Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2019

Patrik Varnila

YHDEN PISTEEN IDENTITEETINHALLINTA JÄRJESTELMIEN HALLINNASSA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2019 | 38 sivua, 15 liitesivua

Patrik Varnila

YHDEN PISTEEN IDENTITEETINHALLINTA JÄRJESTELMIEN HALLINNASSA

Organisaation kasvaessa käyttäjien identiteetin- ja pääsynhallinnasta tulee entistä tärkeämpää. Se parantaa yrityksen tietoturvaa, auttaa kustannusten hallinnassa sekä helpottaa yrityksen IT-työntekijöiden työmäärää. Identiteetin- ja pääsynhallinta kuitenkin usein laiminlyödään ajatellen, että nykyinen järjestelmä toimii jatkossakin ja että meidän yritys ei sitä tarvitse.

Toimeksiantajayritys on eteläsuomalainen nopeasti viime vuosina kasvanut tietoturva-alan yritys. Jatkuvasti kasvava henkilöstömäärä eri toimipisteissä asettaa haasteita käyttäjien hallinnalle ja tästä johtuu kasvava tarve keskitetylle identiteetinhallinta järjestelemälle.

Tässä työssä käsitellään, mitä identiteetinhallinta on ja sen tärkeyttä. Lisäksi tarkastellaan identiteetin elinkaarta ja identiteetinhallinnan eri osa-alueita. Lopuksi tutustutaan markkinoiden identiteetinhallintajärjestelmiin ja pureudutaan syvemmälle järjestelmään, jonka otetaan käyttöön työn käytännönosuudessa.

Käytännönosuudessa virtualisoiduille palvelimille asennetaan identiteetinhallintaohjelmisto ja sen toiminnan takaamiseksi tarvittavat ohjelmistot ja järjestelmät sekä konfiguroidaan ne siten, että yhdestä pisteestä voidaan hallita useampaa järjestelmää yhtäaikaisesti.

Identiteetinhallintaohjelmiston asennuksen aikana kohdattiin ongelmia, jotka johtivat työn keskeytymiseen. Valittu ohjelmisto ei täyttänytkään kaikkia vaatimuksia ja työn evaluoinnin aikana ongelmaan löydettiin toinen ratkaisu. Työn tuloksena on dokumentaatio, johon on kerätty työvaiheet, jotka tehtiin ennen työn keskeyttämistä.

Teoriaosuuden tavoitteena on ymmärtää ja tutkia identiteetin- ja pääsynhallinnan tärkeyttä ja vaiheita. Käytännönosuuden tavoitteena oli tutustua valittuun identiteetinhallintaohjelmistoon ja sen vaatimuksiin. Työ voidaan katsoa onnistuneeksi, vaikka alkuperäisessä suunnitelmassa ei onnistuttu. Työ johti keskusteluun, jossa löydettiin kaikkia osapuolia tyydyttävä ratkaisu.

ASIASANAT:

identiteettihallinta, tietotekniikka, käyttäjienhallinta, pääsynhallinta

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology

2019 | 38 pages, 15 pages in appendices

Patrik Varnila

ONE-POINT IDENTITY MANAGEMENT IN SYSTEMS MANAGEMENT

As the organization grows, user identity and access management become more important. It improves the company's security, helps manage the costs, and simplifies the workload of the company's IT employees. However, identity and access management are often neglected in the sense that the current system will continue to work and that the company does not need it.

The sponsor company is a security company that has grown rapidly in recent years in Southern Finland. The ever-increasing number of staff at different locations poses challenges for user management, and it causes a growing need for centralized identity management.

This work discusses what identity management is and its importance. In addition, the life cycle of identity and different aspects of identity management are examined. Finally, the identity management systems available on the market are looked at and the introduced system put into practice in the practical part is studied more specifically.

All necessary programs and systems used in the practical part will be installed on virtualized servers and configured so that more than one system can be managed simultaneously from one point.

During the installation of the identity management software, there were problems that led to the project being terminated. The selected software did not meet all the requirements and another solution was found during the evaluation of the work. The result of the thesis is a document, where all steps taken before the termination are collected.

The aim of the theory part is to understand and study the importance and steps of identity and access management. The aim of the practical part was to get acquainted with the selected identity management software and its requirements. The work can be considered successful even though the original plan was not followed through. The work led to a discussion that found a satisfactory solution for all parties.

KEYWORDS:

identity management, user management, information technology, access management

SISÄLTÖ

LIITTEET

KUVAT

TAULUKOT

KÄYTETYT LYHENTEET JA SANASTO

AD	Active Directory – Microsoft Windowsin käyttäjätietokanta ja hakemistopalvelu
IDM	Identity Management – identiteetinhallinta
IAM	Identity and Access Management – identiteetin- ja pääsynhallinta
LDAP	Lightweight Directory Access Protocol – Hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla
IPS	Intrusion Prevention System – tunkeilijan havaitsemisjärjestelmä
OS	Open Source – Avoin lähdekoodi
SLA	Service Level Agreement – Palvelutasosopimus
API	Application Programming Interface – Ohjelmointirajapinta
B2B	Business-to-Business – Yritysmyynti
B2C	Business-to-Customer – Kuluttajamyynti
B2E	Business-to-Employee – Yrityksen tuotteiden myynti työntekijälle
SSO	Single Sign-on – Kertakirjautuminen
RBAC	Role-based access control – Roolipohjainen pääsynhallinta

1 JOHDANTO

Opinnäytetyön tilaaja on IT-alan yritys, joka on erikoistunut kyberturvallisuuteen liittyviin asioihin Suomessa ja maailmalla. Yrityksen suurin vientituote on SOC (Security Operations Center), jossa kellon ympäri päivystävä henkilöstö valvoo eri asiakkaiden tietoteknisiä järjestelmiä suljetussa valvomotilassa.

Kun yritykset kasvavat, useasti myös käytössä olevien tietojärjestelmien määrä kasvaa. Ajan myötä määrältään kasvavien järjestelmien hallinta vaikeutuu ja tietoturva riskit kasvavat. Myös henkilöstön kasvu lisäävät näitä ongelmia.

Tilaajayritys on viime vuosien aikana kasvanut nopeaa tahtia ja henkilöstömäärä on moninkertaistunut näiden vuosien aikana. Tästä syystä heräsi tarve paremmalle identiteetin- ja pääsynhallinnalle. IDM-järjestelmän käyttöönotto helpottaa nykyisten ja tulevien käyttäjien hallinnointia ja järjestelmää eteenpäin kehitettäessä, se myös parantaa yrityksen tietoturvaa.

Tässä opinnäytetyössä käsitellään, mitä identiteetinhallinta on ja mitä osa-alueita siihen kuuluu. Organisaation näkökulmasta tarkastellaan sen hyötyjä ja vaatimuksia. Lisäksi tutustumme karkeasti markkinoiden eri ratkaisuihin. Virtualisoiduille palvelimille asennetaan Windows Server 2012 R2 -käyttöjärjestelmä ja Linux CentOS 7. Tähän käyttöjärjestelmään asennetaan myös LDAP-ohjelmisto Apache Directory Browser sekä identiteetin- ja pääsynhallintaohjelmisto Apache Syncope.

Työn tavoitteena on tutustua identiteetinhallintaan teoriassa ja käytännössä. Tutkitaan identiteetinhallinnan osa-alueita ja elinkaarta, sekä tutustutaan sen hyötyihin ja tärkeyteen. Lisäksi tarkoituksena on kehittää omaa IDM- ja LDAP-palveluiden osaamista ja tietämystä.

Opinnäytetyön toisessa luvussa annetaan perustietoa identiteetin- ja pääsynhallinnasta. Tarkastellaan mm. sen tärkeyttä ja tarkoitusta sekä mitä hyötyä siitä voi olla organisaatiolle. Lisäksi tarkastelemme markkinoilla olevia ratkaisuja.

Kolmannessa luvussa tarkastelemme valittua ohjelmistoa ja sen ominaisuuksia. Osiossa kerrotaan ohjelmiston toiminnasta, mitä ominaisuuksia se sisältää ja mitä vaatimuksia sillä on.

Neljännessä luvussa käydään läpi valitun ohjelmiston testausprosessia, lopputulosta ja mahdollisia ongelmia. Testauksesta kirjoitetaan dokumentti, joka tulee liitteeksi opinnäytetyöhön.

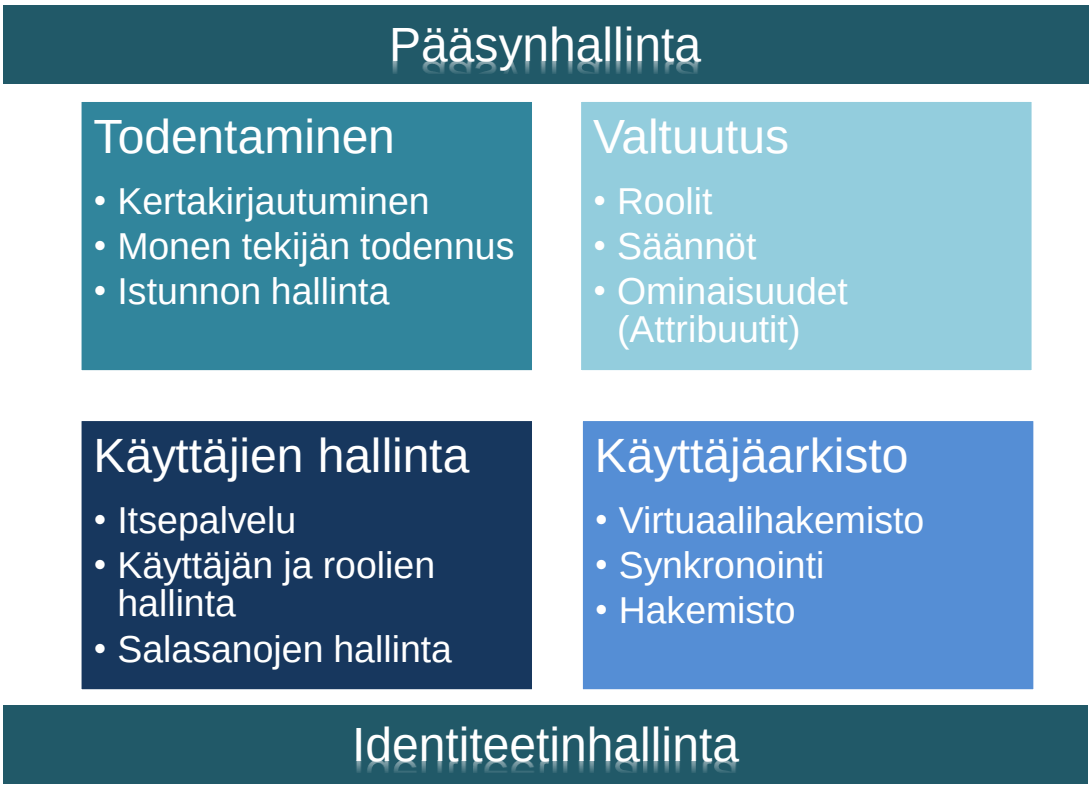
.

2 IDENTITEETIN- JA PÄÄSYNHALLINTA

Identiteetin- ja pääsynhallinta on tärkeä osa nykypäivän yritysten toimintaa. Oikein toteutettuna se laskee kustannuksia, helpottaa hallinnointia ja kasvattaa toiminnallista tehokkuutta. Identiteetinhallinta on prosessi, jossa tunnistetaan, todennetaan ja annetaan oikeudet henkilöille tai ryhmille päästä järjestelmiin, sovelluksiin tai tietoihin. Tämä kaikki täytyy tarjota ilman, että yrityksen tietoturva vaarantuu. Yrityksen vastuuseen kuuluu varmistaa tarjottujen tietojen oikeellisuus, jotta identiteetin- ja pääsynhallinta voi toimia oikein. Identiteetin- ja pääsynhallinnan päätarkoitus on, että ihmiset pääsevät käsiksi tietoon, johon heillä on oikeus (Rouse ym. 2017).

2.1 Identiteetinhallinnan osa-alueet

Identiteetin- ja pääsynhallinta voidaan jakaa neljään eri osa-alueeseen: todentamiseen (Oikeuksien tarkistaminen), valtuuttaminen, käyttäjien hallintaan ja keskitettyyn käyttäjäarkistoon (Hong Kong Polytechnic University). Kuvassa 1 kerrotaan, mitä jokainen osa-alue sisältää.



Kuva 1. Osa-alueet luokittain (Hong Kong Polytechnic University)

2.1.1 Todentaminen

Sähköisistä järjestelmistä puhuttaessa todentaminen (engl. Authentication) tapahtuu käyttäen julkista tunnistetta ja salaisuutta, joka on jaettu todentamisen suorittavan järjestelmän (tästä eteenpäin ”todentaja”) kanssa. Jotta tämä toimii tarkoitetulla tavalla, on identiteetin rekisteröinti suoritettava luotettavalla tavalla. Näin estetään se, että todentajalla ei ole kopiota identiteetistä, eikä kenelläkään toisella henkilöllä ole sitä käytössä.

Todistaakseen identiteetin omistuksen, henkilön täytyy esittää julkinen tunniste (yleensä käyttäjänimi, kuten ”essi.esimerkki”) ja salaisuus (yleensä salasana) jonka vain todentaja tietää. Kun nämä tunnisteet syötetään oikein todentaja vahvistaa, että henkilö on kuka väittää olevansa ja antaa väliaikaisen tunnisteen järjestelmälle, johon henkilö pyrkii pääsemään sisään. Tarjottu tunniste on yleensä voimassa vain niin kauan kuin henkilö käyttää ohjelmaa tai järjestelmää.

Todentaminen ei tee muuta kuin yhdistää henkilön ja tämän sähköisen identiteetin. Se ***ei*** valtuuta henkilöä käyttämään ohjelmaa tai järjestelmää, se yksinkertaisesti todistaa, että henkilö on antanut oikeat tiedot todistaakseen omistavansa kyseisen sähköisen identiteetin (Penn State University Identity Services).

