Mika Piipponen

Kartoitustyökalu osana konfiguraationhallintaa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

23.11.2016

Metropolia

Tekijä Otsikko Sivumäärä Aika	Mika Piipponen Kartoitustyökalu osana konfiguraationhallintaa 40 sivua 23.11.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja	Lehtori Erik Pätynen

Insinöörityön tarkoituksena oli perehtyä pintapuolisesti ITIL Palveluomaisuuden- ja konfiguraationhallinnan prosessiin sekä hieman tarkemmin syventyä IT-infrastruktuurin kartoitustyökaluun. Tavoitteena oli täyttää opinnäytetyöntekijän puutteellisia tietoja palveluomaisuuden- ja konfiguraationhallinnasta ja auttaa paremmin ymmärtämään ja näin kehittämään konfiguraationhallintaa käytännöntyössä. Päätavoitteena oli konkretisoida käytännössä opittua tietoa kartoitustyökalun käytöstä dokumentoinnin avulla ja perehtyä paremmin työkalun ominaisuuksiin ja käyttöön valmistajan virallista dokumentaatiota apuna käyttäen.

Tavoitteiden mukaisesti kirjoitus- ja tiedonhakuprosessi loivat parempaa ymmärrystä konfiguraationhallinnan prosessista ja tärkeydestä osana organisaation toimintaa ja on auttanut käytännössä konfiguraationhallinnan ylläpitotyössä. Lisäksi kartoitustyökaluun tutustuminen tarkemmin on auttanut laajentamaan käytännössä kartoitusten kattavuutta ja antanut ideoita kehityskohteille tämän työkalun käytössä.

Konfiguraationhallinta on nykypäivänä tärkeässä osassa jokaisen IT-palveluita tarjoavan organisaation toimintaa. Palveluiden ja niitä tukevan infrastruktuurin jatkuvasti kehittyessä ja muuttuessa monimutkaisemmiksi ja vaikeammin hallittaviksi kokonaisuuksiksi perinteisin hallintamenetelmin, kuten esimerkiksi Excel-taulukoiden ja tukkimiehenkirjanpidon muodostaessa konesalin inventaariolistan, tarvitaan kehittyneempiä työkaluja tukemaan palveluiden jatkuvaa toimintaa ja ylläpitoa. Tällaisia työkaluja konfiguraationhallinnassa nykypäivänä ovat muun muassa konfiguraatiotietokanta ja kartoitustyökalu. Kartoitustyökalun tehtävänä on käytännössä auttaa kartoittamaan IT-infrastruktuuria mahdollisimman automaattisesti ja työtunteja säästäen. Sen tarkoituksena on havaita ja tuoda organisaation käyttöön tarkkaa ja ajantasaista tietoa sen ylläpitämästä IT-ympäristöstä. Se ei ole välttämättä vain työkalu fyysisten ja virtuaalisten laitetietojen keräämiseen, vaan sen avulla voidaan lopulta mallintaa helposti järjestelmien tai palveluiden muodostamia kokonaisuuksia ja tarkastella niiden eri osia ja niiden sisäisiä riippuvuuksia. Konfiguraatiotietokannan tarkoituksena taas on tallentaa ja esittää muun muassa kartoitustyökalun tuottamia tietoja. Nämä taas luovat lopulta pohjaa palvelun helpommalle analysoinnille ja sitä myöten kehittämiselle.

Avainsanat	ITIL, SACM, BMC, Discovery, ADDM, CMDB, konfiguraationhallinta, omaisuudenhallinta, IT-infrastruktuuri,

Author(s) Title Number of Pages Date	Mika Piipponen Discovery tool part of Configuration management 40 pages 23 November 2016
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor	Erik Pätynen, Senior Lecturer

The goal of this study was to research the ITIL Service Asset and Configuration Management process and analyze what part the discovery tool serves in the process of configuration management. The primary purpose was to document how the discovery tool is used in practical daily work and research the manufacturer's official documentation to provide more detailed information of the features of the discovery tool and get new ideas of how to develop the use of the tool in client environments.

As a result, better understanding of the service asset and configuration management process and the discovery tool was achieved. The thesis gives some tools and ideas to pursuit excellence for anyone working as a beginner Service Asset and Configuration Management Analyst. Secondly, the study on the techniques of the discovery tool has helped to gain higher coverage percentage of discovered systems in different client environments and it has given some development ideas to gain better security while managing the tool.

A well planned and implemented service asset and configuration management process is one of the main pillars of a modern IT service organization when its services and IT infrastructure pursuits continual development. As part of an organization, it provides detailed and up-to-date information and a complete top-to-bottom model on what components make up the IT services that the organization manages. With the data and information that asset and configuration management provides it enables continual development of IT services. The discovery tool is a significant part of modern asset and configuration management as it provides an automated solution to discover and produce precise and trustworthy data of the components and dependencies of IT infrastructure.

Keywords	ITIL, SACM, BMC, Discovery, ADDM, CMDB, Cofiguration Management, Asset Management, IT infrastructure

Sisällys

Lyhenteet

CCTA	Central Computer and Telecommunications Agency. Britannian valtion tietojenkäsittelyn ja televiestinnän laitos.
ITIL	Information Technology Infrastructure Library. AXELOS Ltd:n ylläpitämä tietotekniikan infrastruktuurikirjasto hyväksi havaituista käytänteistä tietotekniikan alalla.
CMDB	Configuration Management Database. Konfiguraationhallintatietokanta.
SACM	Service Asset and Configuration Management. Palveluomaisuuden- ja konfiguraationhallinta.
RFC	Request for Change. Muutospyyntö.
OSI	Operating System Instance. Käyttöjärjestelmäinstanssi.
WMI	Windows Management Instrumentation. Instrumentti Windows-järjestelmien hallintaan.
API	Application Programming Interface. Sovellusliittymä tai palvelurajapinta.
SSH	Secure Shell. Protokolla salattuun tiedonsiirtoon.
SNMP	Simple Network Management Protocol. Protokolla verkonhallintaan.
LDAP	Lightweight Directory Access Protocol. Kevennetty hakemistopalveluprotokolla.
FIPS	Federal Information Processing Standard. Yhdysvaltain liittovaltion tiedonkäsittelystandardi salausalgoritmien ja salausavainten käyttöön.
STIG	Secure Technical Implementation Guidelines. Yhdysvaltain puolustuslaitoksen laatimia suosituksia teknisten toteutuksien tuottamiseen.

