit-osion toiminnolla Tuo. Sähköpostiprofiilit määriteltiin Kirjasto-työtilan luetteloon ja tarvittava osa organisaatiosta Kokoonpanonimikkeet-työtilassa sijaitsevaan uuteen organisaatioluokkaan, joka hallintapaketissa oli määritelty.



Kuvio 5. Uuden palvelutarjouksen luominen

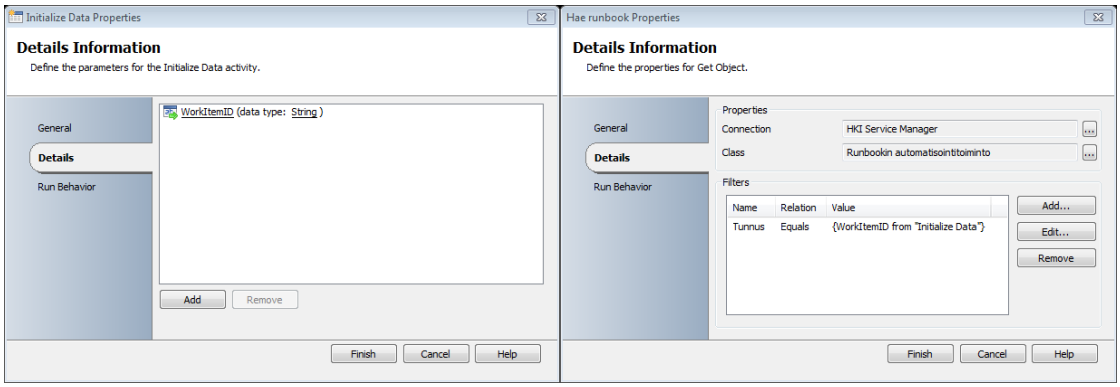
Tämän jälkeen luotiin Kirjasto-työtilassa palveluluetteloon uusi palvelutarjous (service offering) kuviossa 5 näkyvää velhoa käyttäen. Palvelutarjous on käytännössä palveluluettelo, jonka alle yksittäiset pyyntötarjoukset (Request Offering) kerätään. Palvelutarjoukselle määritettiin luokka ja hallintapaketti, johon tarjous tallennetaan. Muita tietoja, kuten mitä pyyntötarjouksia palvelutarjoukseen kuuluu, ei vielä tässä vaiheessa määritetty. Tämän jälkeen palvelutarjous julkaistiin.

3.3.3 Runbookien määrittely

Seuraavaksi luotiin runbook-työnkulut. Runbookit luodaan Runbook Designer -työkalulla ja se asennetaan Orchestratorin asennusmedialta. Orchestrator ei ole vain Service Managerin käyttöön tarkoitettu tuote. Kaikki Service Managerissa tarvittavat runbookit kannattaa rakentaa yhteen kansioon ja tuoda vain kyseinen kansio Service Managerin yhdistimellä. Tällöin Service Manageriin ei tuoda tarpeettomasti muiden järjestelmien käyttöön tarkoitettuja runbookeja. Jotta runbook voi tuoda tai viedä tietoa muihin järjestelmiin, on niiden yhteydet määritettävä Runbook Designerin Options-valikossa. Valikossa (samoin kuin aktiviteeteissa) näkyy vain ne järjestelmät, joiden integraatiopaketit on asennettu.

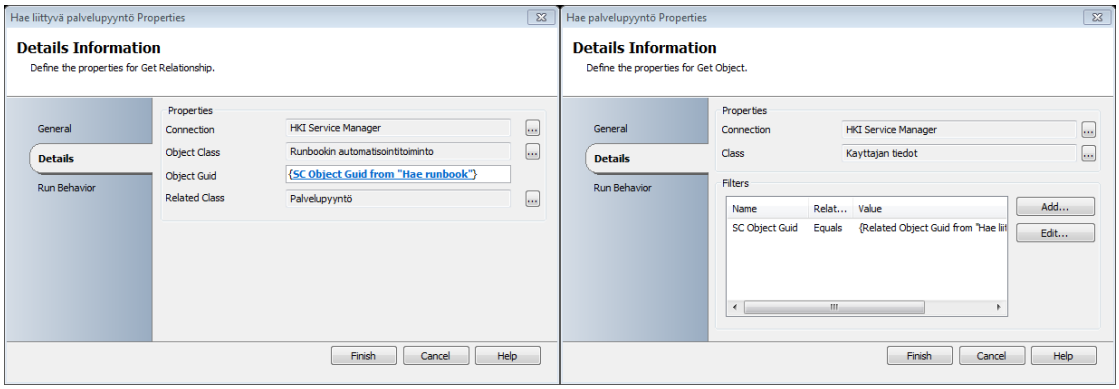
Runbook Designeria ei ole lokalisoitu suomeksi, Service Manager on. Designer hyödyntää Service Managerin omia kirjastoja, mikä johtaa erittäin sekakieliseen käyttäjäkokemukseen. En ole etsinyt toiminnoille englanninkielisiä vastineita, vaan kuvauksessa on käytetty sen kielistä ilmaisua, joka käyttöliittymässä on näkyvillä.

Kun runbook tarvitsee käyttäjän antamia tietoja, sen on alettava tietojen alustus (initialize data) -aktiviteetilla. Aktiviteetilla voi tuoda myös yksittäisiä parametreja. Kukin parametri on määritettävä sekä Orchestratoriin että Service Manageriin. Tietojen runsaus suurentaa riskiä kirjoitusvirheistä parametreissa, joten helpompaa on määritellä yksi parametri, joka tuo koko pyynnön runbookin dataväylään.



Kuvio 6. Aktiviteetit, jotka hakevat palvelupyynnön tunnuksen runbookille

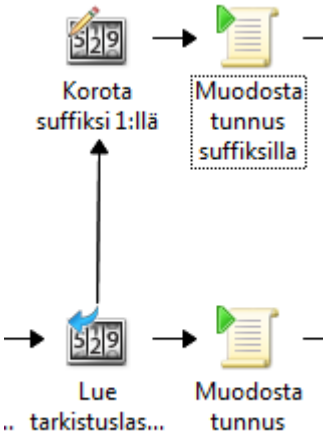
Jotta päästään pyynnön tietoihin käsiksi, tarvitaan useampia hakuja. Aktiviteettien ominaisuudet on esitetty kuvioissa 6 ja 7. *Initialize Data* -aktiviteettiin määritettiin parametri WorkItemID, joka on pyynnön sisäinen tunnus. Seuraavaksi lisättiin Service Manager -aktiviteetti *Get Object*, jolle määritettiin Service Manager -yhteys ja luokaksi määritettiin *Runbookin automatisointitoiminto*. Runbookin dataväylässä kulkevat tiedot (kuten myös muuttujat, jos niitä on määritetty) liitetään suodattimeen napsauttamalla hiiren oikealla painikkeella ja valitsemalla *Subscribe* > *Published Data*. *Value*-kenttään haettiin parametri WorkItemID aktiviteetista *Initialize Data*.