Todentamisen tapoja on monia. Näitä ovat muun muassa:

- **Jotain mitä sinä tiedät:** salasana tai salalause, yleensä jotain minkä henkilö voi muistaa. Tässä on ongelmana, että ne eivät voi olla vaikeita tai pitkiä unohtamisen vaaran vuoksi, ja henkilö voidaan myös huijata antamaan ne hyökkääjälle
- **Jotain mitä sinulla on:** laite, joka sisältää salaisuuden (ns. laitteistotunnuksen) mitä ei voida suoraan antaa hyökkääjälle. Omistajuus todistetaan käyttämällä laitetta ja se antaa väliaikaisen todisteen omistajuudesta todentajalle. Tällaisia ovat esimerkiksi avaimenperälaite, joka näyttää väliaikaisen numerosarjan, joka syötetään todentajan käyttäjäliittymään.
- **Jotain mitä sinä olet:** Sormenjälki, kasvo- tai käsitunniste, väri- tai verkkokalvotunniste, käyttäjän tapaa kirjoittaa tietokoneella tai jotain muuta käyttäjän vakiintunutta käytöstä. Tässä on ongelmana, että kaikilla ei ole olemassa olevaa silmää, sormea, kättä jne. Käyttämisen kaavat ovat yleensä enemmän johdonmukaisia, mutta ne voivat muuttua ajan saatossa ja ovat vielä aikaisessa kehitys vaiheessa käytettäväksi todentamisessa.

2.1.2 Valtuuttaminen

Käyttäjän onnistuneen todentamisen jälkeen järjestelmän täytyy tietää mihin resursseihin käyttäjällä on pääsy ja millä oikeuksilla.

Valtuuttaminen (engl. Authorization) ei ole sama asia kuin todentaminen. Ero on pieni, mutta erittäin tärkeä.

Todentaminen vain todistaa, että henkilö omistaa tämän sähköisen identiteetin eikä mitään muuta. Valtuutus kertoo järjestelmälle onko henkilöllä onnistuessaan todentamisessa oikeuksia päästä järjestelmään (sallia tai estää pääsy) ja mitä oikeuksia hänellä on tehdä järjestelmässä (roolit ja etuoikeudet). Valtuuttaminen tapahtuu vertailemalla resurssin pääsy pyyntöä valtuutus käytäntöön, jotka on varastoitu identiteetin- ja pääsynhallinnan käytäntövarastoon. Valtuutus tarjoaa myös kulunvalvontaa, joka perustuu rooleihin. Pääsynvalvonta, joka perustuu informaatioon ja käytäntöihin, jotka sisältävät käyttäjän roolit, ryhmät, ominaisuudet, toimet, pyydetyt resurssit, ulkoiset tiedot ja yrityksen säännöt on mahdollista valtuutuksella (Penn State University Identity Services).

2.1.3 Käyttäjien hallinta

Käyttäjien hallinta koostuu salasanojen hallinnasta, roolien ja ryhmien hallinnasta sekä käyttäjien ja ryhmien provisioinnista. Käyttäjien hallinta sisältää muun muassa identiteettien luonnin ja käyttäjien identiteetin ja oikeuksien hallinnan. Yksi näistä tehtävistä on käyttäjän identiteetin elinkaaren hallinnointi, jolla yritys voi määritellä kauanko kyseisellä identiteetillä on pääsy yrityksen resursseihin.

Osaa näistä tehtävistä kannattaa hallita keskitetysti, ja osa jättää päätelaitteiden käyttäjille. Hajautettu hallinta auttaa yritystä jakamaan työkuormaa eri osastojen kesken. Hajauttaminen voi myös auttaa, kun vastuun siirtää henkilölle, jota tilanne tai informaatio koskee.

Itsepalvelu on myös tärkeä osa käyttäjien hallintaa. Käyttäjä voi itse päivittää tietojaan, eikä yrityksen tarvitse huolehtia käyttäjätietojen päivittämisestä. Myös salasanan oma nollaaminen on hyödyllinen toiminto, jolla voidaan vähentää huomattavasti helpdeskin työtaakkaa (Hong Kong Polytechnic University).

2.1.4 Keskitetty käyttäjäarkisto

Keskitetty käyttäjäarkisto varastoi ja toimittaa käyttäjätietoja toisille palveluille ja toimii itse palveluna, jossa voidaan tunnistaa käyttäjien antamia tietoja. Keskitetty käyttäjä arkisto esittää yrityksen identiteetit joko ryhmissä tai loogisessa näkymässä. LDAPv3 standardeja käyttävät hakemistopalvelut ovat tulleet hallitsevaksi teknologiaksi keskitetylle käyttäjä hakemistolle. Meta- ja virtuaalihakemistoa voidaan käyttää erilaisten identiteettitietojen hallintaan eri sovelluksien ja järjestelmien tiedostoista. Metahakemisto kokoaa yhteen eri tunnistetietoja ja yhdistelee niitä muista tietojärjestelmistä kerätyistä identiteeteistä. Virtuaalihakemisto yhdistää eri tietokantojen käyttäjätiedot yhdeksi kokonaisuudeksi ja tarjoaa näistä identiteeteistä yhtenäisen LDAP-näkymän.

2.2 Sähköinen identiteetti

Tietotekniikassa sähköisellä identiteetillä tarkoitetaan kohdetta, jota kuvaillaan attribuuteilla. Kohteet voivat olla ihmisiä tai laitteita. Kuvailevia attribuutteja voivat olla muun muassa nimi, käyttäjätunnus, IP-osoite tai domain-nimi. Ihmistä kuvaileva identiteetti on tosielämän projektio järjestelmässä. Esimerkiksi käyttäjätunnus ”EssEsi” kuuluu Essi Esimerkki nimiselle henkilölle (ISO Standardi 24760-1:2011; Rouse, M).

Attribuutit

Identiteetti koostuu monista eri attribuuteista. Attribuutit sisältävät tietoa henkilöstä tai laitteesta, kuten esimerkiksi nimi, ikä ja kotiosoite (Windley Phillip). Attribuuttien liittäminen käytettävään identiteettiin riippuu käyttötilanteesta ja muiden kuin tarpeellisten attribuuttien kerääminen ja tallentaminen on kielletty tietosuojalaissa. (Tietosuojalaki 2018/1050)

2.3 Identiteetin elinkaari

Identiteetti kulkee olemassa olonsa aikana eri vaiheiden läpi. Näitä vaiheita kutsutaan identiteetin elinkaareksi ja ne voidaan jakaa neljään eri osioon, jotka ovat

- identiteetin provisiointi
- identiteetin käyttö
- identiteetin päivittäminen
- identiteetin deprovisiointi.

Hallinnointi on myös osa identiteetin elinkaarta. (Silander 2013, 8–9)

2.3.1 Identiteetin luomisprosessi

Identiteetin luominen koostuu vaiheittaisista prosesseista. Näiden vaiheiden voidaan kuvitella olevan: attribuuttien varmistamisesta, valtuustietojen myöntämisestä ja lopulta varsinaisen identiteetin muodostamisesta. Attribuuttien varmistaminen tarkoittaa jonkin luotetun tahon, esimerkiksi viranomaisen, todistusta käytettävien attribuuttien oikeellisuudesta. Vähemmän säädellyt palvelut, kuten sähköpostipalvelu, saattavat yksikertaisesti luottaa siihen, että käyttäjän syöttämät attribuutit ovat oikeat ilman virallisia todisteita.

Attribuuttien varmistamisen jälkeen siirrytään valtuustietojen myöntämiseen. Riippuen valtuustiedon tyypistä, niitä voi myöntää joko jokin auktoriteetti tai kohde itse. Esimerkkeinä näistä, auktoriteetti voi olla itse organisaatio ja jälkimmäisessä tapauksessa tyypillisin esimerkki lienee salasana, jonka käyttäjä itse valitsee. Valtuustietojen myöntämisen lisäksi tarvitaan vielä jokin tunniste, kuten henkilönumero tai käyttäjänimi, jotta identiteetti voidaan muodostaa (Silander 2013, 9–10).

2.3.2 Provisiointi

Elinkaaren ensimmäinen askel on provisiointi, joka käsittää identiteetin luomisen sekä identiteetin tietojen välittämisen edelleen eri kohdejärjestelmille.

Provisioinnilla voidaan automaattisesti luoda identiteettejä suoraan jostain lähdejärjestelmästä, joka sisältää tarvittavat attribuutit identiteetin luomiseksi kohteelle. Tämä

tehostaa esimerkiksi työhönottoa, kun manuaalisen työnmäärä minimoidaan ja uuden identiteetin käyttöönotto nopeutuu.

Kun kohteelle on luotu identiteetti, täytyy sen tiedot välittää kaikille sen tietoja käyttäville kohdejärjestelmille. Kohdejärjestelmillä tarkoitetaan tässä kaikkia sovelluksia, tietojärjestelmiä tai muita resursseja, jotka tarvitsevat näitä tietoja. Esimerkkejä kohdejärjestelmistä ovat mm. sähköpostijärjestelmä, palkanlaskentajärjestelmä ja tuntiseurantajärjestelmä. Kohdejärjestelmiä voi olla organisaation sisällä kymmeniä tai jopa satoja, jolloin provisioinnin automatisoimisen tärkeys kasvaa (Silander 2013, 10).

2.3.3 Identiteetin käyttö

Identiteetin käyttäminen on ehkä helpoimmin ymmärrettävä aihe identiteetin elinkaaressa. Kohteet käyttävät identiteettejä esimerkiksi eri järjestelmiin todentamiseen ja oikeuttavat niillä erilaisia toimintoja kuten esimerkiksi kirjautumisen työpaikan sisäverkkoon ja pääsyn yrityksen verkkolevyille. Identiteettien käyttö mahdollistaa myös luotetun viestinnän, koska viestinnän osapuolet voivat etsiä, löytää sekä varmentaa muiden identiteettejä. Esimerkiksi sähköpostit on mahdollista allekirjoittaa digitaalisesti, jotta lähettäjän identiteetistä voidaan varmistua ja lisäksi viestit voidaan salata, jos halutaan varmistua niiden luottamuksellisuudesta. Viestinnän lisäksi myös muilla tahoilla, kuten esimerkiksi kulunvalvonnalla, on mahdollista käyttää muiden kohteiden identiteettejä.

Vaikka kaikki mitä identiteetin käyttämisestä on kirjoitettu yllä koskee ihmiskohteita, pätevät samat asiat myös laitteiden ja sovellusten näkökulmasta. Laite voi tarvita identiteettiä, jotta se voi esimerkiksi liittyä verkkoon tai tunnistautua palveluun. Myös laite- ja sovelluskohteiden ulkopuoliset tahot, kuten valvonta- ja raportointijärjestelmä, käyttävät kohteiden identiteettejä seurantaan samaan tapaan kuin henkilöstönhallinta tarvitsee työntekijöiden identiteettejä tuntiseurantaan (Silander 2013, 11).

2.3.4 Identiteetin päivittäminen

Kaikkia identiteettejä joudutaan ajoittain päivittämään, koska osa attribuuteista muuttuu ajan myötä. Roolit, työnkuvat, osoitteet ja monet muut attribuutit voivat muuttua useitakin kertoja identiteetin olemassaolon aikana. Attribuuttien muutokset saattavat vaikuttaa valtuutustietoihin, esimerkiksi roolin tai työnkuvan muuttuessa, kohde voi menettää

valtuuksia ja saada tilalle uusia. Valtuustiedot vaativat päivittämistä myös riippumatta attribuuttien muutoksista, koska valtuustiedoille on usein asetettu jokin voimassaoloaika ja ne täytyy uusia voimassaoloajan loppuun mennessä.

Yleisesti kaikki päivitykset identiteetteihin tulisi tehdä viipymättä, ettei syntyisi tilanteita, joissa kohteella ei esimerkiksi ole oikeutta tehdä tehtäväänsä tai pahemmassa tapauksessa kohteella on edelleen oikeus, jota sillä ei saisi olla. Automaattinen provisiointi auttaa merkittävästi tämän ajantasaisuuden ja yhtenäisyyden saavuttamisessa etenkin ympäristöissä, joissa sekä päivitettäviä identiteettejä ja järjestelmiä on paljon (Silander 2013, 11–12).

Tietojen ajantasaisuuden ohella tärkeää olisi pitää kirjaa kaikista muutoksista, joita identiteetille tehdään. Tämä mahdollistaa sisäisen tutkinnan ja tarkastuksen pitkänkin ajan jälkeen. Ilman kirjanpitoa voi olla vaikea osoittaa, että jollain henkilöllä on ollut jokin tietty valtuustieto jonain tiettynä hetkenä menneisyydessä, mikä on esimerkiksi mahdollistanut jonkin luvattoman toiminnon. Seurantaan liittyen on syytä varmistaa, että identiteetin pääasialliset tunnisteet, esimerkiksi henkilönumero, pysyvät muuttumattomana koko identiteetin elinkaaren ajan.

2.3.5 Identiteetin deprovisiointi

Deprovisiointi liittyy läheisesti provisiointiin ja monissa yhteyksissä se jopa luetaan siihen sisältyväksi. Käyttäjän identiteetin elinkaaren tullessa loppuun, sen avulla identiteetti ja siihen liittyvät tiedot voidaan poistaa. Kuten provisioinnissa, myös deprovisioinnissa voidaan tiedot poistaa kaikista kohdejärjestelmistä yhtäaikaisesti. Käytännön esimerkkinä, kun työntekijä vaihtaa työtehtävää, hänet deprovisioidaan joistain kohdejärjestelmistä, mutta samalla provisioidaan toiseen kohdejärjestelmään osan kohdejärjestelmäidentiteeteistä pysyessä ennallaan. Työsuhteen loppuessa voidaan hänen identiteetti deprovisoida kaikista kohdejärjestelmistä ja tietoturvan näkökulmasta deprovisiointia voidaankin pitää provisiointia tärkeämpänä.