1 Johdanto

IT-palveluita tuottavan yrityksen tai organisaation yhtenä tärkeimpänä osana liiketoimintaa on sen tuottama tai ylläpitämä IT-infrastruktuuri, johon käytännössä kaikki nykyaikaisen organisaation toiminnot nojautuvat. Jotta tämä organisaation kivijalka olisi tukeva ja sen kehittäminen vahvemmaksi ja organisaatiota paremmin kannattelevaksi sen jatkuvasti muuttuessa olisi mahdollista, on kaiken ytimessä luotettava tieto siitä, mistä IT-infrastruktuuri koostuu: mitä se sisältää, missä sen eri osat ovat, mitkä sen eri osat vaikuttavat mahdollisesti muihin osiin tai tuotettavaan palveluun, kuka sitä ylläpitää, kenen vastuulla on mikäkin osa, kuinka laskea kustannukset ja kuinka paljon palvelusta kannattaa laskuttaa asiakkaalta. Jos jokin sen osa tai osia rikkoutuu tai katoaa, mistä löydetään nopeasti ja vaivatta tieto siitä mitä pitäisi korjata tai hankkia tilalle? ITIL-tietotekniikan infrastruktuurikirjaston kuvaamat palveluomaisuuden- ja konfiguraationhallinnan viitekehykset auttavat hakemaan vastauksia näihin kysymyksiin ja moniin muihin organisaation toiminnan kannalta oleellisiin kysymyksiin. Sen tarkoituksena on ylläpitää tietoa. Tieto perinteisesti on voimaa ja luotettava ja ajantasainen tieto luo pohjaa organisaation kehitykselle ja tuottavuudelle.

Yhtenä palveluomaisuuden ja konfiguraationhallinnan tärkeänä osana ovat erilaiset työkalut, jotka tuottavat ja keräävät tietoa organisaation hallinnassa olevasta IT-infrastruktuurista. BMC Discovery on yksi tällainen työkalu, ja tässä insinöörityössä on tarkoituksena tutustua tähän työkaluun, syventää ja konkretisoida jo käytännössä opittuja tietoja ja ymmärrystä itse työkalusta ja sen käytöstä ja myös selventää yleisellä tasolla ITIL-palveluomaisuuden- ja konfiguraationhallinnan prosesseja. Työssä perehdytään BMC Discoveryn yleisiin ominaisuuksiin, perusvaatimuksiin ja toimintaan siltä pohjalta, miten tätä työkalua on käytetty kirjoittajan omassa työssä. Tarkoituksena ei ole paneutua kaikkiin Discoveryn ominaisuuksiin ja metodeihin tai pitemmälle jalostettuihin toimintoihin kuten sovelluspalveluiden kuvaamiseen ja siihen liittyen infrastruktuurin tarkempaan skannaamiseen sovellustasolla ja mallintamiseen, joka olisi luonnollinen seuraava vaihe. Tämä muun muassa siitä syystä, ettei kirjoittajan työssä ole vielä käytännössä toteutettu tai hyödynnetty läheskään kaikkia Discoveryn tarjoamia mahdollisuuksia.

2 ITIL- tietotekniikan infrastruktuurikirjasto

IT Infrastucture Library (ITIL) eli tietotekniikan infrastruktuurikirjasto on Ison-Britannian hallituksen ja Capita Oy:n yhteishankkeen AXELOS Ltd:n ylläpitämä kokoelma dokumentteja, jotka sisältävät viitekehyksen hyväksi havaituista käytännöistä IT-palveluiden hallintaan ja tuottamiseen. Se on malli tehokkaampaan johtamiseen, hallintoon sekä IT-palveluiden suunnitteluun ja tuottamiseen. Sen tarkoitus ei ole olla standardi tai tiukka teoria siitä, miten asiat pitää tehdä, vaan tarkoituksena on antaa organisaatiolle vapaus valita itselleen sopivimmat työkalut, joita voidaan täydentää omien tarpeiden ja vaatimusten mukaan. ITIL:n tarkoituksena on auttaa organisaatiota muutoksessa käsityöammatista tehokkaaksi teollisuudenalaksi. Sen pyrkimyksenä on jatkuva kehitys. [1.]

1980-luvun loppupuolella Ison-Britannian valtion tietojenkäsittelyn ja televiestinnän laitoksen, Central Computer and Telecommunications Agencyn (CCTA) tarkoituksena oli kehittää tehokkaita ja suorituskykyisiä tapoja tuottaa laadukkaampia ja samalla kustannustehokkaampia IT-palveluita. Tästä lähti liikkeelle ympäri maailmaa tunnustettujen ja käytännössäkin todettujen IT-prosessiviitekehyksien kehittäminen. [3.]

ITIL-kirjoja on julkaistu vuodesta 1989 lähtien, ja ITIL itsessään on tähän päivään mennessä kehittynyt versioon numero 3. Tällä hetkellä ITIL v3 sisältää viisi osa-aluetta, jotka painottavat palvelunäkökulmaa ja jotka on jaettu palvelun elinkaaren mukaan:

- Palvelustrategia (Service Strategy) kuvaa palvelustrategiaa ja arvontuottamista, IT-palvelujen kohdistamista liiketoiminnan tarpeisiin, palvelustrategian suunnittelua ja käyttöönottoa.
- Palvelusuunnittelu (Service Design) kuvaa palvelujen suunnittelun tavoitteita ja elementtejä, palvelumallin valintaa, kustannusmalleja, riskejä, analyysejä, palvelusuunnitelman käyttöönottoa sekä palvelujen mittausta ja valvontaa.
- Palvelutransitio (Service Transition) kuvaa organisaation ja organisaatiokulttuurin muutoksen hallintaa, tiedon hallintaa (Knowledge Management), palvelun tiedon hallintajärjestelmää (Service Knowledge Management System), menetelmiä ja käytäntöjä sekä työkaluohjelmistoja ja palvelujen mittaamista ja kontrollointia.
- Palvelutuotanto (Service Operation) kuvaa sovellusten hallintaa, muutoksen, hallintaa, tuotannon hallintaa, kontrolliprosesseja ja funktioita sekä mittausta että valvontaa. [2.]

- Jatkuva palvelun kehittäminen (Continual Service Improvement) kuvaa organisaatio- ja kulttuurimuutoksen hallintaa, kehittämisen liiketoiminta- ja teknologia-ajureita, menetelmiä ja käytäntöjä sekä työkaluja, mittaamista ja valvontaa. [2.]