Kuvio 7. Seuraavissa vaiheissa haetaan palvelupyynnön sisältö

Seuraava askel oli *Get Relationship* -aktiviteetti, jolle määritettiin Service Manager -yhteys, objektiluokka *Runbookin automatisointitoiminto*, objektin GUID-kenttään haettiin edeltävän aktiviteetin *SC Object Guid* ja siihen liittyvä luokka *Palvelupyyntö*.

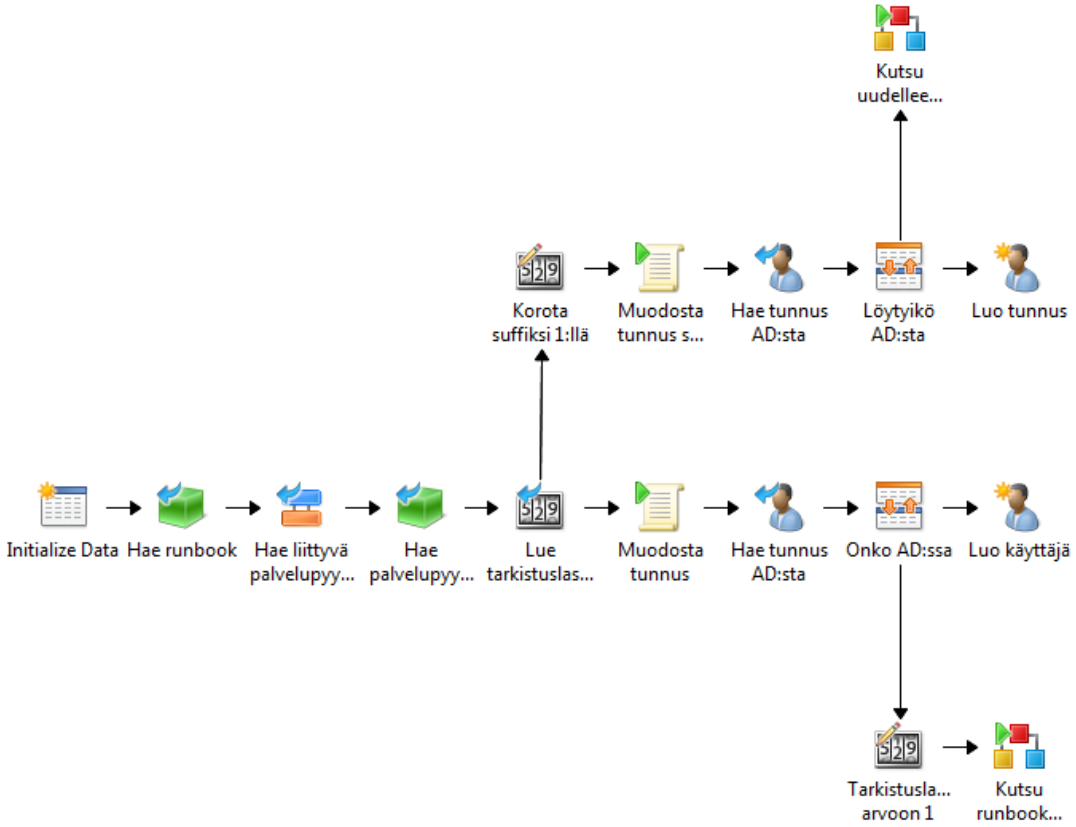
Tämän jälkeen päästiin hakemaan itse palvelupyyntö *Get Object* -aktiviteetilla. Yhteys oli edelleen Service Manager ja luokaksi määritettiin itse tehty laajennettu palvelupyyntö-luokka. Suodattimeksi määritettiin *SC Object Guid* = *Related Object Guid* edelliseltä aktiviteetilta. Tämän jälkeen runbookin dataväylällä kulkee palvelupyynnölle määritettyjen kenttien sisältö.



Kuvio 8. Laskureiden avulla valitaan etenemispolku

Runbookille ei ole mahdollista luoda hyppyjä taaksepäin prosessissa. Näistä tulee syklistä varoittava virhe. Runbook voi kuitenkin kutsua itseään. Tällöin myös tiedot kulkevat dataväylällä. Tätä varten loin kaksi laskuria. Ensimmäinen laskuri tarkistaa onko runbook käynnissä ensimmäisen kerran vai onko se muilla kierroksilla. Mikäli laskurin arvo on nolla eli runbookia suoritetaan ensimmäistä kierrosta, muodostetaan käyttäjätunnus normaalin nimisäännön perusteella (kuviossa 8 alempi polku). Tunnus muodostetaan sukunimi- ja etunimikentistä PowerShell-skriptillä käyttäen *Run .NET Script* -aktiviteettia. Muodostettua tunnusta haetaan AD:sta *Get User* -aktiviteetilla. Kyseisellä aktiviteetilla ei voi käyttää vertailulausekkeita, joten halutun muotoisen arvon saamiseksi käytin vielä *Compare Values* -aktiviteettia. Mikäli tunnusta ei löydy AD:sta, se luodaan. Mikäli tunnus puolestaan löytyy AD:sta, tarkistuslaskuri asetetaan arvoon 1 *Modify Counter* -aktiviteetilla ja kutsutaan runbookia itseään uudelleen *Invoke Runbook* -aktiviteetilla.

Kun tarkistuslaskurin arvo on 1, muodostettavan tunnuksen perään lisätään toisella laskurilla muodostettava juokseva numero (kuviossa 8 ylempi polku). Näin uudelleen muodostettu tunnus haetaan AD:sta samalla menetelmällä kuin edellä on kerrottu. Mikäli tunnusta ei löydy, se luodaan. Mikäli haettava tunnus on AD:ssa, kutsutaan runbookia itseään. Tarkistuslaskuri pysyy arvossa 1, joten tunnussuffiksin laskuria korotetaan taas yhdellä. Polku jatkuu niin kauan kunnes löytyy tunnus, jota ei AD:ssa ole ennestään.