Ilman kattavaa identiteetinhallintaa, jolla voidaan mahdollisesti deprovisioida kaikki käyttäjätunnukset kaikista kohdejärjestelmistä, entisistä työntekijöistä voi tulla mahdollisia tietoturvauhkia. Kun kaikkia entisen työntekijän identiteettejä ei deprovisioida yhdestä paikasta, on riskinä, että järjestelmiin jää ns. unohdettuja identiteettejä, jotka mahdollistavat ulkoisten hyökkääjien pääsyn järjestelmiin. Hukatut, varastetut tai paljastuneet

identiteetit mahdollistavat myös ulkopuolisten pääsyn järjestelmän rajoitettuihin resursseihin, jos identiteettiä tai sen osia ei deprovisioida tällaisen vahingon sattuessa. Hukatut, varastetut tai paljastuneet identiteetit (ts. käyttäjätunnukset ja salasanat) ovat IT-alan yksiä merkittävimpiä tietoturvariskejä ja puutteellinen deprovisiointi korostaa tätä riskiä entisestään (Silander 2013, 12).

2.3.6 Identiteettien hallinnointi

Kaikkia edellä mainittuja tehtäviä, joita identiteeteille tehdään sen elinkaaren aikana, tulisi hallita selkeillä politiikoilla. Identiteettien hallinta on tärkeä osa organisaation sisäistä valvontaa ja jotta vaatimustenmukaisuudet (engl. Compliances) saadaan täytettyä, se on myös suunniteltava ja suoritettava oikein.

Identiteetinhallintaan liittyvät politiikat liittyvät pääosin varmennukseen ja valtuutukseen. Politiikat määrittelevät olosuhteet, jonka perusteilla annetaan kohteiden käyttää identiteettiin pohjautuvia palveluja tai informaatiota. Näitä politiikkoja kutsutaan varmennuspolitiikoiksi ja ne määritelevät vaaditun varmuuden (engl. Assurance) identiteetin kaikille toimille. Esimerkkinä ne voivat määrittää sijainnin tai kohteen, josta yhteyden muodostus on sallittu.

Politiikoiden lisäksi on tärkeää pitää huolta, että jäljitysketjuun (engl. Audit trail) kirjataan identiteetteihin liittyvät muutokset ja toimet. Jäljitysketju sisältää yksityiskohtaiset ja todistettavat toimet, johon identiteetti on ollut osallisena. Tällä tavoin voidaan kiista tilanteita ennaltaehkäistä, koska toimet voidaan jäljittää kuka on tehnyt, missä on tehnyt, koska on tehnyt, mitä on tehnyt ja miksi on tehnyt.

Olivat identiteettipolitiikat ja jäljitysketjut kuinka tahansa hyvin toteutettu, se on kaikki turhaa työtä, jos niille ei ole kunnolla toteutettua valvontaa ja läpikäyntiä. Markkinoilla on tarjolla erinomaisia valvonta- ja raportointityökaluja, jotka reaaliajassa valvovat esimerkiksi käyttöoikeuksia ja identiteeteillä tehtyjä toimia, sekä raportoivat näistä tapahtumista. Ilman valvontaa ja raportointia, useat poikkeamat voidaan havaita liian myöhään tai ne saattavat jäädä havaitsematta kokonaan (Silander 2013, 13).

2.4 Identiteetin- ja pääsynhallinnan tärkeys

Identiteetin- ja pääsynhallinta on tärkeä osa nykypäivän yrityksiä. Käyttäjät vaativat nopeaa ja helppoa pääsyä erijärjestelmiin riippumatta ovatko he kotona, työmatkalla tai toimistossa. Useimmat organisaatiot tiedostavat tarpeen, mutta vastaan tulee haastavat tietoturvavaatimukset. Kyberrikolliset tietävät, että useimmat yritykset mahdollistavat etänä työskentelyn ja pyrkivät saamaan tunnuksia sosiaalisen tiedustelun (engl. Social engineering) myötä ja sitä kautta saada pääsyn järjestelmiin.

Tietohallinto on nykypäivän organisaatioissa hyvin työllistetty. Päivittäin tulee tapahtumia, joissa täytyy muokata käyttäjien oikeuksia. Uusia henkilöitä palkataan ja heidän pääsynsä eri kohdejärjestelmiin täytyy provisioida. Samaan aikaan työntekijöitä lähtee organisaation palveluksesta ja heidän identiteettinsä täytyy deprovisioida kunnolla, jotta vältetään turha tietoturvauhka. Toisen käyttäjän rooli organisaation sisällä muuttuu ja hänen oikeuksiaan täytyy muokata, jotta hänellä on pääsy uuden roolin vaatimiin resursseihin samalla kun poistetaan oikeudet päästä resursseihin, joita käyttäjä ei enää tarvitse.

Näiden vaatimusten täyttämiseen eri järjestelmissä tarvitaan keskitetty identiteetin- ja pääsynhallinnan ratkaisu. Tuotteen täytyy pystyä hallitsemaan useita eri identiteettejä, jotka käyttävät useita eri laitteita päästäkseen käsiksi eri resursseihin. Kulunvalvonta täytyy pystyä toimimaan niin jo olemassa olevissa järjestelmissä, kuin mahdollisesti tulevissa.

Haastavuutta aiheeseen tuo pilvipalvelut ja mobiililaitteet, joiden avulla dataa voidaan jakaa entistä laajemmalle alueelle ja pääsynhallinta vaikeutuu, eikä organisaatio voi enää luottaa ainoastaan palomuureihin ja IPS-järjestelmiin, vaikka nämä ovatkin edelleenkin tärkeä osa yrityksen tietoturvaa.

Oikein toteutettuna, identiteetin- ja pääsynhallinta ratkaisu helpottaa tietohallinnon työtaakkaa ja vähentää kustannuksia. Lisäksi se tarjoaa suojaa kyberhyökkäyksiltä ja parantaa liiketoiminnan tuottavuutta, kun yrityksen resurssit ovat helpommin työntekijöiden saatavilla. (Biztech 2016)

2.5 Identiteetinhallintajärjestelmän toiminnot

Useimmat identiteetinhallintajärjestelmät koostuvat neljästä perusominaisuudesta:

1. Hakemisto, joka sisältää identiteettien tiedot
2. Työkalut, joilla voidaan lisätä, muokata tai poistaa dataa.
3. Järjestelmä, jolla säädetään käyttäjien oikeuksia
4. Jäljitysketju ja raportointi järjestelmä

Käyttäjien oikeuksien hallintaan on perinteisesti liittynyt useita tunnestautumistapoja käyttäjän identiteetin varmistamiseksi, kuten esimerkiksi salasanoja, digitaaliset sertifikaatit ja älykortit. Laitteistotunnus ja älykortit toimivat yhtenä osana kaksivaiheistatunnistautumista, joka yhdistää jotain mitä käyttäjä tietää (esim. salasana) ja jotain mitä käyttäjällä on (esim. avaimenperälaite) varmistaessa käyttäjän identiteettiä. Älykorteissa on sulautettu piiri, joka voi olla joko mikrokontrolleri tai muistisiru (CSO 2018).

2.6 Identiteetinhallinnan toteuttamisen haasteet

Identiteetinhallinta on haastavaa monien olemassa olevien järjestelmien takia. Järjestelmillä voi olla oma datahakemistonsa ja todentamistapansa. Ohjelmistojen käyttämä identiteettidata ei ole välttämättä standardien mukaista.

Onnistuneen identiteetti hallinnan toteuttaminen ei onnistu hetkessä. Se vaatii ennakkotyötä ja suunnittelemista. Todennäköisimmän prosessissa onnistuu organisaatiot, joilla on yhtenäinen strategia hallinnasta ja selkeät tavoitteet projektissa.

Keskitetyssä identiteetinhallinnassa on myös varjopuolensa. Kun kaikkea voidaan hallita yhdestä pisteestä, herättää se myös kyberrikollisten mielenkiinnon. Helpottaessa IT-ylläpitäjän töitä, helpotetaan myös mahdollisen hyökkääjän, kun kaikki toiminnot ovat yhdessä pisteessä. Mikäli järjestelmään murtaudutaan, voi hyökkääjä luoda itselleen korkeimman turvaluokituksen tunnukset ja edetä järjestelmässä pidemmälle ja vaarantaa kaikki organisaation resurssit (CSO 2018).

2.7 Markkinoiden identiteetinhallintajärjestelmät

Markkinoilla on paljon eri valmistajien identiteetin- ja pääsynhallinta ratkaisuja. Ratkaisuja löytyy niin suurilta tekijöiltä, kuten Microsoftilta ja Oraclelta kuten myös pieniltäkin. Myös avoimeen lähdekoodiin perustuvia ohjelmistoja löytyy. Tässä osiossa esitellään lyhyesti kahdeksaa eri vaihtoehtoa, joista osa on kaupallisia ja osa avoimen lähdekoodin. Avoimen lähdekoodin tunnistaa perässä olevasta ”(OS)” merkinnästä.

2.7.1 Microsoft Azure Active Directory

Azure Active Directory on Microsoftin tuottama pilvipohjainen identiteetti- ja pääsynhallinta palvelu.

Azure AD tukee useita avoimia turvallisuusprotokollia, kuten oAuth 2.0, mikä mahdollistaa sen integroinnin kolmannen osapuolen palveluiden kuten esimerkiksi Facebookin ja Googlen kanssa. Azure AD tarjoaa kertakirjautumisen kaikkiin Microsoftin tuottamiin palveluihin, esimerkiksi Office 365, mutta tämä ominaisuus on myös saatavilla suosittuihin ulkopuolisiin ohjelmiin, kuten esimerkiksi DropBox ja Google Apps. Saatavilla on myös natiivi tuki monen tekijän todennukselle (Online Tech).

Microsoft Azure Active Directory -ominaisuuksia:

- Korkea saatavuus. 54 Datakeskusta ympäri maailman takaavat, että kuka tahansa voi käyttää Azure AD:ta. 99,9%:n saatavuus (SLA) kaikille Azuren maksetuille versioille.
- Itsepalvelu toiminnot. Esimerkiksi vastaamalla turvakysymyksiin on mahdollista vaihtaa itse oma unohtunut salasana
- Kattavat turvallisuus- ja aktiviteetti raportit
- Natiivi monen tekijän todennus

2.7.2 Okta Identity Management

Okta on Identiteetin- ja pääsynhallinta palvelu, joka on erittäin joustava. Se kattaa kuusi komponenttia, jotka on rakennettu pilveen ja sopii jokaiselle käyttäjälle.

Okta Identity Cloud on itsenäinen ja neutraali alusta, jossa on työkalut jokaiseen tarpeeseen. Palvelua päivitetään erittäin aktiivisesti, joten mitä tahansa teknologisia edistyksiä yritys tekee, Oktan ratkaisut sopeutuvat niihin.

Identity Cloud myös sisältää laajan valikoiman valmiita yhdistimiä, millä voi turvallisesti synkronoida yrityksen kolmannen osapuolen palveluita.

Okta tarjoaa myös universaalin hakemiston, joka mahdollistaa yrityksen kasvun ilman sen aiheuttamia tietohallinnon ongelmia (Finance Online).

Okta Identity Cloud -ominaisuuksia:

- Kertakirjautuminen
- Adaptiivinen monen tekijän todennus
- API Pääsynhallinta
- Elinkaaren hallinta (Finance Online).

2.7.3 Oracle Identity Manager

Oracle Identity Manager on hallinnollinen ratkaisu, joka tarjoaa itsepalvelun, provisioinnin ja salasanan hallinta palvelut paikallisesti tai pilvessä.

Oracle Identity Manager mahdollistaa yritysten hallita asiakkaiden, yrityskumppaneiden ja työntekijöiden identiteettejä ja käyttöoikeuksia yhdestä pisteestä. Se mahdollistaa näiden käyttäjien hallita itse omia identiteettejään ja muiden käyttäen valtuutettua hallintoa. Yritysten on mahdollista määritellä useita rooleja, kuten IT-ylläpitäjä ja päätekäyttäjä, ja näitä rooleja voi automaattisesti jakaa määrittelemällä eri sääntöjä. Näiden roolien ja pääsypolitiikan avulla, organisaatiot voivat varmistua, että käyttäjätiedot ovat aina automaattisesti ajan tasalla.

Oracle Identity Manager automatisoi identiteetin elinkaaren prosesseja riippumatta siitä onko palvelu paikan päällä vai pilvessä. Automatisoidut palvelut ovat identiteetin provisiointi, päivittäminen ja deprovisiointi. Lisäksi on mahdollista automatisoida salasanojen provisiointi ja käyttöoikeuksien antaminen / poistaminen (Oracle Technology Network).

Oracle Identity Manager -ominaisuuksia:

- Käyttäjän hallinta: Oracle Identity Manager tarjoaa web-pohjaisen käyttöliittymän, mistä pystyy hallitsemaan omaan identiteettiin liittyviä asioita. Liittymästä pystyy mm. päivittämään identiteetin tietoja, mikä vähentää IT-ylläpitäjien työmäärää. Liittymästä voi laittaa palvelupyyntöjä, jos esimerkiksi käyttäjän rooli täytyy vaihtaa
- Salasanan hallinta: Yksi yritysten yleisempiä ongelmia nykypäivänä. Oracle Identity Manager voi luoda sarjan vaikeita ja muokattavia kysymyksiä, joihin vastaamalla käyttäjä voi nollata oman salasanansa. Oraclen mukaan suurin osa helpdesk soitoista koskee salasanojen nollaamista ja käyttäjätunnusten lukkiutumisen poistoja, joten tämä vähentää näitä soittoja huomattavasti
- Politiikkojen ja työnkulun hallinta: Näiden avulla automatisoida bisnes ja IT prosesseja, jotka parantavat tehokkuutta, turvaa ja kustannustehokkaampi määräysten seuraaminen (Oracle Technology Network)

2.7.4 Auth0

Auth0 on todentamisen ja valtuuttamisen hallinnointi alusta palvelu, joka on saatavilla verkkosovelluksille sekä IoT- ja mobiililaitteille. Universaali identiteetti alusta yrityksille tukee B2B, B2C, B2E ja näiden yhdistelmiä. Alusta tarjoaa adaptiivinen monikerroksisen turvan ja siinä on vankka arkkitehtuuri turvallisuuden parantamiseksi. 1,5 miljardia kirjautumista kuukausittain ja 1,3 miljoonaa haitallista kirjautumista estettynä, alusta on aina valmis ja lupaa erittäin korkeaa saatavuutta. Alusta toimii hyvin kehittäjien kanssa yhteistyössä ja antaa heidän tunnistaa API:ta ja ohjelmia monilla eri identiteetin tarjoajilla eri alustoilla. Ohjelmisto ratkaisu käyttää myös edistyneitä teknologioita ja parhaita käytäntöjä auttaakseen asiakkaita mukautumaan tiukkoihin alan asetuksiin ja standardeihin (Finance Online).