Kuvassa 1 on havainnollistettu ITIL:n osia: kuinka sen käytännöt ja suositukset tukevat ja auttavat kehittämään palvelun ydintä eli palvelun strategiaa, jonka ohjaamana toimivat sen tarpeiden mukaan luodut toiminnot. Näitä toimintoja ovat palvelun suunnittelu sen rakenteen muutokset ja kehitys sekä palvelun jatkuvat operatiiviset toimet, joita kaikkia tulee mitata ja seurata, jotta organisaation kokonaisvaltainen kehitys on mahdollista tuottavasti.

Kuva 1. ITIL Elinkaarimallin toimintamalli [4].

3 Palveluomaisuuden- ja konfiguraationhallinta

SACM:n, service asset and configuration management, eli palveluomaisuuden- ja konfiguraationhallinnan prosessien tarkoituksena on kehittää palvelun kokonaistehokkuutta, vähentää palvelun kustannuksia ja riskejä, joita huono tai puuttuva konfiguraationhallinta aiheuttaa. Tällaisia riskejä ovat muun muassa palvelukatkokset, sanktiomaksut, liian suuret lisenssikulut ja epäonnistuneet auditoinnit. [4.]

SACM:n tehtävänä on antaa organisaatiolle ajantasaista ja luotettavaa tietoa sen ylläpitämien IT palveluiden komponenteista ja omaisuudesta, ja näin mahdollistaa

- muutosten ja jakeluiden onnistunut ennustettavuus ja arviointi sekä suunnittelun, toimittamisen ja niiden jäljitettävyyden
- tehokkaamman häiriön- ja ongelmanratkaisu
- sovitun palvelutason ja -takuun toimittaminen
- tarkempi standardien, lakien ja säädöksien noudattaminen
- kyky tunnistaa palvelusta aiheutuvat kustannukset [4].

SACM-prosessi on keskeisessä osassa organisaation liiketoimintaa, vaikkei se siihen välttämättä vaikuta suorasti.

Palveluomaisuuden- ja konfiguraationhallintaan kuuluu viisi elementtiä:

1. Suunnittelu: Määritellään strategia, politiikat, laajuus, tavoitteet, roolit, vastuut, prosessit, menettelytavat ja työkalut.

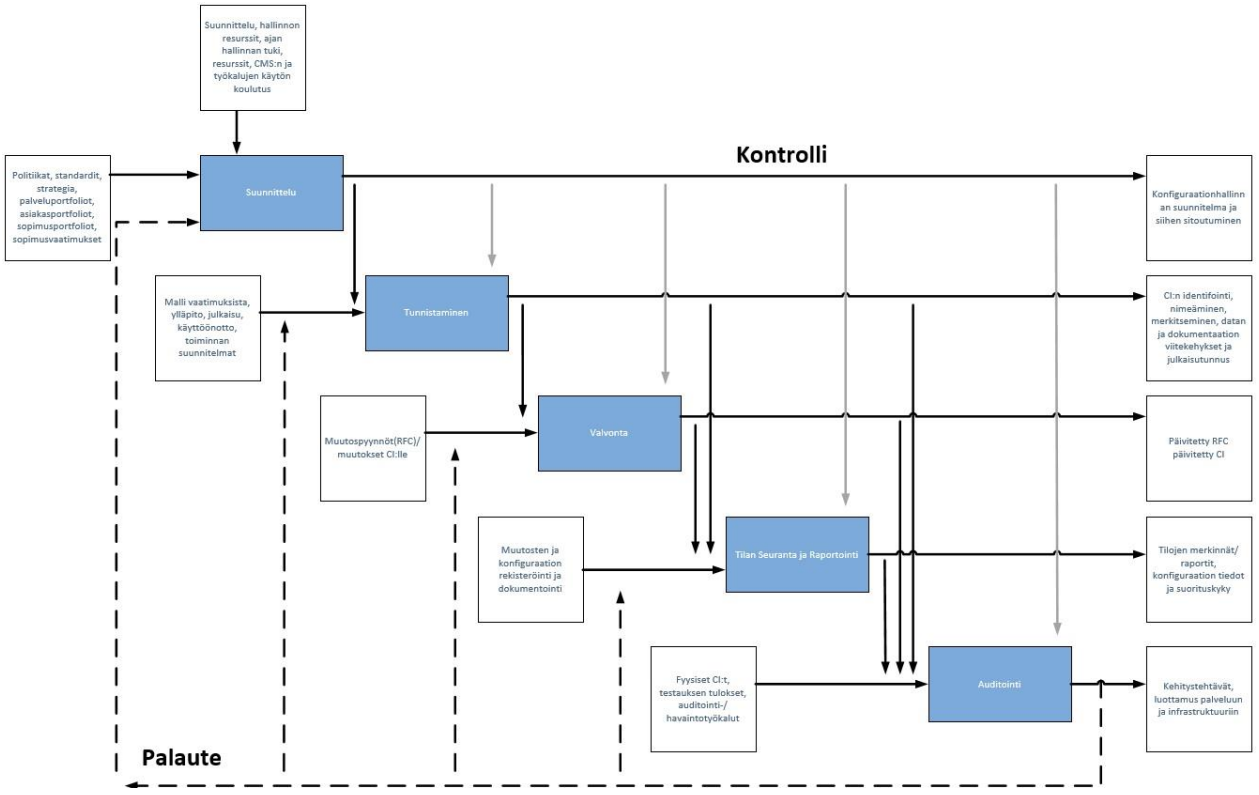
2. Tunnistaminen: Tunnistetaan ja dokumentoidaan konfiguraation rakenneosat (engl. Configuration Item), niiden väliset suhteet ja nimikoidaan ne niin, että vastaavat konfiguraatiotietueet löydetään. Nämä tiedot sisältävät uniikin tunnistetiedon, kuten sarjanumeron ja muut suunnitelmassa määritellyt pakolliset tiedot. Määritellään konfiguraation rakenneosien attribuutit ja suhteet. [4.]

3. Valvonta: Varmistetaan, että tunnistettujen ja dokumentoitujen konfiguraation rakenneosien koko elinkaari hankinnasta poistoon on kuvattu. Se onnistuu kontrolloimalla rakenneosien lisäämistä, muuttamista, vaihtamista tai poistamista vain hyväksytyillä muutos- tai palvelupyynnöillä (engl. request for change, RFC).