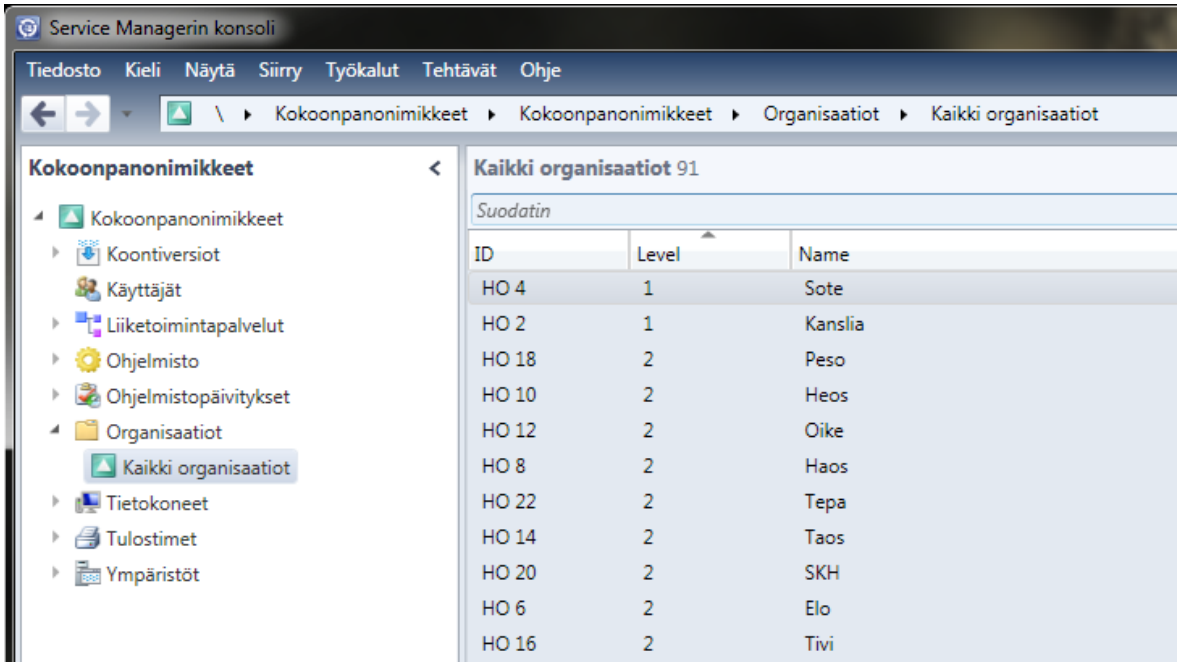
Kuvio 9. Runbook-työnkulku, joka luo uuden työntekijäkäyttäjän tunnuksen aktiivihakemistoon

Kuviossa 9 on esitetty valmis runbook kokonaisuudessaan. Nuolikuviot ovat älykkäitä linkkejä (Smart Links), joille voidaan määritellä kyseiseen aktiviteettiin liittyviä ehtoja. Tässä tarkistuslaskurin ja AD:sta löytymisen arvojen perusteella valitaan etenemispolut.

Yhteiskäyttötunnuksen, koulutustunnuksen, vierailijatunnuksen, AD-ryhmän ja konetilin luonnissa noudatettiin nykyisen tunnushallintatyökalun toiminnallisuutta. Käyttäjältä kysytään luotava tunnus tai nimi. Mikäli se löytyy jo ennestään AD:sta, tilaus menee virhelistalle.

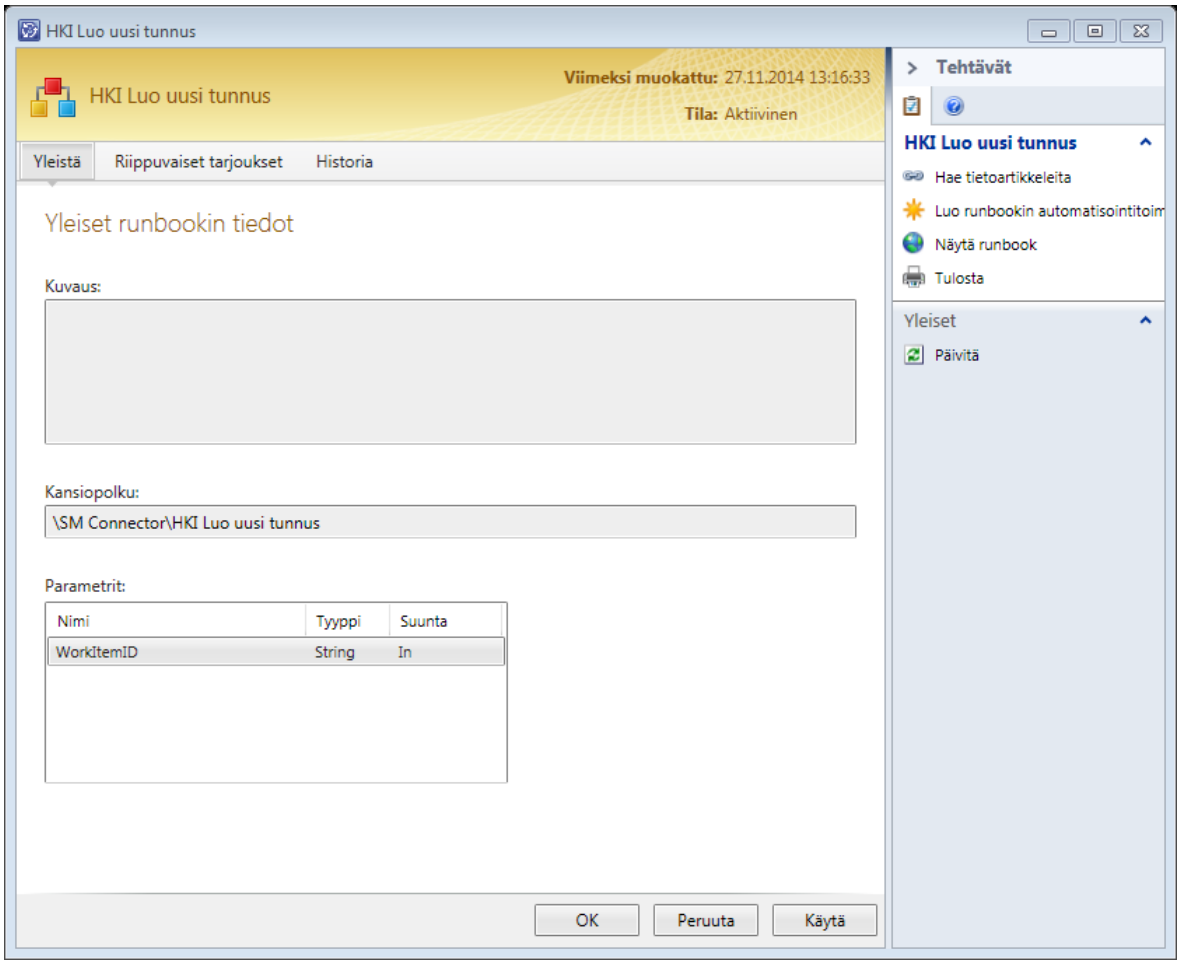
3.3.4 Service Managerin konfigurointi

Organisaatiotietoa varten luotiin Service Managerin Kokoonpanonimikkeet-osioon Organisaatio-kansio, kuten kuviosta 10 voidaan nähdä. Kansioon tehtiin näkymä, joka näyttää kaikki organisaatioluokan kokoonpanonimikkeet. Pohjatiedoksi vietiin kaupunginkanslian ja osa sosiaali- ja terveysviraston organisaatiota.