Auth0 -ominaisuuksia:

- Auth0 tekee kertakirjautumisesta yksinkertaista ja sallii yritysten antaa niiden kumppaneille, työntekijöille ja asiakkaille kertakirjautumisen vapauden, samalla kun valvotaan ja varmistetaan turvallisuus.
- Keskitetty provisiointi ja valtuutus palvelin.
- Sovellus todentaminen ja varmentaminen, kertakirjautuminen, auditointilokit, muokattavat kirjautumissivut
- Rooli pohjaiset luvat (Finance Online).

2.7.5 MidPoint (OS)

MidPoint on Evolveumin kehittämä avoimen lähdekoodin identiteetinhallinta ratkaisu, joka pystyy skaalautumaan pienistä organisaatioista suuriin, jopa yrityksiin, joilla miljoonia identiteettejä. MidPoint ymmärtää tietoturvan vakaavuuden ja on siksi suunniteltu minimoimaan niin sisäiset kuin ulkoisetkin uhat. Tätä korostaa ohjelmiston säännölliset päivitykset, jotka varmistavat, että MidPoint pysyy hallittavissa tulevaisuudessakin. Jatkuvat kehittämisprosessit pitävät MidPointin innovatiivisena ratkaisuna, joka reagoi markkinoiden tarpeisiin ajoissa. Evolveum-tiimi tarjoaa ammattitaitoisia palveluja, jotka kattavat myös tukitoiminnan, joka mahdollistaa tuotteen nopean käyttöönoton ja optimoinnin. (Evolveum)

MidPoint -ominaisuuksia:

- Identiteetin hallinta: Antaa organisaatiolle kontrollin identiteettien käytöstä, säilönnästä ja jakamisesta. Se on vaihtoehto määritellä, pakottaa, auditoida ja tarkastaa politiikkoja, jotka ovat vastuussa informaation kulusta niin sisäisissä kuin ulkoisissa järjestelmissä
- Organisaation rakenne: MidPoint voi synkronoida organisaation rakenteen eri henkilöstönhallintajärjestelmistä tai se voi itse olla organisaation rakenteen lähde
- Salasanan hallinta: Organisaatiolla on mahdollisuus luoda vahvoja ja ainutlaatuisia salasanoja sekä käyttäjille että resursseille ja myös huolehtia niistä koko elinkaarensa aikana. MidPoint validoi salasanoja ja luo niitä tiettyjen käytäntöjen mukaisesti (Evolveum).

2.7.6 OpenIAM (OS)

OpenIAM LLC on avoimen standardin identiteetin- ja pääsynhallintayhtiö, joka rakentaa ja suunnittelee täysin integroituja ratkaisuja, jotka vastaavat monenlaisiin tarpeisiin ja sopeutuvat muuttuviin liiketoiminnan tarpeisiin.

OpenIAM tarjoaa kattavat ja integroidut identiteetinhallinta ja verkkosivujen hallintaratkaisut, jotka perustuvat avoimiin standardeihin ja joita tarjotaan ammattimallin mukaisesti. Ratkaisut on suunniteltu kattamaan miljoonia käyttäjiä ja tarjoamaan joustavuutta sopeutua vaativimpiin ympäristöihin.

OpenIAM-tuotteet on suunniteltu tarjoamaan keskitettyjä, standardoituja ja automatisoituja identiteetinhallintapalveluja riskien vähentämiseksi, kustannusten vähentämiseksi ja toiminnan tehostamiseksi. Rikas palveluihin perustuva sovellusliittymä ja sen helppokäyttöiset ominaisuudet vähentävät huomattavasti työn määrää identiteettien hallinnan aloittamiseksi. Tämän seurauksena ratkaisu tarjoaa keskisuurille ja suurille yrityksille mahdollisuuden käyttää henkilöllisyysinfrastruktuuria ilman tarpeettoman suuria maksuja, jotka liittyvät tyypillisesti henkilöllisyys- ja pääsynhallintaprojekteihin (OpenIAM).

OpenIAM -ominaisuuksia:

- Salasanojen hallinta: Antaa käyttäjien ylläpitää yhtä kaikki järjestelmät kattavan salasanan, joka vähentää tarvetta muistaa useita eri salasanoja, joka myös vaihtoehtoisesti nostaa tuottavuutta
- Provisiointi: Automaattinen käyttäjien ja resurssien provisiointi, deprovisiointi ja uudelleen provisiointi. Parantaa turvallisuutta varmistamalla pääsyoikeudet on annettu ja poistettu tarvittaessa
- Roolien hallinta: Työroolien integrointi identiteetin elinkaaren kanssa parantaa liiketoiminnan ja IT-puolen linjauksia (OpenIAM).

2.7.7 WSO2 Identity Server (OS)

WSO2 Identity Server tarjoaa turvallisen identiteetin hallinnan yritysverkkosovelluksille, palveluille ja sovellusliittymille hallitsemalla käyttäjien identiteettiä ja oikeuksia turvallisesti ja tehokkaasti. Identity Server -palvelun avulla yrityksen arkkitehdit ja kehittäjät voivat vähentää identiteettien provisiointi aikaa, taata turvallisen verkko kanssakäymisen ja tarjota pienemmän kertakirjautumis ympäristön. WSO2 Identity Server vähentää identiteettien hallinnan ja oikeuksien hallinnan hallinnollista rasitusta sisällyttämällä roolipohjaisen käyttöoikeuksien hallinnan (RBAC) yleissopimuksen, käytäntöpohjaisen pääsynhallinnan ja SSO-yhteyden.

Identity Server -palvelun avulla voit luoda, ylläpitää ja lopettaa käyttäjätunnuksia yhdessä käyttäjien identiteettien kanssa useissa järjestelmissä, sisältäen pilvipalvelut. Kun on olemassa useita sovelluksia, jotka edellyttävät todennusta, käyttäjien pitäisi voida kirjautua sisään yhdellä paikalla ja saada silti saumaton pääsy kaikkiin muihin sovelluksiin (WSO2).

WSO2 Identity Server -ominaisuuksia:

- Skaalautuva muotoilu sopii koko yrityksen käyttöön
- Yksinkertainen kokoonpano käyttöinen rakenne, joka auttaa yhdistämään kaikki identiteettiin liittyvät osat
- Mahdollistaa IAM: n löysästi kytketyn ratkaisun, jossa on helppokäyttöisiä laajennuspisteitä IAM-ongelmiin liittyvien kolmansien osapuolten järjestelmien liittämiseen
- Tarjoaa turvallisen ja luotettavan yrityksen IAM-ratkaisun, jossa on ennakoivat korjaukset ja säännölliset tietoturvapäivitykset (Karunarathna & Karunaratne 2017).

2.7.8 Shibboleth (OS)

Shibboleth Identity Provider tarjoaa kertakirjautumis -ominaisuuksia, todentaa käyttäjiä ja toimittaa tietoja palveluille, laajentaen ulottuvuuttaan yli yhden organisaation. Yksinkertaisen kyllä / ei-vastauksen lisäksi todentamispyyntöön Identity Provider voi tarjota runsaasti käyttäjäkohtaisia tietoja palveluihin. Nämä tiedot voivat auttaa palvelua tarjoamaan henkilökohtaisemman käyttäjäkokemuksen, tallentamaan käyttäjän tarvitsematta manuaalisesti syöttää tietoja, joita palvelu tarvitsee, ja päivittää tiedot joka kerta, kun käyttäjä kirjautuu palveluun (Shibboleth).

Shibboleth -ominaisuuksia:

- Tuki säilöntä pohjaisiin todentamisjärjestelmiin, LDAP, Kerberos, JAAS, X.509, SPNEGO ja Duo Security
- Tuki käyttäjätiedon lukemiseen LDAP-hakemistoista ja relaatiotietokannoista ja vaikeiden tai yksinkertaisten tehtävien suorittaminen haetulle datalle
- Valvoo päästettyä dataa ja varmistaa sen luovuttamisen vain sallituille järjestelmille
- Erinomainen skaalautuvuus, niin suorituskyvyssä kuin hallittavuudessa. Yksi istunto pystyy käsittelemään miljoonia todennuspyyntöjä päivässä ja kommunikoida tuhansien palveluntuottajien kanssa
- Yhteensopiva kaikkien SAML 1.1 ja 2.0 toteutuksien kanssa (Shibboleth).

3 APACHE SYNCOPE

Apache Syncope on Tirasan kehittämä ja myöhemmin Apache Software Foundationille lahjoitettu avoimen lähdekoodin ohjelmisto.

Syncope mahdollistaa identiteetin hallinnan koko sen elinkaaren aikana, olivat ne sitten käyttäjiä, ryhmiä tai muita. Syncope on mahdollista ottaa käyttöön niin pilvessä kuin paikallisesti ja se tarjoaa useita ominaisuuksia, kuten esimerkiksi tapahtumien ilmoitukset, ohjelmien ajon ja aikataulutuksen, provisioinnin ja sovituksen (Tirasa).

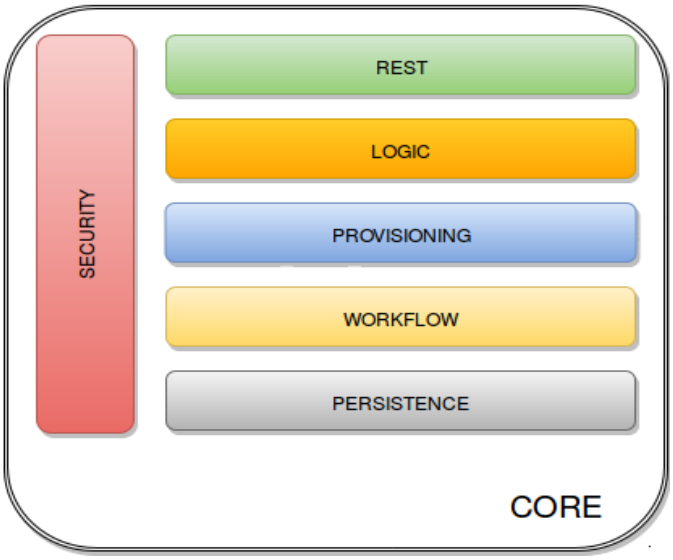
Syncope pohjautuu Java EE -teknologiaan ja se on suunniteltu pitämään yrityksen identiteetti data yhdenmukaisena ja synkronoituna läpi raakakantojen, data formaattien ja mallien (Hall 2016).

3.1 Apache Syncopen komponentit

Apache Syncope sisältää monia eri komponentteja. Tässä osiossa tarkastellaan mitä komponentteja Syncope sisältää ja mitkä ovat niiden toiminnot (Apache Syncope RS, luku 2).

3.1.1 Ydin

Kaikki Apache Syncopen tarjoamat palvelut tulevat ytimen kautta. Ydin on vielä itsessään pilkottu moneen pienenpään osaan (jatkossa jokainen osa on oma ”kerros”), joista jokaisella on oma tärkeä tehtävänsä. Kuvassa 2 ydin on pilkottu pienenpiin osiin ja sen alla käydään läpi jokaisen kerroksen nimi ja tarkoitus.



Kuva 2 Apache Syncopen ydin ja sen sisältö (Apache Syncope RS)

- REST-kerros
  Pääasiallisin tapa käyttää ytimen palveluita on REST-käyttöliittymä, mikä mahdollistaa täyden pääsyn kaikkiin ominaisuuksiin. Tämä käyttöliittymä antaa kolmannen osapuolen ohjelmien, kirjoitettuna millä tahansa ohjelmointikielellä, käyttää IDM palveluita.
- Logiikka-kerros
  Sijaitsee käyttöliittymän alapuolella, logiikka on vastuussa muiden kerrosten ohjaamisesta, implementoimalla operaatiot, jotka voidaan laukaista REST palveluilla. Se on myös vastuussa muutaman muun ominaisuuden ohjaamisesta (ilmoitukset, raportit ja auditointi).
- Provisiointi-kerros
  Provisiointi-kerros on mukana hallitsemassa sisäistä (Työnkulun kautta) ja ulkoista (tiettyjen yhdistäjien kautta) käyttäjien, ryhmien ja objektien esittämistä.
  Yksi tärkeimmistä ominaisuuksista on kartoitus ominaisuus: Sisäinen data (Esim. käyttäjät) on korreloitu saatavilla olevista identiteetti varastoista
- Työnkulku-kerros
  Työnkulun kerros on vastuussa käyttäjien, ryhmien ja objektien sisäisestä elinkaaren hallinnasta.
- Jatkuvuuden-kerros
  Kaikki data (Käyttäjät, ryhmät, attribuutit, resurssit jne.) on sisäisesti hallitta standardia JPA 2.0 käyttäen, joka pohjautuu Apache OpenJPA:ahan. Data välittyy

alla olevaan tietokantaan, jota kutsutaan ***Internal Storage*** -nimellä. Jatkuvuus varmistetaan kattavalla Spring Frameworkin tuomalla tapahtuman hallinnalla

- Turvallisuus-kerros
  Sen sijaan että turvallisuus olisi erillinen kerros, suojaustoiminnot laukeavat saapuvan pyynnön käsittelyn aikana.

3.1.2 Ylläpitäjän käyttöliittymä

Ylläpitäjän käyttöliittymä on web-pohjainen konsoli, millä voidaan konfiguroida ja ylläpitää käytössä olevia versioita, joka tukee täysin delegoitua ylläpitoa.

Kommunikaatio ylläpitäjän käyttöliittymän ja ytimen kesken on yksinomaisesti RESTiin pohjautuva.