4. Tilan seuranta ja raportointi: Seurataan konfiguraation rakenneosien tilaa läpi niiden elinkaaren palvelupyyntöjen ja raportoinnin avulla. Erilaisia tiloja voivat olla esimerkiksi tilattu, toimitettu, asennuksessa, pois päältä, käytössä, poistettu, varastoitu tai hävitetty.

5. Auditointi: Varmistetaan ja todennetaan konfiguraation rakenneosan olemassa olon paikkansapitävyys esimerkiksi fyysisesti tai kyseessä olevan rakenneosan omistajan vahvistuksella tai elektronisesti havaintotyökalulla tai kaikilla kolmella. [4.]

Kuvassa 2 on havainnollistettu näiden viiden elementin yhteyttä ja vaikutusta toisiinsa.



Kuva 2. SACM:n prosessin elementit ja niiden yhteydet toisiinsa [4].

3.1 Konfiguraation rakenneosat

Konfiguraation rakenneosa voi olla fyysistä omaisuutta, palvelun komponentti tai muu kohde, joka on tai tulee olemaan konfiguraationhallinnan valvonnassa. Konfiguraation rakenneosa voi vaihdella laajasti kompleksisuudesta, koosta ja tyypistä, niin kokonaisesta palvelusta tai järjestelmästä sisältäen laitteiston ja yksittäisen ohjelmiston, dokumentin ja työntekijän, yhteen ohjelmiston osaan tai laitteiston komponenttiin. Ne voivat olla ryhmitelty ja hallittuja yhdessä: esimerkiksi palvelin ja sen eri komponentit voivat olla jokainen oma rakenneosansa. Konfiguraation rakenneosa voi olla periaatteessa lähes mitä tahansa jolla on attribuutteja ja joka halutaan dokumentoida. [5.]

Esimerkkejä erilaisista konfiguraation rakenneosista:

- Palvelun elinkaaren rakenneosa, kuten liiketaloudellinen oikeutus (engl. business case), palvelunhallintasuunnitelma, palvelun elinkaaren suunnitelma, julkaisu, testaus tai muutos suunnitelma. Palveluja kuvaava rakenneosa: miten niitä toimitetaan, odotettuja hyötyjä ja kuluja.

- Palvelun rakenneosat, kuten

    - palvelukyvyn ominaisuudet: johto, organisaatio, prosessit, tieto ja työntekijät

    - palvelun resurssit: taloudellinen pääoma, järjestelmät, applikaatiot, data, infrastruktuuri ja laitteistot sekä työntekijät

    - palvelumallit

    - huoltopaketit

    - julkaisupaketit

    - palvelun hyväksyntäkriteerit. [5.]

- Sisäiset konfiguraation rakenneosat, joita tarvitaan palvelun tai infrastruktuurin tuottamiseen ja ylläpitämiseen,. kuten fyysiset tai aineettomat rakenneosat, esimerkiksi rakennus, toimisto, konesali, ohjelmisto palvelin [5].

- Ulkopuoliset rakenneosat, kuten asiakasvaatimukset ja palvelusopimukset, julkaisut tuotteen tai palvelun toimittajilta sekä ulkoistetut palvelut [5].

Konfiguraation rakenneosa on määrittelyltään hyvin laaja käsite. Sen takia on tärkeää tarkkaan määritellä, mitä rakenneosia on oleellista dokumentoida palvelun kannalta. Ei ole kustannustehokasta eikä hyödyllistä dokumentoida sellaista tietoa, millä ei ole minkäänlaista käyttöarvoa, sillä kaikkea tietoa tulee pystyä myös ylläpitämään. Ei siis ole järkevää tuhlata resursseja sellaisen tiedon ylläpitämiseen, jota ei kuitenkaan hyödynnetä.

3.2 Konfiguraationhallintajärjestelmä

Configuration management system (CMS) eli konfiguraationhallintajärjestelmä on työkalupakki palveluomaisuuden- ja konfiguraationhallinnan (SACM) toteuttamiseksi ja tukemiseksi. Sen tehtävänä on kerätä, varastoida, päivittää sekä analysoida ja esittää konfiguraation rakenneosat ja niiden väliset suhteet. SACM ylläpitää konfiguraationhallintajärjestelmää, ja kaikki IT-palvelunhallinnan prosessit käyttävät sitä. [7.]

Konfiguraationhallintajärjestelmä nimensä mukaisesti on järjestelmä ja sisältää useita eri työkaluja tiedon esittämiseen, raportointiin, analysoimiseen, ylläpitämiseen ja tallentamiseen, sen tuottamiseen ja keräämiseen sekä näiden kaikkien kokonaisuudeksi integroimiseen. [7.] Näitä työkaluja ovat

- havaintotyökalu tai -työkalut (Discovery Tool) keräämään, ylläpitämään ja auditoimaan tietoa rakenneosista
- yksi tai useammat konfiguraatiotietokannat (CMDB), jotka sisältävät tiedot konfiguraation rakenneosista (CI)
- raportointityökalu tai -työkalut
- rajapinnan muille konfiguraationhallintajärjestelmän (integrated CMDB) työkaluille [7].

3.3 Havaintotyökalu

Havaintotyökalun tai -työkalujen tehtävänä on kerätä ja tuottaa tietoa IT-infrastruktuurista konfiguraatiotietokantaan (CMDB), ylläpitää ja auditoida tätä tietoa sekä erityisesti automatisoida näitä toimintoja. Automaattiset havaintotyökalut tarjoavat tehokkaan ja helpon tavan kerätä ajantasaista tietoa IT-ympäristöstä, mutta valmistajasta riippuen ne eivät välttämättä pysty keräämään kaikkea tarvittavaa tietoa erilaisista järjestelmistä tai laitteista. Toisaalta ne saattavat johtaa keräämään liikaa tietoa ja näin luoda monimutkaisemman ja vaikeammin hallittavan kokonaisuuden kuin todellisuudessa on tarve, mikä taas voi olla haitaksi. [7.] Havaintotyökalu tai -työkalut eivät siis korvaa hyvin suunniteltua konfiguraationhallinnan prosessia ja organisaation sitoutumista sen toteuttamiseen. Ihmisen tekemää manuaalityötä tarvitaan myös aina tietynlaisen tiedon täyttämiseen ja ylläpitämiseen sekä tietenkin itse työkalun ylläpitämiseen ja valvontaan. Manuaalisesti täydennettävää ja ylläpidettävää tietoa ovat muun muassa omistajuudet, tukipalvelu ja -henkilötiedot, sijainti, sovellukset korkealla tasolla ja niiden yhteydet palveluihin ja niiden alla oleviin rakenneosiin. Havainto- ja kartoitustyökalut ovatkin avuksi alemmalla tasolla, kun kartoitetaan verkossa olevia fyysisiä ja virtuaalisia komponentteja, tietoa niiden sisältämistä komponenteista ja ohjelmistoista sekä näiden kaikkien välisistä yhteyksistä ja riippuvuuksista. Näitä tietoja voidaan mahdollisuuksien mukaan tuottaa konfiguraatiotietokantaan erilaisista lähteistä.