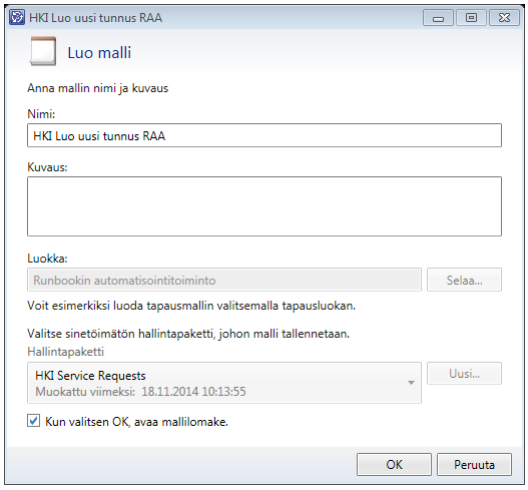


Kuvio 10. Organisaatio-kokoonpanonimikkeet

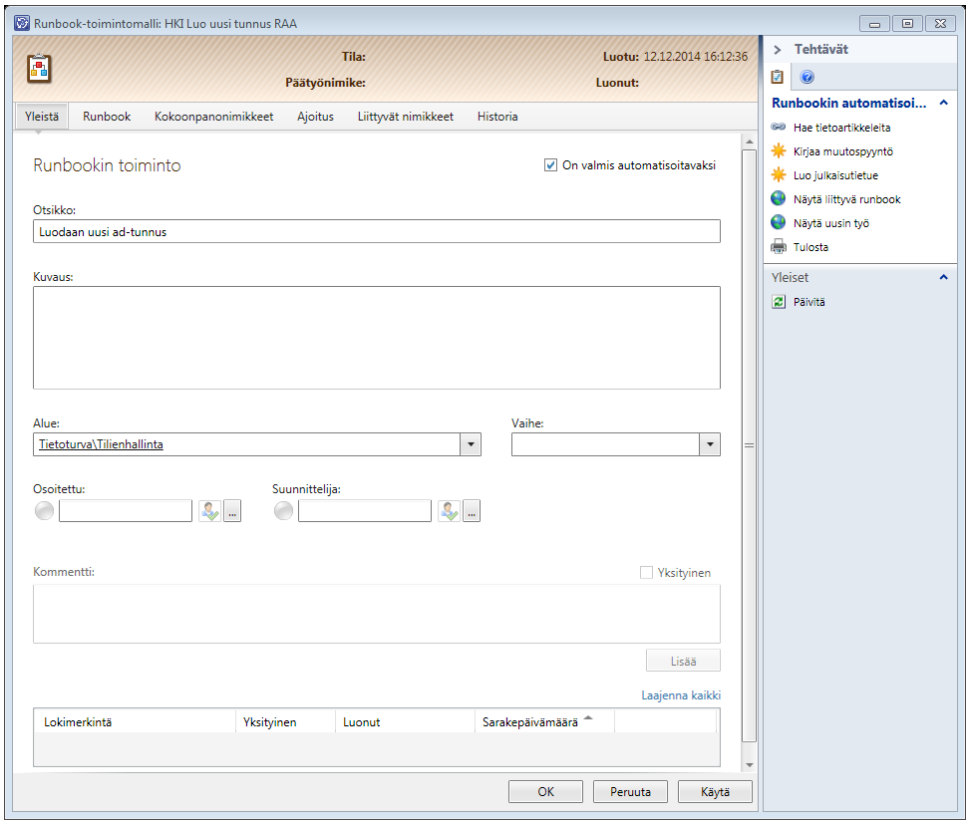
Kun runbook synkronoitui Service Managerin kirjastoon, se avattiin (kuvio 11) ja napsautettiin tehtäväpalkista *Luo runbookin automatisointitoiminnon malli*. Mallille annettiin otsikko ja valittiin hallintapaketti, johon se tallennetaan (kuvio 12). Kaikki mallit tallennetaan kirjastossa samaan paikkaan, joten mallinimessä on hyvä näkyä, että kyseessä on runbookin automatisointimalli. Itse merkitsin otsikon perään kirjainyhdistelmän RAA (Runbook Automation Activity). Erityisen tärkeää on merkitä rasti ruutuun kentässä *On valmis automatisoitavaksi* (kuvio 13). Ilman sitä Service Manager ei saa käynnistettyä runbookia. Runbook-välilehdellä Parametrin yhdistäminen -osiossa Muokkaa yhdistämistä -painikkeen alta valitsin Työnimike-osiosta Id (kuvio 14). Lopuksi tallensin mallin Ok-painikkeella.



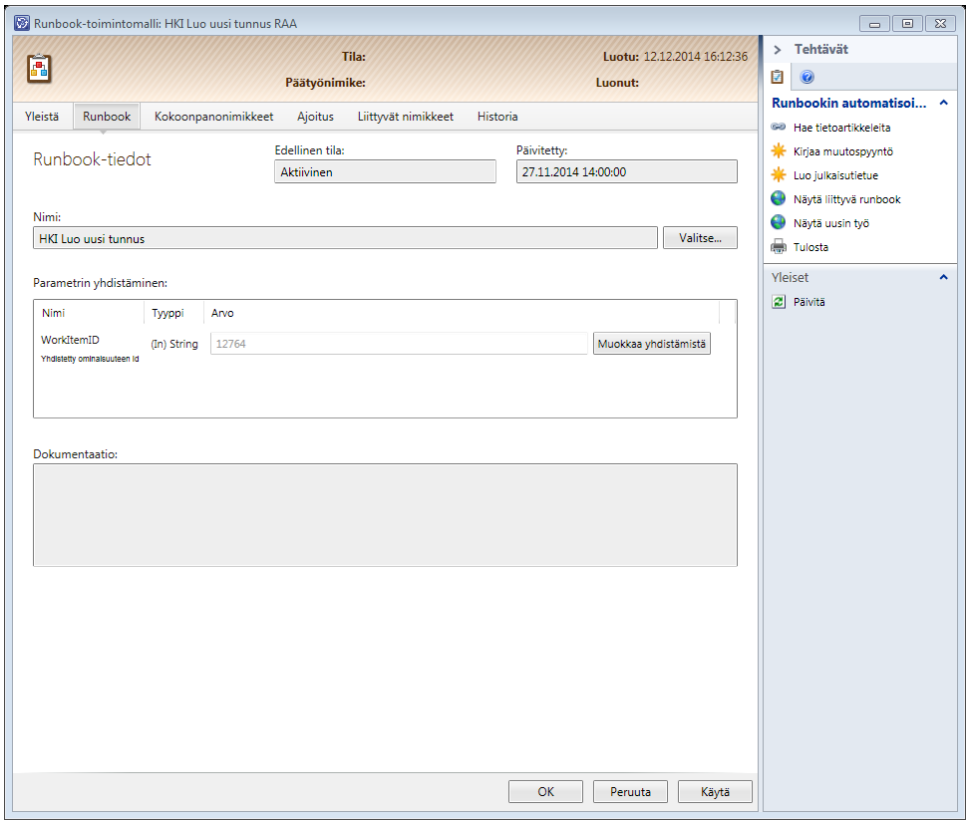
Kuvio 11. Runbook Service Managerin näkymässä