Käyttöliittymä sisältää monia eri sivuja, joista voi hallita mm. käyttäjiä ja ryhmiä tai nähdä karttanäkymän eri resursseista. Näitä sivuja on muun muassa:

- Datakojelauta
  Datakojelauta (Engl. Dashboard) näyttää yleiskuvan Apache Syncope ympäristöstä. Se sisältää monia pienohjelmia ja välilehtiä, jotka näyttävät tietoja ja yksikohtia jokaisesta saatavilla olevasta komponentista
- Alue-sivu
  Alue-sivulla (Engl. Realms page) ylläpitäjät voivat muokata ja hallita käyttäjiä, ryhmiä ja objekteja.
- Topologia
  Topologia sivu tarjoaa karttanäkymän eri yhdistäjistä ja ulkoisista resursseista, jotka ovat saatavilla ja konfiguroitu.
- Raportit
  Raportit sivuilta ylläpitäjät näkevät eri raportteja ja voivat luoda ja muokata raportti pohjia.
- Konfiguraatio
  Konfiguraatio sivulla ylläpitäjät voivat muokata useita eri alueita organisaation tarpeisiin sopivaksi. Näitä on mm. auditointi asetukset, lokit, ilmoitukset yms.

Näiden sivujen lisäksi ylläpitäjän käyttöliittymästä näkee mm. mikäli käyttäjä on itsevaihtanut salasanansa ja mahdollisen epäonnistumisen syyn. Lisäksi jos ylläpitäjät lisäävät lisäosia Apache Syncopeen, näkyvät ne myös täällä. (Apache Syncope RS, luku 4.1)

3.1.3 Päätekäyttäjän käyttöliittymä

Päätekäyttäjän käyttöliittymän pääsijainen tarkoitus on tarjota päätekäyttäjille mahdollisuuden itse muokata tietojaan tai nollata salasana. Ylläpitäjillä on mahdollisuus myös muokata päätekäyttäjien käyttöliittymää organisaation tarpeen mukaisiksi, esimerkiksi vaihtaa värimaailmaa, logo yms. Käyttöliittymä on tehty AngularJS formaatilla.

AngularJS kuitenkin avaa käyttöliittymän eri hyökkäyksille kuten XSRF (Engl. Cross-Site Request Forgery), mutta käyttöliittymä on suojattu näitä vastaan. Lisäksi sivulla on mahdollista lisätä esimerkiksi Googlen tarjoama re-Captcha (Apache Syncope RS, luku 4.2).

3.1.4 Komentorivikäyttöliittymä

Komentorivikäyttöliittymä tarjoaa samat ominaisuudet kuin graafinen ylläpitäjän käyttöliittymä, kuten esimerkiksi käyttäjien hallinta, raportit ja konfiguraation muokkaus (Apache Syncope RS, luku 4.3).

3.1.5 Kolmannen osapuolen ohjelmat

Kolmannen osapuolen ohjelmille tarjotaan täysi pääsy IDM-palveluihin hyödyntämällä REST-Käyttöliittymää joko Java Client Libraryn tai http-kutsujen kautta.

- Eclipse IDE liitin mahdollistaa sähköposti ilmoitusten ja raportti pohjien etähallinnan ja toimii esimerkkinä, kun Java ohjelmisto toimii Client Library varassa ollessaan yhteydessä ytimeen RESTin kautta.
- Netbeans IDE liitin mahdollistaa samat kuin Eclipse IDE, mutta mahdollistaa myös Apache Groovy ympäristön etähallinnan (Apache Syncope RS, luku 2.5)

3.2 Apache Syncopen vaatimukset

Tässä osiossa käydään mitä vaatimuksia Apache Syncopella on laitteiden ja ohjelmistojen suhteen (Apache Syncope GS, luvut 2.1 – 2.4)

Taulukossa 1 näkyvät laitteistovaatimukset ovat erittäin vähäiset eikä niiden saavuttaminen pitäisi tuottaa ongelmia yhdellekään yritykselle.

Prosessori	Dual core, 2Ghz vähintään
RAM-Muisti	2Gb vähintään
Levytila	100MB vähintään

Taulukko 1 Laitteisto vaatimukset

Apache Syncope toimii useille eri sovelluspalvelimilla ja toiminta on varmistettu seuraavilla:

- Apache Tomcat 9
- Glassfish 5
- Payara Server 5
- Wildfly 14

Apache Syncope toimii useimmilla tunnetuilla tietokantaohjelmistoilla ja toiminta on varmistettu seuraavilla tietokantaohjelmistoilla:

- PostgreSQL (>= 10.3, JDBC driver >= 42.2.5)
- MariaDB (>= 10.3.7, JDBC driver >= 2.3.0)
- MySQL (>= 5.7, JDBC driver >= 5.1.47)
- Oracle Database (>= 11g, JDBC driver >= ojdbc8 12.2.0.1)
- MS SQL Server (>= 2017, JDBC driver >= 6.4.0.jre8)

4 APACHE SYNCOPE TESTAUS

Tässä osiossa käsitellään opinnäytetyön käytännönosuutta. Kerrataan tavoitteet, testaus tavat, mahdolliset ongelmat ja lopputulokset.

4.1 Tavoite

Työn tavoitteena on tutkia Apache Syncope identiteetinhallintajärjestelmän ominaisuuksia, jotta tilaajayritys saisi käsityksen mihin ohjelmaa voidaan käyttää, mitä hyötyä siitä on ja onko se oikea valinta yritykselle.

4.2 Testaus

Alkuperäinen suunnitelma oli rakentaa avoimen lähdekoodin ohjelmistoilla toteutettu testausympäristö ja tehdä testaus tilaajayrityksen tiloissa, mutta aikaongelmien takia testaus siirtyi itse rakennettuun virtualisoituun ympäristöön. Testausta koskeva dokumentaatio löytyy opinnäytetyön lopusta liitteenä otsikolla Apache Syncope -testausdokumentaatio (LIITE1).

4.3 Ilmenneet ongelmat

Syncopen dokumentaatiossa mainittiin, että *syncopeMasterDataSource* -lähde pitää olla konfiguroituna. Dokumentaatiosta ei suoraan löytynyt, että minne kyseinen lähde kuuluu lisätä.

Yritin ensin rakentaa vaadittavaa tietokantaa käyttäen PostgreSQL -tietokantaa, mutta asennusohjelma ei tuntemattomasta syystä saanut yhteyttä tietokantaan. Päädyin vaihtamaan tilalle MySQL -tietokannan, johon asennusohjelma sai yhteyden.

Asennuksen loppuvaiheessa tuli virheilmoitus, joka keskeytti asennuksen. Tätä ongelmaa tutkiessani päädyin kysymään apua tilaajanyrityksen järjestelmäarkkitehdilta. Asian selvittelyn jälkeen päätimme lopettaa kehitystyön.

Projektia ei kuitenkaan hylätty. Yhdessä tilaajayrityksen henkilöstön kanssa löysimme vaihtoehtoisen ratkaisun, jossa voimme hyödyntää teoriaosuuden oppeja sekä ennen kehitystyön loppua opittuja käytännönasioita (ks. kappale 4.4).

4.4 Lopputulokset

Testauksen lopputuloksena on dokumentaatio, mihin on kerätty työvaiheet, jotka tehtiin ennen kehitystyön lopettamista. Verkossa olevaa kokeiluversiota testatessa sekä ohjelman dokumentaatioon tutustuessa sain karkean kuvan ohjelman toiminnasta, asennuksesta oikeaan ympäristöön ja ylläpidosta. Asennuksen loppuvaiheilla ilmeni ongelmia, jotka johtivat tuotteen uudelleen arviointiin. Uudelleen arvioinnissa kävimme läpi kokemukseni kokeiluversiosta ja mitä ohjelman dokumentaatiosta on käynyt ilmi. Tuote ei täyttänyt kaikki vaatimuksia ja keskustelun aikana löysimme toisen ratkaisun, joka sopii tarkoitukseemme.

Arvioinnin aikana keskusteltiin myös vaihtoehtoisesta tuotteesta. Tuotteita on monia ja ratkaisuksi päädyttiin rakentamaan alusta, johon tulevaisuudessa voidaan rakentaa IDM-ohjelmisto. Alusta koostuu mahdollisesti seuraavista komponenteista:

- LDAP
- FreeIPA
- Windows Active Directory
- Keycloak.

LDAP -ohjelmiston tulisi olla helposti ylläpidettävä ja se sisältäisi yrityksen master datan.

FreeIPA -ohjelmistokokonaisuuden avulla hallittaisiin yrityksen Linux tietokoneita.

Windows Active Directory -sisältää yrityksen Windows -pohjaiset tietokoneet sekä niiden käyttäjät.

Keycloak on avoimeen lähdekoodiin perustuva ohjelmisto, joka tarjoaa kertakirjautumista (SSO). Keycloakia käytetään kirjautumaan yrityksen sisällä käytettäviin ohjelmistoihin. Ohjelmistoja on monia, joten näin vältetään toistuvat käyttäjien autentikoinnit ja työskentely nopeutuu.

Täyden IDM-ohjelmiston katsottiin tällä hetkellä olevan ylimitoitettu ratkaisu. Yllä mainittu alustaratkaisu mahdollistaa, että tulevaisuudessa IDM-ohjelmisto voidaan rakentaa sen

päälle. Näin yritys saa toimivan ratkaisun nykyiseen ongelmaan, ja sen joustavuuden takia heillä on myös ratkaisu tulevaisuudessa.

5 POHDINTA JA TULOKSET

Opinnäytetyön tavoitteena oli tutkia identiteetinhallintaa, sen tarkoitusta ja hyötyjä sekä tutkia Apache Syncope -ohjelmistoa. Identiteetinhallinta on erittäin tärkeä osa nykypäivän yrityksiä. Se parantaa tietoturvaa, helpottaa ylläpitotehtäviä sekä helpottaa IT-helpdeskin työtaakkaa, kun päätekäyttäjät voivat tehdä toimintoja itse. Useimmat identiteetinhallintaohjelmistot koostuvat samoista ominaisuuksista. Tämä korostaa järjestelmän hinnoittelua, sen käytettävyyttä ja ylläpitoa. Oikean järjestelmän valinta voi olla vaikeaa. Kun tiedetään mitä tarvitaan ja mihin, oikea järjestelmä löytyy kyllä.

Vaikka alkuperäinen suunnitelma Apache Syncope -ohjelmiston asentamisesta ja käyttöönotosta ei toteutunut, löysimme yhdessä tilaajayrityksen kanssa ratkaisun, johon myös he ovat tyytyväisiä. Tämän vaihtoehtoisen ratkaisun kehitystyön parissa jatkan tulevaisuudessa. Tavoitteena on kehittää järjestelmä, joka vastaa nykypäivän yrityksen tarpeita toimintojen ja tietoturvan puolesta sekä on helppo ylläpitää.

Valittu Apache Syncope -ohjelmisto vaikutti alkuselvityksen aikana teoriassa ohjelmistolta, joka soveltuisi vaadittuun käyttöön. Asennusvaiheen aikana kuitenkin selvisi puutteita, jotka estävät kyseisen ohjelmiston käyttöönoton. Työn evaluoinnin aikana selvitettiin jatketaanko kehitystyötä toisen ohjelmiston parissa. Päädyimme tulokseen, että kaiken kattava IDM-ohjelmisto ei olekaan vielä tällä hetkellä oikea ratkaisu. Työtä jatketaan rakentamalla alusta, johon IDM-ohjelmiston voi tulevaisuudessa rakentaa.

Teoriaosuudessa käydyt asiat opettivat identiteetinhallinnan tärkeyden. Ilman keskitettyä identiteetinhallintaa järjestelmään voi jäädä ns. unohdettuja identiteettejä. Kun näitä identiteettejä ei päivitetä, eikä kukaan tiedä niiden olemassa olosta, antavat ne mahdollisille hyökkääjille hyökkäysvektorin yritykseen ja altistavat yrityksen huonoimmassa tapauksessa vakavalle tietoturvamurrolle ja miljoonien eurojen vahingoille.

LÄHTEET

Apache Syncope RS. Apache Syncope reference guide. Viitattu 22.4.2019 https://syncope.apache.org/docs/2.1/reference-guide.html

Apache Syncope GS. Apache Syncope getting started. Viitattu 22.4.2019 https://syncope.apache.org/docs/2.1/getting-started.html

BizTech. (2016) 3 Reasons to Deploy an Identity and Access Management Solution. Viitattu 04.04.2019 https://biztechmagazine.com/article/2016/09/3-reasons-deploy-identity-and-access-management-solution

CSO Online, Martin J., Waters J. (2018) What is IAM? Identity and access management explained

Viitattu 04.04.2019 https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html?page=1

Evolveum. Identity Management and Identity Governance as the CIO's and CISO's priority. Viitattu 22.4.2019 (PDF-tiedosto) https://evolveum.com/?wpdmdl=4759

Finance Online. (2019) Auth0 review. Viitattu 20.4.2019 https://reviews.financeonline.com/p/auth0/

Finance Online. (2019) Okta Identity Cloud Review. Viitattu 20.4.2019 https://reviews.financeonline.com/p/okta-identity-cloud/

Hall, S. (2016) Apache Syncope Offers Open Source Single Sign-On Identity Management. Viitattu 21.4.2019 https://thenewstack.io/apache-syncope-embraces-id-management-cloud-iot/

Tietosuojalaki 2018/1050. Annettu Helsingissä 5.12.2018. Viitattu 25.03.2019 https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Hong Kong Polytechnic University. Identity and Access Management Viitattu 04.03.2019 https://www.polyu.edu.hk/ags/Newsletter/news0911/IAM_details.html

Information technology - Security techniques - A framework for identity management - Part 1: Terminology and concepts (2017) Standardi 24760-1:2011. Viitattu 25.03.2019 https://www.iso.org/standard/57914.html

Karunarathna, I. & Karunaratne I. 2017. What is WSO2 Identity Server? Viitattu 21.4.2019 https://wso2.com/library/articles/2017/08/what-is-wso2-identity-server/

Online Tech. What is Azure Active Directory (AAD)? Viitattu 20.4.2019 http://www.online-tech.com/resources/references/what-is-azure-active-directory-aad

OpenIAM. OpenIAM Identity and Access Management (2018) Viitattu 21.4.2019 http://docs40.openiam.com/#introduc-tion/about.htm%3FTocPath%3DOpenIAM%25204.0%2520documentation%7C_____1

Oracle Technology Network. (2018) Fusion Middleware Administering Oracle Identity Manager. Viitattu 20.4.2019 https://docs.oracle.com/cd/E52734_01/oim/OMADM/over-view.htm#OMADM5632

Penn State University Identity Services (IdS) White paper (2014). The Role of Authentication in Identity Management. Viitattu 13.03.2019 http://www.identity.psu.edu/resources/documenta-tion/current/the-role-of-authentication/

Penn State University Identity Services (IdS) White paper (2014). The Role of Authorization in Identity Management. Viitattu 13.03.2019 http://www.identity.psu.edu/resources/documenta-tion/current/the-role-of-authorization/

Rouse M. (2017) Definition: Digital Identity. Viitattu 25.03.2019 https://whatis.techtarget.com/de-finition/digital-identity

Rouse, M.; Rosencrance, L. & Mathias, C. 2017 Identity management (ID management) Viitattu 04.03.2019 https://searchsecurity.techtarget.com/definition/identity-management-ID-manage-ment

Shibboleth. Shibboleth Identity Provider. Viitattu 21.4.2019 https://www.shibboleth.net/prod-ucts/identity-provider/

Silander (2013) Katsaus identiteetinhallinnan teknologioihin ja niiden tulevaisuuden näkymiin. Vii-tattu 25.03.2019 https://aaltodoc.aalto.fi/bitstream/handle/123456789/10426/master_Silan-der_Jon_2013.pdf?sequence=1

Tirasa Apache Syncope. Viitattu 21.4.2019 https://www.tirasa.net/en/develop/identity-management

Windley, Phillip J. (2005). Digital Identity. O'Reilly Media, Inc. Sivut 8–9. Viitattu 25.03.2019

ISBN 978-0596008789.