Automaattiset havaintotyökalut pyrkivät kartoittamaan IT-infrastruktuurin kaikki osa-alueet. Etuna on tiedon keräämisen ja konfiguraationhallintajärjestelmään syöttämisen yksikertaisuus ja helppous. Kun tavoitteena on mahdollisimman automatisoitu ja yksinkertaistettu ympäristö, on tällainen työkalu välttämätön osa sitä.

Esimerkkejä automaattisista havaintotyökaluista:

- BMC Discovery
- HP Universal Discovery
- IBM Tivoli Application Dependency Discovery Manager
- ServiceNow Discovery.

Mainittujen ohjelmistojen valmistajista jokainen tarjoaa myös oman kokonaisratkaisunsa palvelu- ja konfiguraationhallintaan.

Lisäksi on kohdistettuja havaintotyökaluja esimerkiksi Ciscon Secure Device Manager (SDM) IOS-pohjaisille verkkolaitteille tai Microsoft System Center Configuration Manager Windows-järjestelmille. Ne antavat tarkasti tiedon omasta kohdealueestaan. Silloin yleensä tarvitaan useita eri työkaluja haluttujen osa-alueiden kattamiseksi. Ongelmaksi voi tulla näiden työkalujen integrointi konfiguraationhallintajärjestelmään. Esimerkiksi voi olla, että niistä ulos saatu data ei ole sopivassa muodossa, jotta sitä voitaisiin syöttää järjestelmään, jolloin tätä tietoa joudutaan rikastamaan joko manuaalisesti tai sitä varten räätälöidään oma järjestelmä. Pienessä ympäristössä tällaiset yksittäiset työkalut saattavat olla kustannustehokkain ratkaisu.

Sopivan työkalun valinnan määrittelee muun muassa se, millaiset tavoitteet konfiguraationhallinnalla on, millaisia prosesseja noudatetaan, minkä kokoista ja millaista ympäristöä ylläpidetään, millaisia työkaluja on jo ennestään hankittu ja käytössä, ovatko ne integroitavissa muihin konfiguraationhallintajärjestelmän työkaluihin, onko organisaatio sidoksissa johonkin tiettyyn valmistajaan tai ympäristöön sekä tietenkin lopulta hinta ja arvioidut kokonaiskustannukset.

4 Kartoitustyökalu BMC Discovery

4.1 Sovelluslaite BMC Discovery

BMC Discovery – edesmennyt BMC Atrium Discovery and Dependency Mapping – on sovelluslaite IT-omaisuuden kartoittamiseksi mahdollisimman automaattisesti. Se on alun perin Tideway nimisen yrityksen kehittämä tuote ja Tidewayn yritysoston myötä sen kehitystä on jatkanut BMC Software Inc. [10.]

BMC Software Inc.

BMC Software, Inc on vuonna 1980 Texasin osavaltiossa Yhdysvalloissa perustettu ohjelmistoalan yritys. Sen nimi tulee perustajajäsenten sukunimistä: Scott Boulette, John Moores ja Dan Cloer. Sillä on yli 10 000 asiakasta, noin 6 000 työntekijää 30:ssä eri maassa ja sen liikevaihto on noin kaksi miljardia Yhdysvaltain dollaria. [8.]

BMC on erikoistunut liiketoiminnan palvelunhallinnan ohjelmistoratkaisuihin. Sen IT ratkaisut ja tuotteet keskittyvät tietotekniikan palvelunhallintaan, tietotekniikan toimin-

toihin, pilvipalveluiden hallintaan, tietotekniikan automaatioon, sekä keskustietokoneratkaisuihin. Sen tuotteita on laajalti käytössä ympäri maailmaa erikokoisissa yrityksissä ja organisaatiossa. [9.]

BMC Discovery

Discoveryn tarkoituksena on pyrkiä sen sisältämien erilaisten työkalujen ja tekniikoiden avulla löytämään ja tunnistamaan verkossa olevat komponentit ja keräämään niistä oleelliset tiedot mahdollisimman nopeasti ja kuluttamatta ylimääräisiä resursseja. Tämä mahdollistaa lopulta havaitun datan pohjalta mallintaa näiden komponenttien muodostamat sovellukset ja palvelut.

Discoveryn avulla voidaan automatisoida iso osa tiedon syöttämisestä ja ylläpitämisestä konfiguraatiotietokantaan. Kartoittamalla IT-ympäristöä se tunnistaa verkkoon liitetyt IP-osoitteella varustetut komponentit, kerää tietoja niistä ja kuvaa yhteydet ja riippuvuudet näiden eri osien välillä. Se mahdollistaa nopeamman, helpomman ja varman konfiguraatiotietokannan populoinnin ja kasvattaa tiedon luotettavuutta automaattisesti päivittämällä sitä ajastetusti tietokantaan.

Oleellisin BMC Discoveryn osa ja vahvuus sekä aivot on sen niin sanotussa päättelykoneessa (engl. Reasoning Engine), jonka avulla se analysoi kohdejärjestelmän, suorittaa sen pohjalta kaavamaisesti mahdollisia lisäkyselyitä ja kaiken kokonaisuudessaan kerätyn tiedon avulla muodostaa mallin tarkasteltavasta ympäristöstä. Discoveryn päättelykone on niin sanotusti tapahtuma-ehto-toimintapohjainen (engl. Event-Condition-Action, ECA) ja sen apuna toimii BMC:n luoma The Pattern Language (TPL) eli kaavakieli, joka luo logiikkaa Discoveryn toimintaan. [11.] Parasta tähän liittyen on, että Discoveryssa on BMC:n joka kuukausi päivittämä teknologiatietokirjasto, joka kattaa todella laajan määrän erilaisia laitteita, järjestelmiä, sovelluksia ja ohjelmia. Sen lisäksi Discoveryn ylläpitäjän ei tarvitse tukeutua vain BMC:n tuottamiin kaavoihin ja skripteihin, vaan TPL-kielellä voidaan muokata jo olemassa olevia kaavoja tai kirjoittaa kokonaan uusia tunnistekaavoja esimerkiksi tunnistamattomille ohjelmille, järjestelmille tai periaatteessa mille tahansa.