Kuvio 12. Mallin nimeäminen

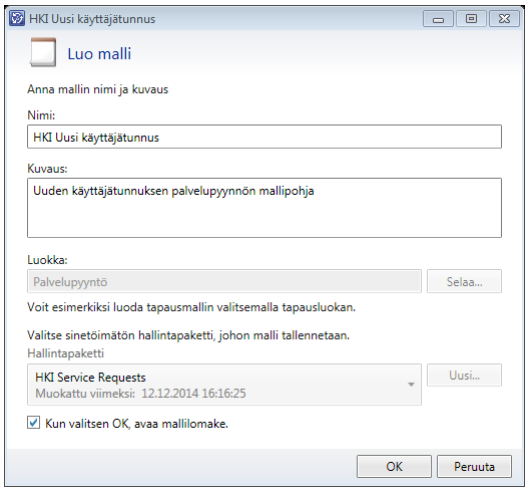


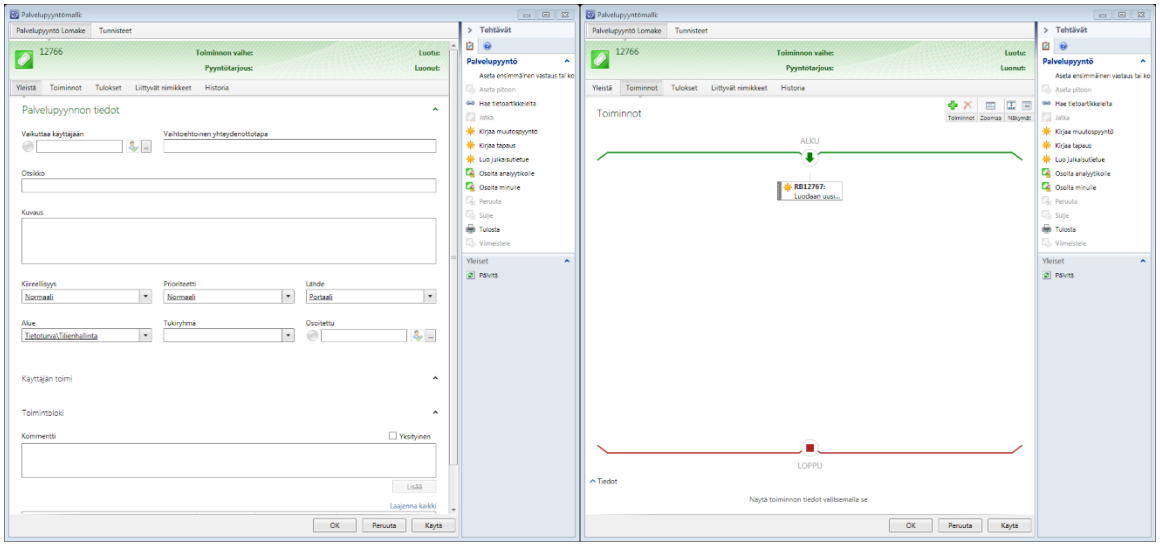
Kuvio 13. Runbook-toimintomalli



Kuvio 14. Saman mallin Runbook-välilehti

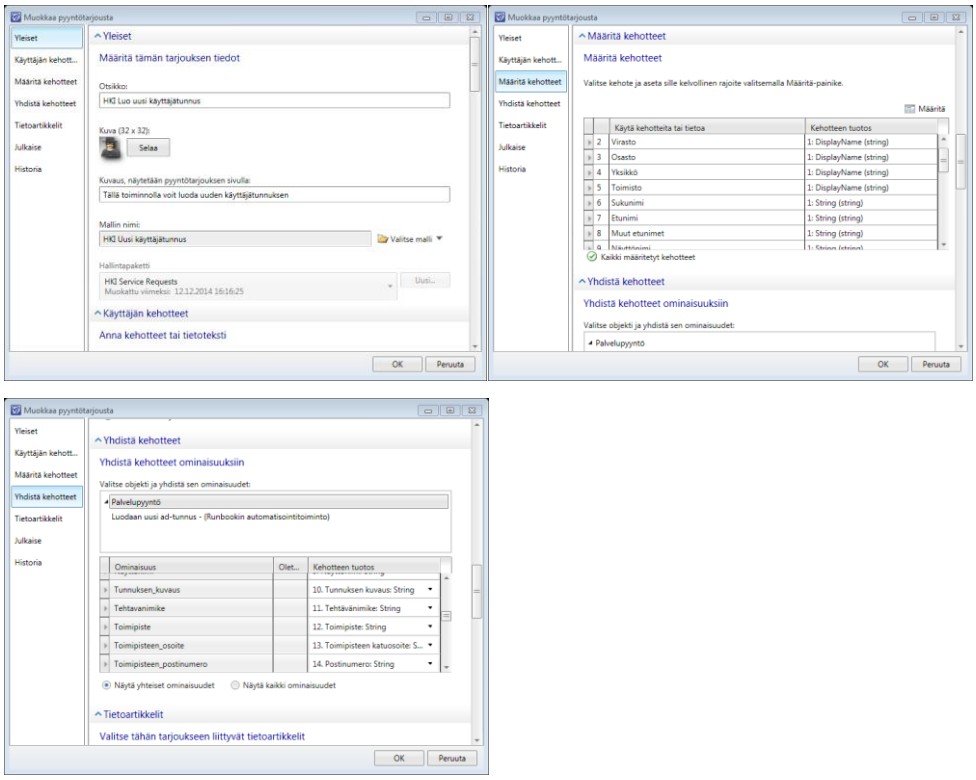
Seuraavaksi luotiin palvelupyynnölle malli. Kirjaston Mallit-kansiossa napsautettiin Luo malli, sille määritettiin nimi, luokaksi Palvelupyyntö ja vielä valittiin sinetöimätön hallintapaketti, johon malli tallennettiin (kuvio 15). Kiireellisyys-, prioriteetti-, lähde- ja alue-luokittelut täytettiin valmiiksi. Toiminnot-välilehdelle lisättiin edellä luotu runbookin automatisointitoiminnon malli. Lopuksi palvelupyyntömalli tallennettiin Ok-painikkeella.