WSO2 Identity Server Documentation. Viitattu 21.4.2019 https://docs.wso2.com/display/IS570/Overview

LIITTEET

LIITE 1 Apache Syncope testausdokumentaatio

Apache Syncope -testausdokumentaatio

Dokumentaatiosta

Tämän dokumentaation alkuperäinen tarkoitus oli sisältää ominaisuuksien kuvaukset ja niiden toiminnan toteaminen käytännössä käytössä olevasta Apache Syncope -ohjelmistosta. Dokumentaation piti sisältää mm. kuvia ja selityksiä mitä eri välilehdissä voidaan tehdä, sekä vaiheet miten esimerkiksi Syncopessa luotu käyttäjä synkronoituu Windows Active Directoryyn. Työssä ei kuitenkaan onnistuttu ja siirryttiin uuden ratkaisun kehittämiseen. Alkuperäisestä suunnitelmasta poiketen, tämä dokumentaatio sisältää nyt työvaiheet kuvineen ja selityksineen mitä tehtiin ennen projektin lopettamista.

Vaatimukset

Apache Syncope on suunniteltu Linux -pohjaisille käyttöjärjestelmille. Tilaajalla on käytössä Linuxin CentOS -jakelun käyttöjärjestelmiä, joten luonnollisesti valitsin myös itse CentOS 7 -käyttöjärjestelmän.

Syncope vaatii myös Java EE containerin eli sovelluspalvelimen, tietokannan ja Apache Mavenin. Sovelluspalvelimeksi valittiin Apache Tomcat 9 ja tietokannaksi MySQL 5.7. Kaikki vaiheet pois lukien Apache Syncopen asennus tehdään käyttöjärjestelmän terminaalista.

Dokumentaatio alkaa Apache Mavenin asennuksella. Tämän jälkeen siirrytään Tomcatin asennukseen ja konfiguraatioon. Kun Tomcat on valmis käyttöön, asennettaan ja valmistellaan MySQL -tietokanta. Näiden jälkeen asennettaan Apache Syncope ja edetään siinä niin pitkälle, kunnes prosessi keskeytyy. Asennukset eivät ole täysin kronologisessa järjestyksessä, mutta dokumentaatiota seuraten pääsee samaan lopputulokseen.

Apache Maven

Apache Maven on ohjelmien rakentamiseen tarkoitettu automaatiotyökalu, jota käytetään pääosin Java projekteissa.

Syncope installer -sisältää skriptejä, jotka automaattisesti ajavat Mavenin komennot. Mitään komentoja ei siis itse tarvitse syöttää asentamisen jälkeen.

Aloitetaan asennus lataamalla Mavenin tar -pallo wget -komennolla (Kuva1).

```
[Patrik@localhost ~]$ cd /tmp/
[Patrik@localhost tmp]$ wget http://mirror.netinch.com/pub/apache/maven/maven-3/
3.6.1/binaries/apache-maven-3.6.1-bin.tar.gz
```

Kuva 3 tar -Pallon lataaminen

Lataamisen jälkeen puretaan tar -pallo */opt/* hakemistoon (Kuva 2). Tämä tehdään koska */tmp/* hakemistosta tiedostot poistetaan automaattisesti tietyn ajan kuluessa. Kun purkaminen on valmis, kerrotaan Mavenille mistä hakemistosta se ajaa komentonsa (Kuva 3). Kun tämä on tehty, Apache Maven on valmis käyttöön.

```
[Patrik@localhost tmp]$ sudo tar -C /opt -xf apache-maven-3.6.1-bin.tar.gz
```

Kuva 4 Ladatun tar -pallon purku */opt/* hakemistoon

```
[Patrik@localhost tmp]$ cd /opt
[Patrik@localhost opt]$ alias mvn='/opt/apache-maven-3.6.1/bin/mvn'
```

Kuva 5 Määritellään Mavenin kotihakemisto alias -komennolla

Apache Tomcat 9

Tomcat 9 vaatii Java 8:n tai uudemman. Tarkistetaan käytössä oleva Java versio komennolla *java -version* (Kuva 4).

```
[Patrik@localhost ~]$ java -version
openjdk version "1.8.0_212"
OpenJDK Runtime Environment (build 1.8.0_212-b04)
OpenJDK 64-Bit Server VM (build 25.212-b04, mixed mode)
[Patrik@localhost ~]$
```

Kuva 6 Java version tarkistus

Java versio oli oikea, joten sitä ei tarvitse päivittää.

```
[Patrik@localhost /]$ cd /tmp
[Patrik@localhost tmp]$ wget http://www.nic.funet.fi/pub/mirror/apache.org/tomcat/tomcat-9/v
9.0.19/bin/apache-tomcat-tomcat-9.0.19.tar.gz
```

Kuva 7 Haetaan tar -pallo

Siirrytään */tmp/* hakemistoon ja ajetaan hakemiston sisällä wget -komento (Kuva 5). Kun komennon perään laitetaan verkko-osoite, voidaan komennolla ladata verkosta tiedostoja. Tomcatin sivuilla on osoite, josta voidaan ladata Tomcatin tar -pallo. Latauksen valmistuttua puretaan ladattu tar -pallo komennolla *tar -xf*. Parametri *x* (extract) purkaa ja *f* (filename) määrittää, että seuraava parametri on tiedoston nimi.

```
[Patrik@localhost tmp]$ tar -xf apache-tomcat-tomcat-9.0.19.tar.gz
```

Kuva 8 tar -Pallon purku

```
[Patrik@localhost tmp]$ sudo mv apache-tomcat-tomcat-9.0.19 /opt/
```

Kuva 9 Purettujen tiedostojen siirto

Siirretään puretut tiedostot pois */tmp/* hakemistosta */opt/* hakemistoon, jossa myös Apache Maven sijaitsee.

```
[Patrik@localhost /]$ sudo vim /opt/apache-tomcat-9.0.19/conf/tomcat-users.xml
```

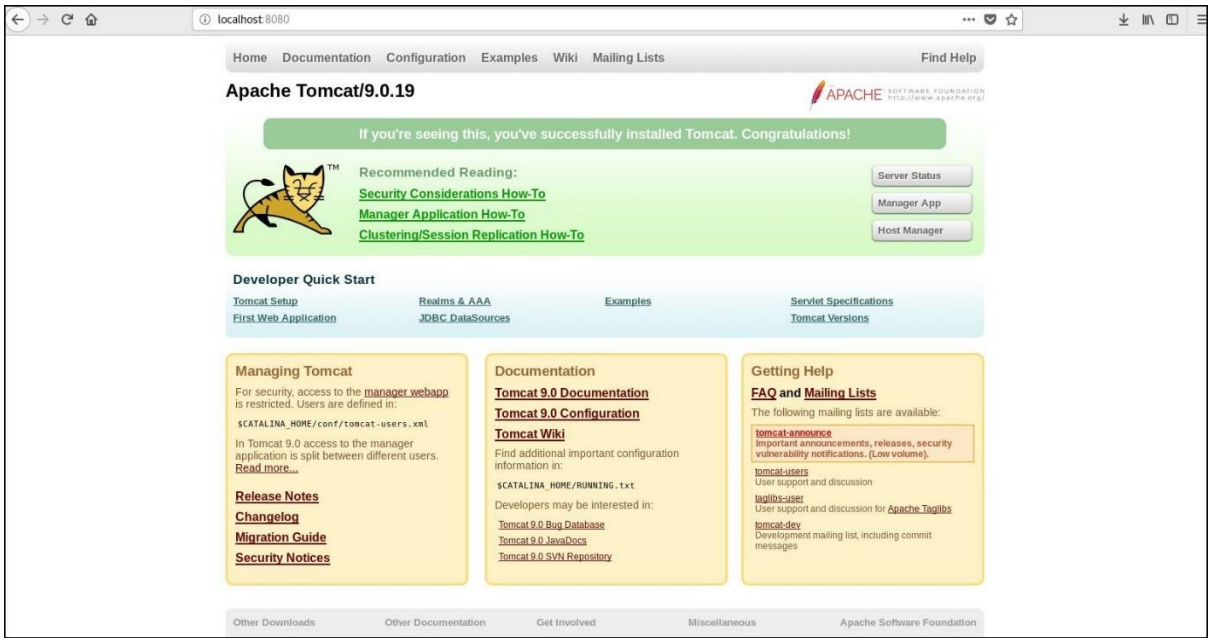
Kuva 10 Avataan Vim -tekstinkäsittelyohjelmalla tomcat-users.xml tiedosto

Apache Syncopen dokumentaatiossa mainitaan, että jotta Syncope pystyy kommunikoimaan Tomcat 9 palvelun kanssa pitää *tomcat-users.xml* tiedostoon lisätä kuvassa 9 näkyvät rivit.

```
-->
<role rolename="admin-gui"/>
<role rolename="manager-gui"/>
<role rolename="manager-script"/>
<role rolename="manager-jmx"/>
<role rolename="manager-status"/>
<user username="admin" password="qwerty1" roles="admin-gui,manager-gui,manager-script"/>
</tomcat-users>
```

Kuva 11 Lisätyt rivit

Koska työssä verkkokäyttöliittymään ei tarvitse päästä ulkoverkosta, ei Tomcat tarvitse enempää konfiguraatiota toimiakseen. Käyttöliittymään pääsee kirjoittamalla selaimen hakukenttään *localhost:8080* (Kuva 10).



Kuva 12 Tomcat 9 onnistuneesti asennettu

Syncope vaatii myös, että tiedostoon *context.xml* lisätään kuvan 11 mukaiset rivit. Tiedosto sijaitsee polussa */opt/apache-tomcat-9.0.19/conf/*.

```
<Resource name="jdbc/syncopeMasterDataSource" auth="Container" type="javax.sql.DataSource"
          factory="org.apache.tomcat.jdbc.pool.DataSourceFactory" testWhileIdle="true"
          testOnBorrow="true" testOnReturn="true"
          validationQuery="SELECT 1" validationInterval="30000"
          maxActive="100" minIdle="2" maxWait="10000" initialSize="2"
          removeAbandonedTimeout="20" removeAbandoned="true" logAbandoned="true"
          suspectTimeout="20" timeBetweenEvictionRunsMillis="5000"
          minEvictableIdleTimeMillis="5000" defaultAutoCommit="false"
          jdbcInterceptors="org.apache.tomcat.jdbc.pool.interceptor.ConnectionState;
            org.apache.tomcat.jdbc.pool.interceptor.StatementFinalizer"
          username="root" password="Oppari-1!" driverClassName="com.mysql.cj.jdbc.Driver"
```

Kuva 13 syncopeMasterDataSource konfiguraatio

```
JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -server \
-Xms1536m -Xmx1536m -XX:NewSize=256m -XX:MaxNewSize=256m -XX:+DisableExplicitGC \
-Djava.security.egd=file:/dev/./urandom"
```

Kuva 14 setenv.sh -tiedoston sisältö

Apache Tomcat 9 on vain yksi monista sovelluspalvelimista, mitä Syncopen kanssa voidaan käyttää. Jotta Tomcat 9 toimii yhdessä Syncopen kanssa pitää polkuun */opt/apache-tomcat-9.0.19/bin* luoda tiedosto, jonka nimeksi tulee *setenv.sh* ja sen pitää sisältää kuvan 12 mukaiset rivit.

Apache Tomcat 9 konfiguraatio on nyt lähes valmis. Seuraavaksi asennetaan MySQL -ohjelmisto, jolla voidaan luoda tietokantoja. Jotta Tomcat ja luodut tietokannat toimivat yhdessä, pitää verkosta ladata yhdistin (engl. connector) ja sijoittaa se kansioon */opt/apache-tomcat-9.0.19/lib* (Kuva 13).

```
-rw-r-----. 1 root root   63165 Apr 12 17:24 jsp-api.jar
-rw-r--r--. 1 root root  883898 Jun 10  2014 mysql-connector-java.jar
-rw-r-----. 1 root root  283215 Apr 12 17:24 servlet-api.jar
-rw-r-----. 1 root root   11225 Apr 12 17:24 tomcat-api.jar
```

Kuva 15 MySQL connector

Apache Tomcat 9 konfiguraatio on nyt valmis.