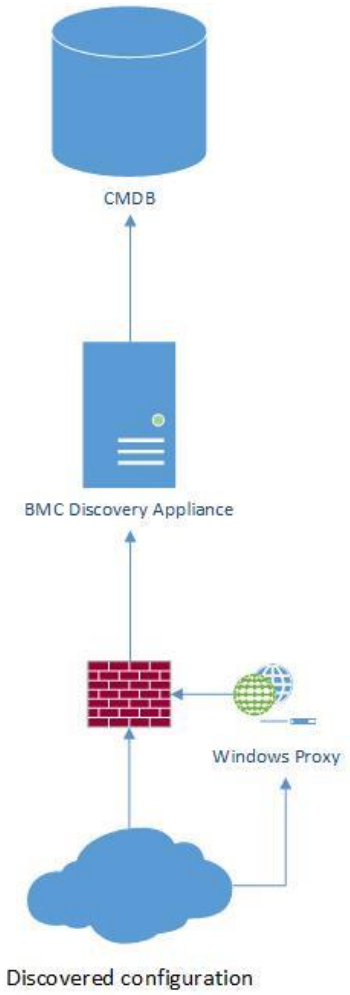
BMC Discovery on virtuaalinen valmisjärjestelmä, joka on rakennettu 64-bittisen Linux RedHat-käyttöjärjestelmän päälle. Se sisältää muun muassa avoimen lähdekoodin BerkleyDB-tietokantamoottorin, Apache Tomcat Web-palvelun käyttöliittymää varten

sekä erilaisia työkaluja laitetietojen keräämiseen. Suurin osa näistä eri työkaluista on koodattu Python-ohjelmointikielellä. [10.]

Pääasiassa kaikki Discoveryn hallinto- ja ylläpitotoimet sekä käyttö tapahtuvat web-käyttöliittymän kautta, joka on helppo omaksua. Itse käyttöjärjestelmää hallitaan konsoliyhteyden kautta, mutta web-käyttöliittymän toiminnot ovat käytettävissä myös komentotulkissa.

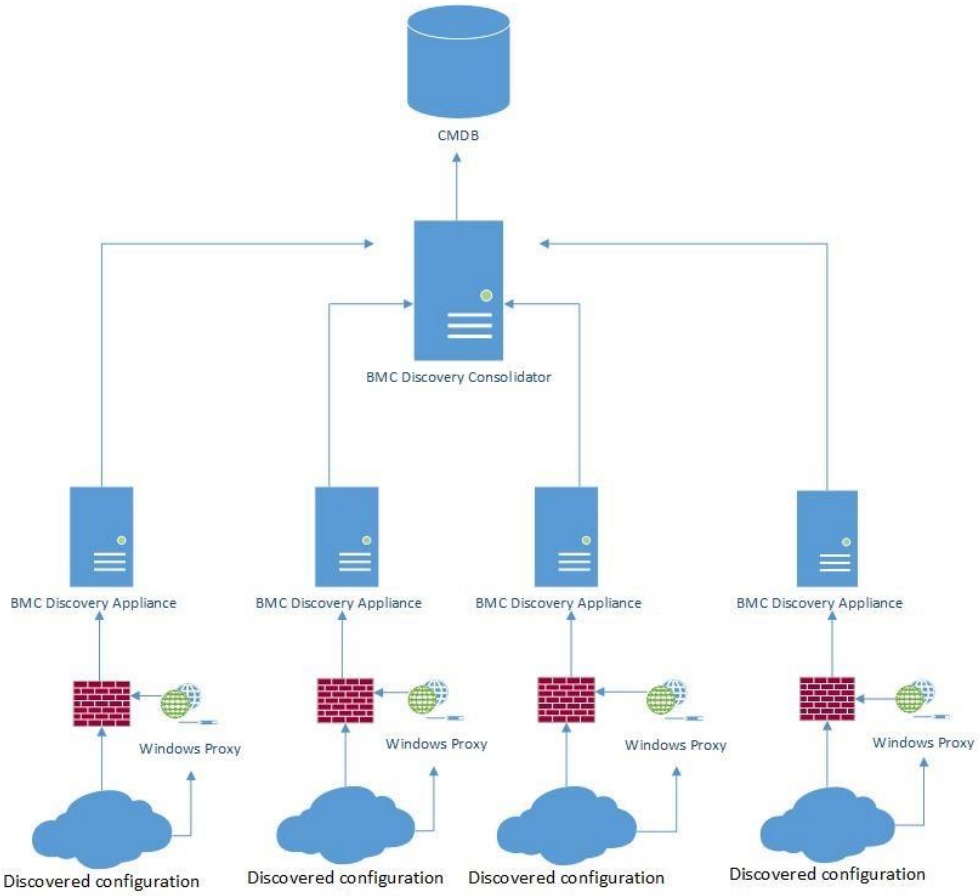
BMC Discovery asennetaan joko skanneriksi (engl. Discovery Scanning Appliance) tai konsolidaattoriksi (engl. Discovery Consolidation Appliance). Lisäksi kokonaisuuteen kuuluu erillinen Proxy-hallintasovellus Windows-palvelimelle. Sitä tarvitaan Windows-laitteiden kanssa kommunikoimiseen. Se asennetaan tutkittavaan toimialueeseen. Proxy-hallintasovellus ei välttämättä vaadi dedikoitua palvelinta kuten skanneri ja konsolidaattori vaan se voi olla muussakin käytössä, mutta ei ole suositeltavaa asentaa sitä palvelimelle, joka isännöi liiketoiminnan kannalta olennaista palvelua, koska Proxy-sovellus käyttää skannauksien aikana jonkin verran isäntäkoneen resursseja ja sen kautta kulkee kaikki data kohteen ja skannerin välillä.