Kuvio 15. Palvelupyynnön mallin luominen

Seuraavaksi luotiin pyyntötarjoukset (kuvio 16). Kirjaston Palveluluettelo-kansion Pyyntötarjoukset-kohdassa valittiin Kirjaa pyyntötarjous. Pyyntötarjoukselle annettiin otsikko ja kuvaus. Malliksi valittiin edellä luotu palvelupyyntömalli. Käyttäjän kehotteet -välilehdelle lisättiin kehotteet kaikille käyttäjältä kysyttäville kentille ja määritettiin niiden tietotyypit. Määritä kehotteet -välilehdellä määritettiin kysely-tietotyypin kyselyt ja kytkennät Service Managerin luetteloihin. Yhdistä kehotteet -välilehdellä yhdistettiin aiemmalle välilehdelle (Käyttäjän kehotteet) määritetyt kentät Ominaisuus-sarakkeesta oman laajennetun palvelupyyntömallin omiin kenttiin Kehotteen tuotos -sarakkeessa. Lopuksi pyyntötarjoukset julkaistiin, jolloin ne tulivat käyttöön myös itsepalveluportaalissa.



Kuvio 16. Pyyntötarjouksen luonnissa täytettyjä osioita

3.3.5 Muut toiminnot

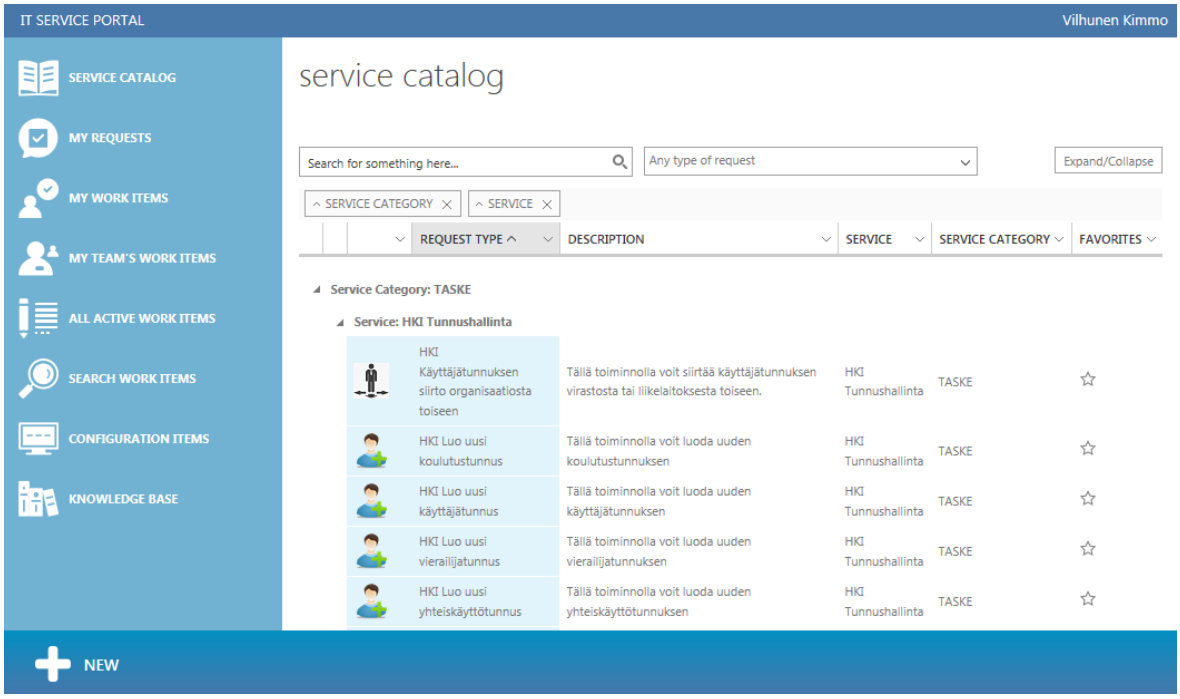
Cireson-itsepalveluportaali ei tue sellaisia hakutoiminnallisuuksia, joissa kyselyehtojen perusteella palautetaan näytölle hakutulos. Näin ollen ei ole mahdollista myöskään hakutuloksen perusteella selata tai muokata kokoonpanonimikkeitä. Lähimmäksi päästään määrittelemällä raportteja, jotka muodostavat ennalta määritettyjen hakuehtojen perusteella dokumentin. Tämä ei ole käytettävyydeltään kovin lähellä nykyistä tunnushallintatyökalua.

Sähköpostin ja Lync-oikeuksien tilaamista toimittajalta ei toteutettu käytännössä. Oikeudet tilataan sähköpostijärjestelmän toimittajalta xml-muotoisella sanomalla käyttäjän tiedoista koostamalla. Runbook-työnkulkuun on helppo lisätä xml-tiedoston muodostamiseen ja toimittajalle lähettämiseen tarvittavat aktiviteetit.

Oletuksena Service Manager synkronoi tiedot aktiivihakemiston kanssa kerran vuorokaudessa. Synkronointiaikataulua on mahdollista muokata PowerShellin avulla, mutta kovin yksinkertaista se ei ole. Tämän seurauksena kokoonpanotietokannan sisältö ei ole reaaliaikainen. Lisäksi Cireson-itsepalveluportaali ei tue näytölle palautettavia hakutuloksia, joita voisi käsitellä. Käyttäjätunnus on tiedettävä tai portaalin käyttäjälle on näytettävä valintalista kaikista tunnuksista, joita hänellä on oikeus käsitellä.

3.4 Tuotos

Tuotoksena syntyi proof of concept -tyyppinen versio tunnushallinnasta, joka kattoi käyttäjätilien, AD-ryhmien ja konetilien luomisen sekä käyttäjän salasanan palauttamisen. Kuviossa 4 on esitetty Cireson-itsepalveluportaaliin luotu palveluluettelo.