MySQL 5.7

Aloitetaan MySQL -ohjelmiston asennus ottamalla käyttöön sen raaka-arkisto.

```
[Patrik@localhost /]$ sudo yum localinstall https://dev.mysql.com/get/mysql57-community-release-el7-11.noarch.rpm
```

Kuva 16 MySQL raaka-arkiston käyttöönotto

Kun komento on syötetty, voidaan palvelu asentaa normaalisti käyttäen *yum* -komentoa.

```
[Patrik@localhost /]$ sudo yum install mysql-community-server
```

Kuva 17 MySQL asennus

Kun asennus on valmis, otetaan palvelu käyttöön komennoilla *sudo systemctl enable mysqld* ja *sudo systemctl start mysqld*.

```
[Patrik@localhost /]$ sudo systemctl status mysqld
[sudo] password for Patrik:
● mysqld.service - MySQL Server
   Loaded: loaded (/usr/lib/systemd/system/mysqld.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2019-05-13 14:09:37 EEST; 59min ago
     Docs: man:mysqld(8)
           http://dev.mysql.com/doc/refman/en/using-systemd.html
  Process: 7239 ExecStart=/usr/sbin/mysqld --daemonize --pid-file=/var/run/mysqld/mysqld.pid $MYSQLD_OPTS (code=exited, status=0/SUCCESS
)
  Process: 7156 ExecStartPre=/usr/bin/mysqld_pre_systemd (code=exited, status=0/SUCCESS)
 Main PID: 7242 (mysqld)
    Tasks: 28
   CGroup: /system.slice/mysqld.service
           └─7242 /usr/sbin/mysqld --daemonize --pid-file=/var/run/mysqld/mysqld.pid
```

Kuva 18 MySQL palvelun toiminta varmistettu

Komennolla *sudo systemctl status mysqld* varmistutaan, että palvelu käynnistyi ja on toiminnassa (Kuva 16).

Vielä ennen käyttöönottoa, pitää ohjelmisto turvata. Otetaan ensin väliaikainen salasana lokitiedostoista komennolla *sudo grep 'temporary password' /var/log/mysqld.log*.

```
[Patrik@localhost /]$ sudo grep 'temporary password' /var/log/mysqld.log
2019-05-13T11:09:34.966319Z 1 [Note] A temporary password is generated for root@localhost: dd(DK4zcwql&
```

Kuva 19 Väliaikainen salasana haettu lokitiedoista grep -komennolla.

Tämän jälkeen voidaan ajaa komento *sudo mysql_secure_installation*. Salasana pyydetään vaihtamaan ja sen pitää olla vähintään 8 merkkiä pitkä ja sisältää vähintään yksi iso kirjain, yksi pieni kirjain, yksi numero ja yksi erikoismerkki. Tämän jälkeen tulee lista

erilaisia kysymyksiä. Näitä on mm. poistetaanko testi tietokanta. Kaikkiin vastataan *y* eli kyllä.

Nyt MySQL:ään voidaan yhdistää terminaalista. Tämä tapahtuu komennolla *mysql -u root -p*. MySQL kysyy salasanaa, joka määriteltiin edellisessä vaiheessa.

Luodaan tietokanta, jonka nimeksi tulee *syncope*. Täällä ei tarvitse tehdä enempää. Kun Syncope asentuu oikein, se syöttää tarvittavan datan automaattisesti tietokantaan.

```
mysql> CREATE DATABASE syncope;
Query OK, 1 row affected (0.00 sec)

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| syncope            |
| sys                |
+--------------------+
5 rows in set (0.05 sec)
```

Kuva 20 Syncope -niminen tietokanta luotu

MySQL on asennettu ja valmis käyttöön.

Apache Syncope Asennus

Ladataan Apache Syncopen sivuilta GUI installerin .jar -tiedosto wget -komennolla.

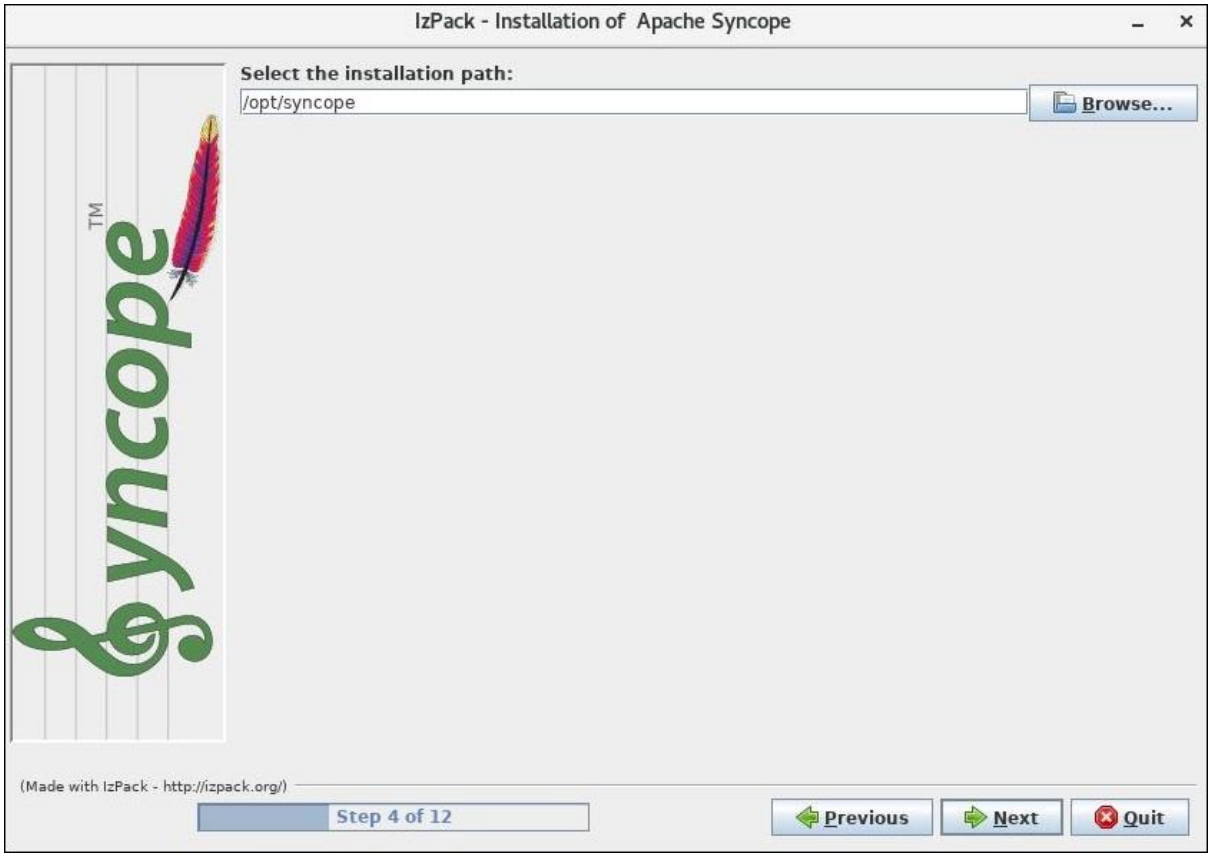
```
[Patrik@localhost /]$ wget http://www.apache.org/dyn/closer.lua/syncope/2.1.4/syncope-installer-2.1.4-uber.jar
```

Kuva 21 wget -Komennolla ladataan tiedosto

Siirretään installer */opt/* kansioon ja ajetaan paketti *java -jar* -komennolla.

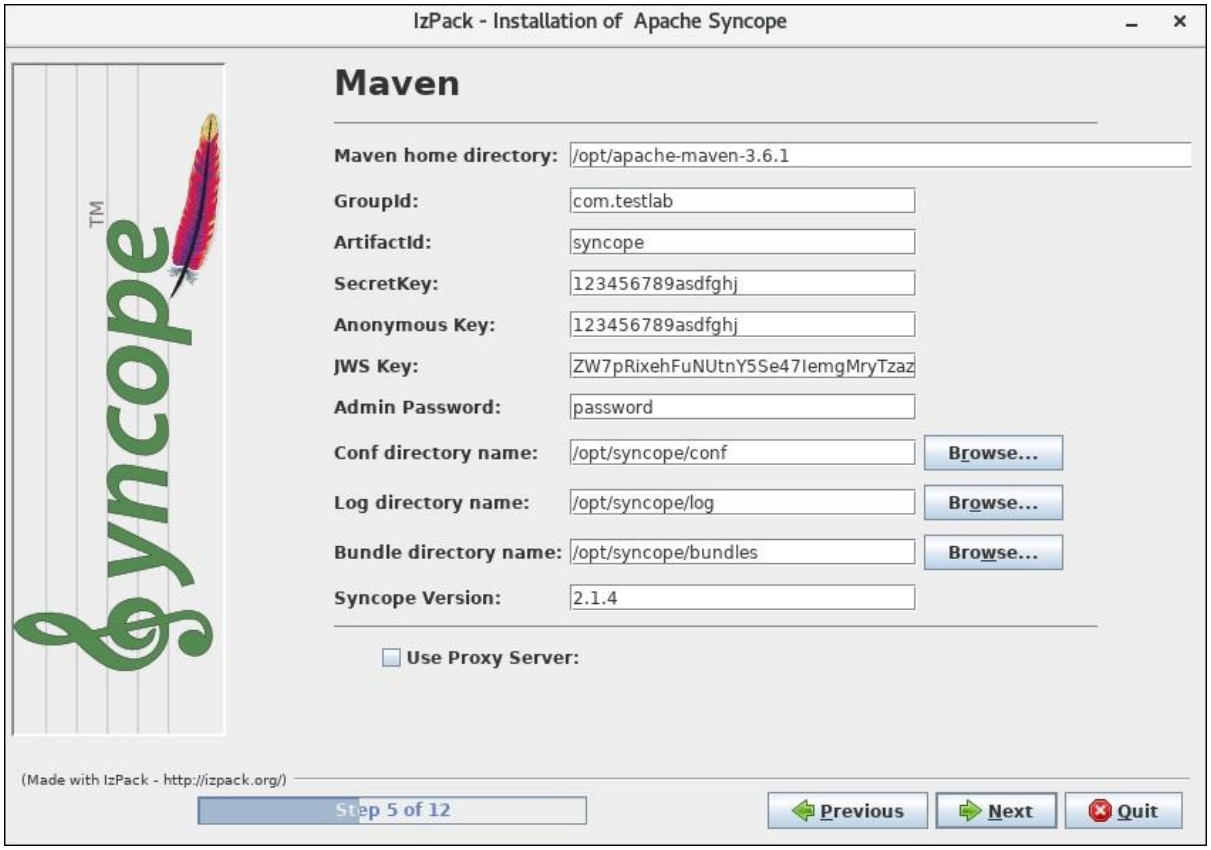
```
[Patrik@localhost opt]$ sudo java -jar syncope-installer-2.1.4-uber.jar
```

Kuva 22 Ajetaan asennuspaketti



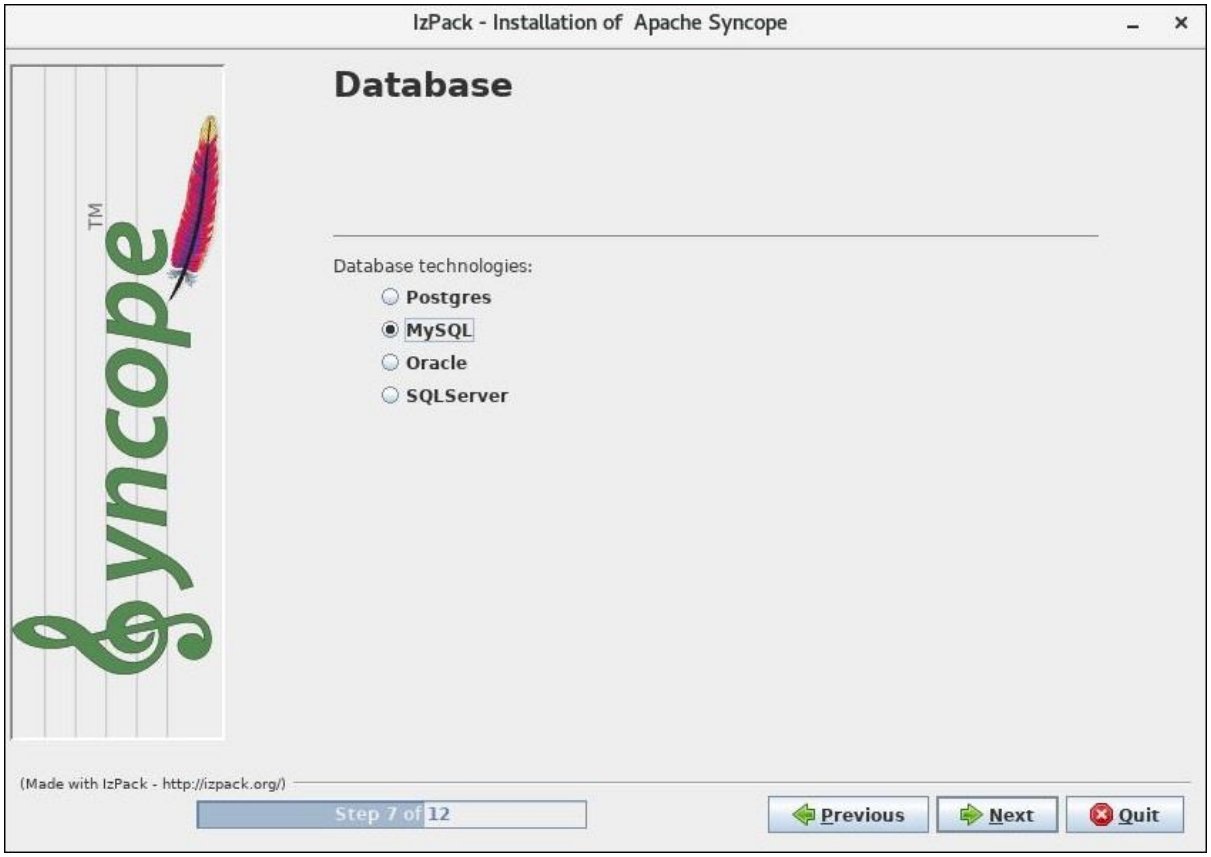
Kuva 23 Asennuspolku

Oletusarvoisesti Syncope yrittää tuntemattomasta syystä asentua */tmp/* hakemistoon. Opimme aikaisemmin, että kyseisestä hakemistosta tiedostot poistetaan tietyn ajan kuluttua. Muutetaan asennuspolku */opt/* hakemistoon, jossa myös muut ohjelmamme sijaitsevat.