Skannerin ja konsolidaattorin erona on, että skanneri nimensä mukaisesti tekee kartoitustyön ja konsolidaattorin tehtävänä on koota yhdellä tai useammalla skannerilla kerätty data ja synkronoida se keskitetysti konfiguraatiotietokantaan ja näin vastata siitä aiheutuvasta kuormasta sekä toimia yhtenäistettynä kantana raportoimiseen. Molemmilla on siis oma tehtävänsä tietynlaisessa kokonaisuudessa, mutta molemmilla voidaan kuitenkin suorittaa täsmälleen samoja tehtäviä. Yksinkertaisimmillaan yhdellä Discovery palvelimella hoidetaan kaikki Discoveryn tehtävät skannaamisesta tietokantasynkronointiin, kuten kuvassa 3 on esitetty.

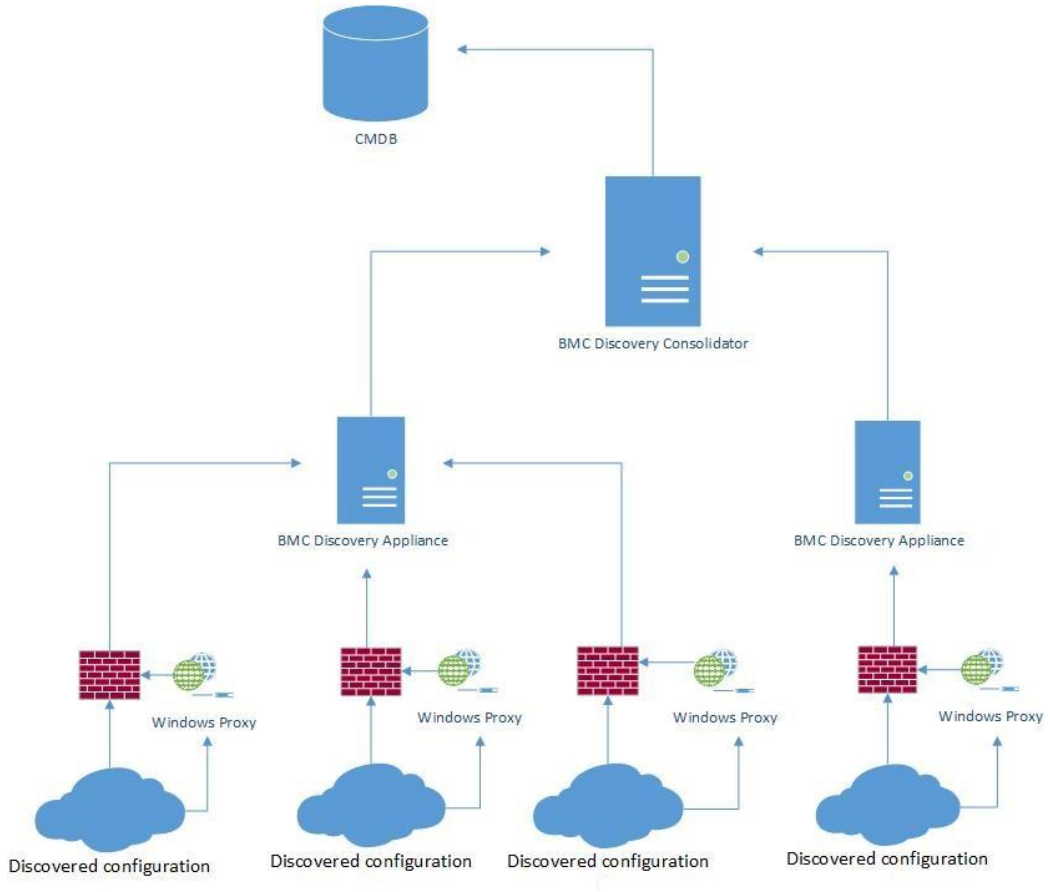


Kuva 3. Yhden Discovery-skannerin kokonaisuus.

Syynä yhden tai useamman skannerin ja konsolidaattorin käyttöön voidaan pitää muun muassa verkon rakennetta eri segmentteineen ja palomuureineen sekä erilaisine tietoturvapolitiikkoineen, jolloin yhdeltä skannerilta ei saa tai voi olla reittiä kaikkiin verkon eri osiin. Esimerkiksi voidaan haluta minimoida palomuuriavauksia tarkasteltavasta ympäristöstä ulos ja sisään, jolloin voidaan sijoittaa skanneri ja Windows-välityspalvelin kyseessä olevaan verkkoon ja konsolidaattori sen ulkopuolelle, kuten kuvissa 4 ja 5 on havainnollistettu. Näin tarvitaan vain yhden portin avaus tutkittavan järjestelmän ja konsolidaattorin välille.



Kuva 4. Esimerkki neljän täysin erillisen konfiguraation ja skannerin kartoittavasta kokonaisuudesta, jotka raportoivat konsolidaattorille. Jokainen konfiguraatio voisi esimerkiksi kuvata erillistä asiakasta.



Kuva 5. Toinen esimerkki usean erillisen konfiguraation ja skannerin kokonaisuudesta. Tässä tapauksessa toinen skannereista kartoittaa useamman eri toimialueen tai konfiguraation, joilla voidaan kuvata esimerkiksi eri asiakkaita.

Jos riittävän isossa ympäristössä on rajoitettu aika skannaamista varten, ongelmaksi voi muodostua aika, joka kuluu skannaamiseen yhdeltä skannerilta. Tällöin voi olla tarpeen jakaa osoitteita usealle skannerille ja jakaa kuormaa. BMC:n arvion mukaan Discovery pystyy käsittelemään noin 500 kohdelaitetta tunnissa. [12.] Skanneri ja konsolidaattori käsittelevät yhtä nopeasti yhden skannatun laitteen. Esimerkiksi jos skannerilta kuluu kohteen skannaamiseen 1 minuutti, niin konsolidaattori käsittelee ja synkronoi yhtä kauan sen tietoja Atrium CMDB:n kantaan eli yhteensä 2 minuuttia kokonaisuudessaan. [12.]