Kuvio 17. Palveluluettelon pyyntötarjoukset Cireson-itsepalveluportaalissa

4 Pohdinta

Opinnäytetyön tavoitteena oli toteuttaa käyttäjätunnushallintaan proof of concept -tyyppinen versio tunnushallinnasta. Lisäksi haluttiin selvittää, voiko käyttäjätunnushallinnan toiminnallisuudet toteuttaa System Center -tuoteperheen Service Manager- ja Orchestrator-tuotteilla ja automaatioastetta nostaa.

Tunnushallinnan volyymiltään suurimmat toiminnot eli uuden käyttäjätunnuksen luonti ja käyttäjän salasanan palauttaminen voidaan hyvin toteuttaa Service Managerin ja Ciresonitsepalveluportaalin palveluina, kuten myös uuden AD-ryhmän ja konetilin luominen.

Tunnuksen tietojen muokkaus voidaan myös toteuttaa. Ratkaisu ei ole aivan niin käyttäjäystävällinen kuin nykyinen työkalu: tunnusta ei voida etsiä hakukriteerien perusteella. Tunnus on tiedettävä tai valittava kaikista viraston tunnuksista valintalistalta. Haasteen muodostaa se, että itsepalveluportaalissa esitetään kokoonpanotietokannan sisältöä, ei reaaliaikaista AD-tietoa. Toisaalta nykyinen tunnushallintatyökalu toimii samoin ja samalla synkronointirytmillä. Jotta muutetut tiedot näkyvät heti myös itsepalveluportaalissa esitettävissä tiedoissa, kannattaa runbook määritellä päivittämään muutetut tiedot sekä AD:hen että kokoonpanotietokantaan.

Virhevalintojen välttämiseksi organisaatiovalinta kannattaa toteuttaa niin, että virasto tunnistetaan automaattisesti AD:n Company-kentästä, joka on kaikilla täytetty intranetin toiminnallisuuksien vuoksi. Tämä mahdollistaa sen, että käyttäjä ei voi luoda tunnusta sellaiseen OU-rakenteeseen, johon virastossa ei ole oikeuksia.

Jotta käyttäjälle voidaan liittää automaattisesti oikeat suojausryhmät organisaation perusteella, tiedot on joko määritettävä ohjaustiedoissa jossakin tai muodostettava organisaation nimien perusteella. Suojausryhmien nimeämiseen ei ole yhtenäistä tapaa viraston lyhenteen merkitsemistä lukuun ottamatta. Sosiaali- ja terveysviraston kohdalla organisaatio-kokoonpanonimikkeet muodostettiin suoraan lyhenteillä. Tämän pohjalta on helppo muodostaa liitettävät suojausryhmät. Tämä lähestymistapa kuitenkin edellyttää virastoilta AD:n tietojen siivoamista yhtenäiseen malliin.

Vaihtoehtoisesti organisaatio-hallintapakettiin voi määritellä lisäkentän, johon merkitään sillä organisaatiotasolla käytettävä AD-ryhmä. Tämä lähestymistapa puolestaan tuo runsaasti ylläpitotyötä, joka toistuu organisaatiomuutosten yhteydessä. Tästä syystä organisaation nimen perusteella liitettävät ryhmät ovat suositeltavampia.

Kullekin virastolle kannattaa luoda AD-ryhmä, jonka jäseniksi liitetään ne käyttäjät, joilla on oikeus tilata käyttäjätunnuksia. Kullekin virastolle kannattaa lisäksi luoda oma jono Service Manageriin ja määritellä, että tunnustilauslomakkeet näkyvät vain kyseiselle AD-ryhmälle. Tällä tavoin voidaan varmistua, että tunnuksen tilaajalla on valtuudet tilata AD-tunnus ja erillistä hyväksyntää ei tarvita. Lisäksi, jotta ryhmät ja konetilit saadaan suodatettua kyselyihin järkevästi, kullekin virastolle kannattaa luoda oma yhdistin viraston OU:hun.

Vaikka tunnuksen luontiin tarvitaan joka virastossa samat tiedot, pyyntötarjouksia kannattaa luoda eri tarpeita varten neljä. Yksi lomake, jossa on mukana viraston AD-ryhmien liittäminen organisaation perusteella. Toinen lomake, jossa tätä toiminnallisuutta ei ole. Sen asemesta lomakkeelle voidaan luoda samantyyppinen toiminto kuin nykyisessä tunnushallintatyökalussa: lomakkeella näytetään kaikki viraston suojausryhmät, ja tilaaja valitsee ne, joihin tunnus liitetään. Kolmas ja neljäs lomake ovat ICT-palvelukeskuksen käyttöön. Toiminnallisuudet ovat samat kuin edellä kuvatuilla lomakkeilla, mutta ICT-palvelukeskuksen on pystyttävä valitsemaan virasto, jolle toiminto tehdään ja jonka OU:hun tiedot menevät. Näin virasto voi hyödyntää tunnushallintaportaalia alusta alkaen ja siirtyä käyttämään automaattista ryhmien lisäämistä kun AD:n puhdistus on ehditty tehdä.

Tunnushallinnan toteutuksen myötä käyttöön saadaan palvelupyyntö-työjono. Tämä mahdollistaa virastokohtaisten palveluiden luonnin palveluluetteloon ja sitä kautta häiriönhallinnan ja palvelupyyntöjen erottamisen omiksi kokonaisuuksikseen.

Alkuperäisessä suunnitelmassa oli mukana virheenhallinta ja lokit, mutta lopullisessa tuotoksessa ne jätettiin ulkopuolelle, jotta opinnäytetyön valmistuminen ei viivästy. Virheenhallinnalla tarkoitan runbookeille määriteltäviä aktiviteetteja siinä tapauksessa, että työnkulku kohtaa virheen.

Kaupungilla on runsaasti lakisääteisiä tehtäviä ja viranomaistehtäviä, joissa käsitellään henkilötietoja tai muuta luottamuksellista tietoa. Käyttöoikeuksien jäljitettävyys on erittäin tärkeää. Tietoja on säilytettävä useita vuosia käyttäjän työsuhteen päättymisen jälkeen. Tunnustilaukset tallentuvat palvelupyyntöinä Service Manageriin, mutta tietokannan puhdistus (grooming) poistaa tiedot asetuksissa määritetyn ajan jälkeen. Ratkaisu voisi olla erillinen tietokanta, johon tallentuu tiedot siitä, kuka teki, mitä teki ja milloin. Ratkaisuun tarvitaan myös käyttöliittymä ja käyttöoikeusmääritykset, kuka lokitietoja pääsee lukemaan. Lokien muodostusta on kaiken kaikkiaan tutkittava tarkemmin.