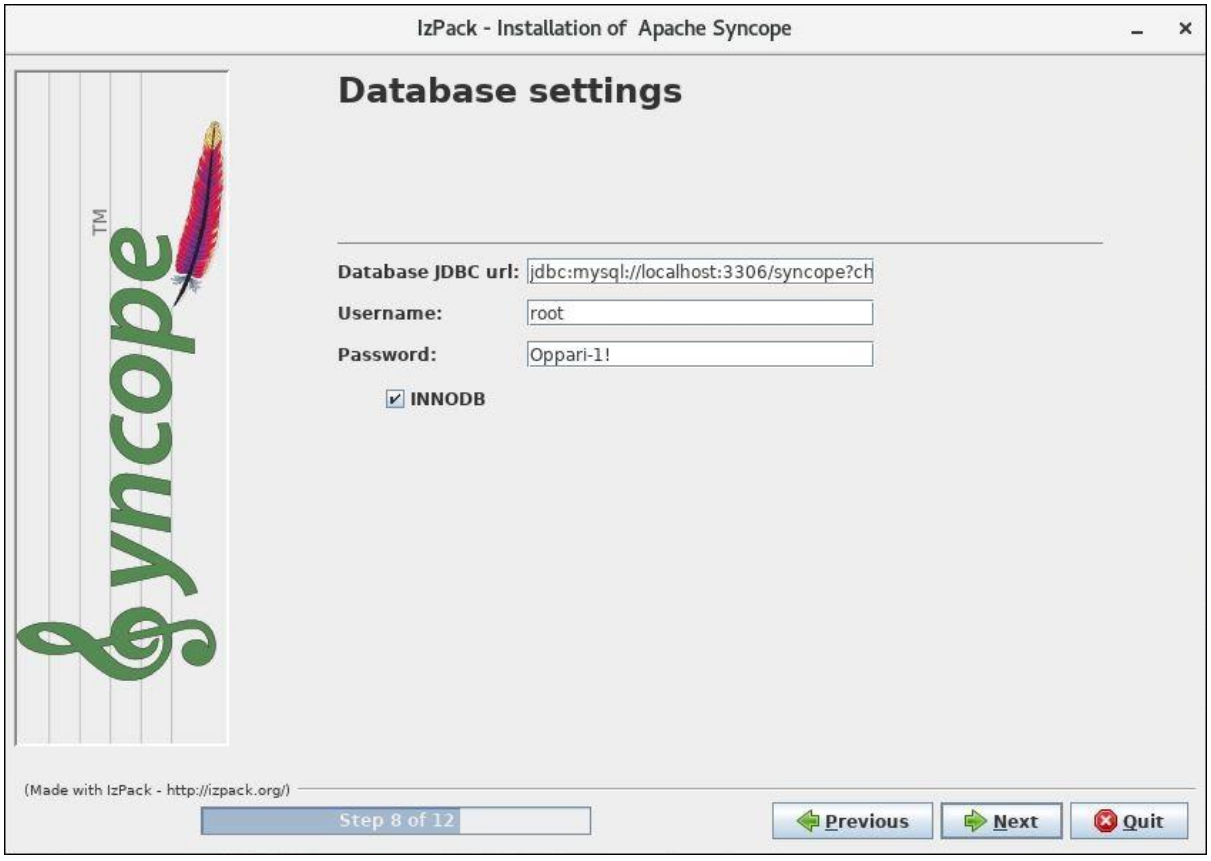
Kuva 24 Apache Maven -asetukset

GroupId -kohtaan muutetaan Windows Serverillä tehty domain nimi, joka on tässä tapauksessa *com.testlab.* Lisäksi muutetaan loki- ja konfiguraatiohakemistojen sekä Connector -pakettien hakemistot */tmp/* hakemistosta */opt/* hakemistoon. Koska työ tehdään testiympäristössä, muut kohdat voidaan jättää oletusarvoihin.



Kuva 25 Tietokannan valinta

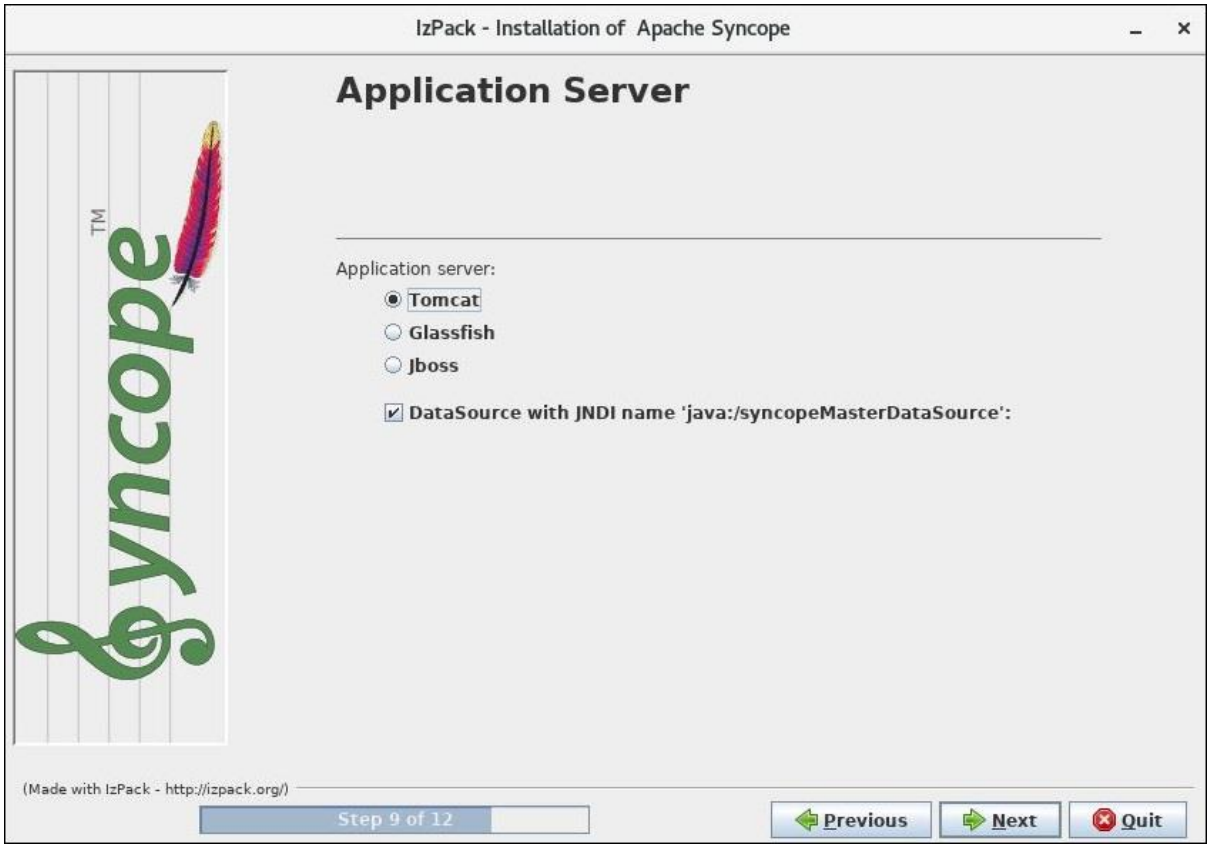
Kokeilin alun perin käyttöjärjestelmän mukana tullutta Postgres -tietokantaa, mutta se ei tuntemattomasta syystä saanut yhteyttä Syncopen asennusohjelmaan. Yritin ratkaista ongelmaa, mutta en siinä onnistunut. Lopulta päätin kokeilla MySQL -tietokantaohjelmistoa. Sen yhdistäminen onnistui välittömästi ja käyttöliittymä vaikutti käyttäjäystävällisemmältä.



Kuva 26 Tietokannan asetukset

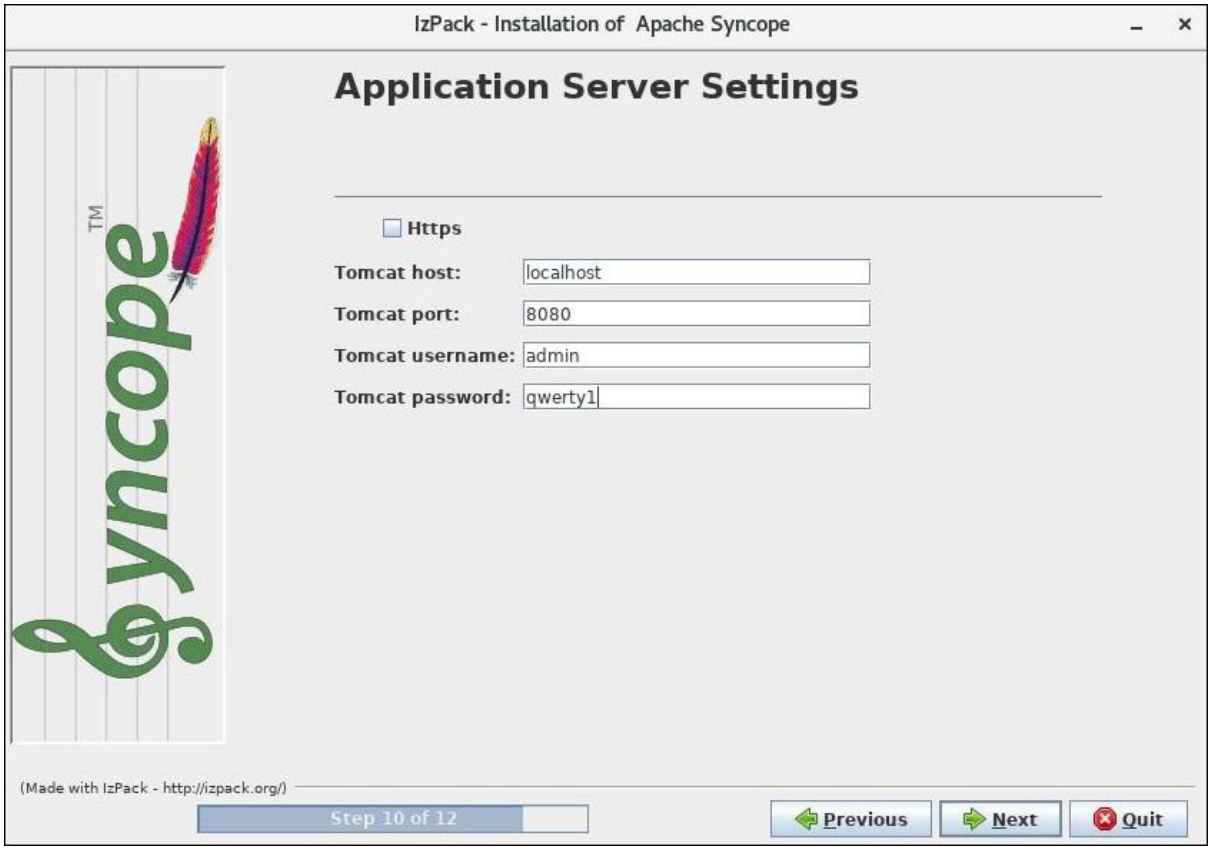
JDBC url eli *Java Database Connectivity url* on osoite mikä määrittelee missä osoitteessa tietokanta sijaitsee. URLin muoto vaihtelee tietokannoittain, mutta yleisesti se on muotoa *jdbc:tietokantaohjelman nimi:tietokannan osoite: tietokannan portti/tietokannan nimi*. Tässä tapauksessa osoite siis on *jdbc:mysql://localhost:3306/syncope*. Osoite on tämä, koska käytössä on MySQL tietokanta, se on käytössä localhostilla eli samalla tietokoneella, se kuuntelee porttia 3306 ja siellä on käytössä syncope -niminen tietokanta.

Username ja password kohtaan kirjoitetaan MySQLn turvaamisvaiheessa annettu salasana ja käyttäjätunnus.



Kuva 27 Sovelluspalvelimen valinta

Asensin ensimmäisessä vaiheessa Tomcatin, joten valitsemme sen. Lisäksi laitetaan merkki kohtaan ”*Datasource with JNDI name ’java:/syncopeMasterDataSource’:* ”, koska se on Tomcatin context.xml tiedostoon määriteltynä.



Kuva 28 Sovelluspalvelimen asetukset

Kuvassa 6 määriteltiin käyttäjänimi ja salasana, jota käytetään tässä. *Host* ja *port* kohta laitetaan *localhost* ja *8080*, koska Tomcat on samalle koneelle asennettu ja se kuuntelee porttia 8080.

Next -painiketta painaessa asennusprosessi alkaa. Pian alkamisen jälkeen tulee kuitenkin kuvan 27 mukainen virheilmoitus. Verkosta ja Syncopen dokumentaatiosta ei löytynyt syitä, mistä ongelma voi johtua, eikä myöskään Syncopen asennuslokeista. Dokumentaatiosta löytyi, että polkuihin */opt/syncope/syncope/core/src/main/resource/domains/Master.properties* ja */opt/syncope/syncope/core/src/main/resource/domains/provisioning.properties* pitää lisätä rivejä, mikäli ne puuttuvat. Lisäsin kuvien 28 ja 29 mukaiset rivit, mutta sillä ei ollut vaikutusta asennusprosessiin.

Kun omista yrityksistä ratkoa ongelmaa ei ollut apua, pyysin apua tilaajayrityksen henkilöstöltä. Järjestimme palaverin tilaajayrityksen kanssa missä keskustelimme ongelmasta ja ohjelmistosta. Palaverin lopputuloksena päätimme lopettaa Apache Syncopen kehitystyön ja etsimme vaihtoehtoisen ratkaisun ongelmaan.

Kuva 29 Virheilmoitus

```
quartz.jobstore=org.quartz.impl.jdbcjobstore.StdJDBCDelegate
quartz.sql=tables_mysql_innodb.sql
```

Kuva 30 Provisioning properties

```
Master.driverClassName=com.mysql.jdbc.Driver
Master.url=jdbc:mysql://localhost:3306/syncope?characterEncoding=UTF-8&relaxAutoCommit=true&relax
AutoCommit=true
Master.schema=
Master.username=root
Master.password=Oppari-1!
Master.databasePlatform=org.apache.openjpa.jdbc.sql.MySQLDictionary(blobTypeName=LONGBLOB,dateFra
ctionDigits=3)
Master.orm=META-INF/spring-orm.xml
Master.pool.validationQuery=SELECT 1
Master.pool.maxActive=10
Master.pool.minIdle=2
Master.audit.sql=audit_mysql_innodb.sql
```

Kuva 31 Master Properties