Kaupungilla on Service Managerista vain tuotantoversio. Osa työstä on tehty virtuaalikoneilla ja System Centerin kokeiluversioilla. System Center -tuoteperhe vaatii laitteistolta

runsaasti tehoa ja keskusmuistia: työasema on ollut kovalla koetuksella ja toiminut erittäin hitaasti. Automaatioiden ja palveluiden kehittämistä varten olisikin Service Managerin testiympäristöstä hyötyä. Orchestratoriin voi tehdä testiympäristöön oman yhdistimen, joten Orchestratorissa ei testiympäristöä tarvita.

Service Manager on käytössä vain muutamassa virastossa. Mikäli työkalu halutaan jatkossakin pitää virastoille vapaaehtoisena, itsepalveluportaalin lisäksi tarvitaan myös Cireson Analyst Portal. Muutoin virastot eivät pääse hallinnoimaan virheeseen päätyneitä palvelupyyntöjä.

Opinnäytetyötä tehdessäni opin miten Service Manager ja Orchestrator toimivat yhteen ja miten työnkulkuja kuvataan. Opin myös miksi häiriönhallinta ja palvelunhallinta kannattaa ITIL:n mukaisesti erottaa toisistaan. Opinnäyteprosessi eteni kohtalaisesti. Mittakaavasta johtuen riskinä oli projektin hallitsematon laajeneminen. Toiveiden tynnyristä löytyy aina ammennettavaa, joten on tärkeää priorisoida asiat asetettujen tavoitteiden mukaisesti.

Lähteet

Helsingin kaupunginkanslia. 2014. Henkilöstöraportti 2013. Luettavissa: http://www.hel.fi/static/kanslia/Hera/Henkrapsu2013.pdf. Luettu: 13.11.2014.

Meyler, K, Van Hoecke, K, Erskine, S, Buchanan, S, Bengtsson, A, Svendsen, J, Wilson, K, van Surksum, K, Landman, O, Sundqvist, P & Quagliarello, P. 2014a. System Center 2012 Service Manager Unleashed. Sams Publishing. Indianapolis.

Meyler, K, Zerger, P, Oh, M, Bengtsson, A, Van Hoecke, K, Gauvin, R, Dattilo, N. 2014b. System Center 2012 Orchestrator Unleashed. Sams Publishing. Indianapolis.

Microsoft. 2008. Microsoft Operations Framework 4.0, 4.3 Customer Service SMF. “The Microsoft Operations Framework 4.0 is provided with permission from Microsoft Corporation.” Luettavissa: http://technet.microsoft.com/en-us/library/cc506049.aspx. Luettu: 12.11.2014.

Microsoft. 2013. System Center 2012 R2 Available October 18th. Luettavissa: http://blogs.technet.com/b/systemcenter/archive/2013/08/14/system-center-2012-r2-available-october-18th.aspx. Luettu: 12.11.2014.

TSO. 2011. ITIL Service Operation. TSO. Lontoo.

van Bon, J & Dyer, J. 2009. Cross Reference ITIL V3 and MOF 4.0. Microsoft. “The Microsoft Operations Framework 4.0 is provided with permission from Microsoft Corporation.” Luettavissa: http://www.microsoft.com/en-us/download/details.aspx?id=17647. Luettu: 12.11.2014.

Liitteet

Liite 1. Alkuperäinen tehtäväluettelo projektisuunnitelmasta

Tehtävä
Nykytilan kartoittaminen
Käyttötapausten tunnistaminen
Prosessin määrittely
Luo uusi käyttäjätunnus
Luo uusi yhteiskäyttötunnus
Luo uusi koulutustunnus
Luo uusi vierailijatunnus
Luo uusi yhteiskäyttöpostilaatikko
Luo uusi AD-ryhmä
Luo uusi konetili
Resetoi käyttäjän salasana
Muokkaa käyttäjän ryhmäjäsenyyksiä
Muokkaa käyttäjän tietoja
Prosessissa tarvittavien tietojen määrittely
Luo uusi käyttäjätunnus
Luo uusi yhteiskäyttötunnus
Luo uusi koulutustunnus
Luo uusi vierailijatunnus
Luo uusi yhteiskäyttöpostilaatikko
Luo uusi AD-ryhmä
Luo uusi konetili
Resetoi käyttäjän salasana
Muokkaa käyttäjän ryhmäjäsenyyksiä
Muokkaa käyttäjän tietoja
Postilaatikon tilaus Fujitsulta
xml-tiedoston määrittäminen
Tietokenttien lisääminen Service Managerin hallintapaketteihin
Luo uusi käyttäjätunnus

Luo uusi yhteiskäyttötunnus
Luo uusi koulutustunnus
Luo uusi vierailijatunnus
Luo uusi yhteiskäyttöpostilaatikko
Luo uusi AD-ryhmä
Luo uusi konetili
Resetoi käyttäjän salasana
Muokkaa käyttäjän ryhmäjäsenyyksiä
Muokkaa käyttäjän tietoja
Virastokohtaiset asetukset
Palveluluokkien luonti
Palvelupyyntö-mallipohjan luonti
Virastokohtaisten AD-ryhmien määrittely
Virastokohtaiset lomakkeet mallipohjasta
Käyttöoikeudet virastokohtaisille lomakkeille
Hakujen ja raporttien määrittely
Etsi käyttäjiä
Etsi ryhmiä
Etsi konetilejä
Runbookien luonti
Luo uusi käyttäjätunnus
Luo uusi yhteiskäyttötunnus
Luo uusi koulutustunnus
Luo uusi vierailijatunnus
Luo uusi yhteiskäyttöpostilaatikko
Luo uusi AD-ryhmä
Luo uusi konetili
Resetoi käyttäjän salasana
Muokkaa käyttäjän ryhmäjäsenyyksiä
Muokkaa käyttäjän tietoja
Virheenhallinta
Luo uusi käyttäjätunnus
Luo uusi yhteiskäyttötunnus
Luo uusi koulutustunnus

Luo uusi vierailijatunnus
Luo uusi yhteiskäyttöpostilaatikko
Luo uusi AD-ryhmä
Luo uusi konetili
Resetoi käyttäjän salasana
Muokkaa käyttäjän ryhmäjäsenyyksiä
Muokkaa käyttäjän tietoja
Lokien määritys
Tallennuspaikka
Luo uusi käyttäjätunnus
Luo uusi yhteiskäyttötunnus
Luo uusi koulutustunnus
Luo uusi vierailijatunnus
Luo uusi yhteiskäyttöpostilaatikko
Luo uusi AD-ryhmä
Luo uusi konetili
Resetoi käyttäjän salasana
Muokkaa käyttäjän ryhmäjäsenyyksiä
Muokkaa käyttäjän tietoja