Todellisen elämän esimerkkinä yhdeltä skannerilta asiakkaan noin 4 300 IP-osoitteen – joista noin 240 on onnistuneesti skannattuja laitteita – skannaamiseen ja CMDB-synkronointiin kuluu aikaa keskimäärin 2 tuntia 40 minuuttia. Skannerin resursseina on 4 prosessoria ja 8 000 megabittiä muistia, 55 gigabittiä ja 200 gigabittiä levytilaa. Toisena esimerkkinä yhden skannerin ja konsolidaattorin yhdistelmällä asiakkaan noin 8 600 IP-osoitteen – joista yli 900 on onnistuneesti skannattuja laitteita – skannaamiseen

ja konsolidaattorin CMDB-synkronointiin kuluu yli 3 tuntia. Tässä esimerkissä skannerin resursseina on 4 prosessoria, 16 gigabittiä muistia ja yhteensä 505 gigabittiä levytilaa. Konsolidaattorin resursseina on 4 prosessoria, 16 gigabittiä muistia ja yhteensä 550 gigabittiä levytilaa. Kolmantena esimerkkinä asiakkaan reilun 2000 IP-osoitteen – joista noin 550 on onnistuneesti skannattua laitetta – skannaamiseen ja CMDB synkronointiin konsolidaattorilla kuluu noin 1 tunti ja 10 minuuttia, samalla skannerilla ja konsolidaattorilla kuin toisessa esimerkissä. Kaikissa kolmessa esimerkissä on hyvä huomioida, ettei niissä skannata ollenkaan verkkolaitteita, vain palvelimia, mutta toisessa esimerkissä seassa on myös työasemia, joita ei kuitenkaan synkronoida konfiguraatiotietokantaan.

Tehokkuuteen voivat vaikuttaa monet eri tekijät, esimerkiksi se, kuinka moni tarkasteltavan verkon osoitteista on oikeasti jokin laite ja kuinka moni käyttämätön osoite. Tähän liittyen skannauksen nopeuteen voi vaikuttaa, jos verkossa oleva kytkin tai kytkimet on konfiguroitu vastaamaan, kun osoite on vapaa tai se on reitittämätön. Aina kun Discovery saa vastauksen osoitteesta, se olettaa toisessa päässä olevan laitteen ja näin ollen pyrkii havaintoprosessin mukaisesti selvittämään, mikä laite on kyseessä. Lisäksi skannaukseen kuluvaan aikaan vaikuttaa tietenkin skannattavien järjestelmien kompleksisuus ja kerätyn tiedon määrä esimerkiksi suurista tietokannoista. [14.]

4.2 Discovery-järjestelmän vaatimukset

Lisensointi

BMC Discovery on lisensoitu käyttöjärjestelmäinstanssien (engl. Operating System Intances, OSI) määrän mukaan eli palvelinkäyttöjärjestelmien määrän mukaan. Tämä tarkoittaa, että Discovery palvelimia voidaan asentaa niin monta kuin on tarve, ja yksi lisenssi tarkoittaa sitä, että sillä voidaan skannata esimerkiksi yhtä palvelinta. Esimerkiksi 500 laitteen skannaamiseksi varten tarvitaan 500 lisenssiä ja niin edelleen. BMC Discoveryä ei ole tarkoitettu henkilökohtaisten tietokoneiden kuten pöytäkoneiden tai kannettavien tietokoneiden kartoittamiseen, mutta se on mahdollista. Oletusasetuksilla käyttöjärjestelmät, jotka tunnistetaan niin sanotuiksi henkilökohtaisiksi tietokoneiksi, ohitetaan. Skannattuja henkilökohtaisia tietokoneita ei lasketa mukaan lisensseihin. Tallennuslaitteiden (engl. storage devices) kartoittaminen vaatii erillisen lisenssin, ja niiden tunnistamiseksi ja tiedon keräämiseksi tulee BMC:ltä ladata erilliset tunnistuskaavat. [13.]

Alusta ja resurssit

Discovery toimitetaan käytännössä ISO-tiedostona, josta voidaan asentaa virtuaalipalvelin vain VMware-virtuaaliympäristöön (ESX/ESXi) versioon 4.1 tai uudempaan. Discoveryn uusinta versiota ei enää toimiteta fyysisille alustoille suunniteltuna. Testaus- ja kehitystarkoitukseen alustoina voidaan käyttää myös VMware Workstation 8.0.2:ta ja VMware Player 5.0.3:a tai uudempia versioita. [15.]

BMC:n alustavat suositukset vaadituista virtuaalipalvelimen resursseista on luokiteltu neljään kokoluokkaan riippuen kartoitettavan ympäristön laitteiden lukumäärästä:

- Proof of Concept (POC) – aika rajoitettu konseptiversio, korkeintaan 150 käyttöjärjestelmälle (OSI)

- Baseline – perustaso, korkeintaan 500 käyttöjärjestelmälle (OSI)

- Datacenter – suuri ympäristö, korkeintaan 5 000 käyttöjärjestelmälle (OSI)

- Consolidated Enterprise – 20 000:n tai useamman laitteen ympäristö, jossa voi olla useampia skannereita ja jotka yhdistävät tiedot yhdelle tai useammalle konsolidaattorille [16.]

Virtuaalipalvelimen resurssien suositellaan olevan niin sanottuja varattuja resursseja, jottei suorituskyky pääse vaihtelemaan epäsäännöllisesti [15]. Taulukossa 1 on resurssisuositukset erikokoisten ympäristöjen skannaamiseen.

Taulukko 1. BMC:n resurssisuositukset Discovery-palvelimelle erikokoisten ympäristöjen skannaamiseen [16].

Resurssi	**POC**	**Baseline**	**Datacentre**	**Consolidated Enterprice**
Prosessorit (kpl)	2	2	4	4–8
Välimuisti (GB)	2–4	4–8	16–32	16–32
Levyvälimuisti (GB)	4–8	8–16	16–32	16–32
Tietokantalevy (GB), ilman-varmuuskopioita	37	100	200	200–660
Tietokantalevy (GB), lokaa-lilla varmuuskopiolla	37	200	400	450–1300

Discoveryn tehokkuutta voidaan myös lisätä klusteroinnilla, jolloin suurien ja komplek-sisten ympäristöjen kartoituksesta aiheutuva kuorma jaetaan useamman Discovery-palvelimen kesken. Lisäksi näin saadaan Discovery skaalautumaan helposti todella suurten ympäristöjen skannaamiseen. Koska Discovery on varsin suljettu valmisjärjes-telmä ja sen resurssien kasvattaminen erityisesti massamuistien osalta on lähes mah-dotonta ilman Discovery-palvelimen uudelleen asentamista, on klusterointi suoritusky-vyn kasvattamiseen paras ratkaisu. Periaatteessa lisätään vain uusi palvelin klusteri-ryhmään, jolloin saadaan lisää tehoa skannaukseen tai konsolidointiin.

Windows Proxy -hallintasovelluksen minimivaatimukset isäntäpalvelimelle ovat Win-dows 2003 SP2 32-bit tai 64-bit tai uudempi Windows-palvelin, välimuistia 2 Gb.

Verkko

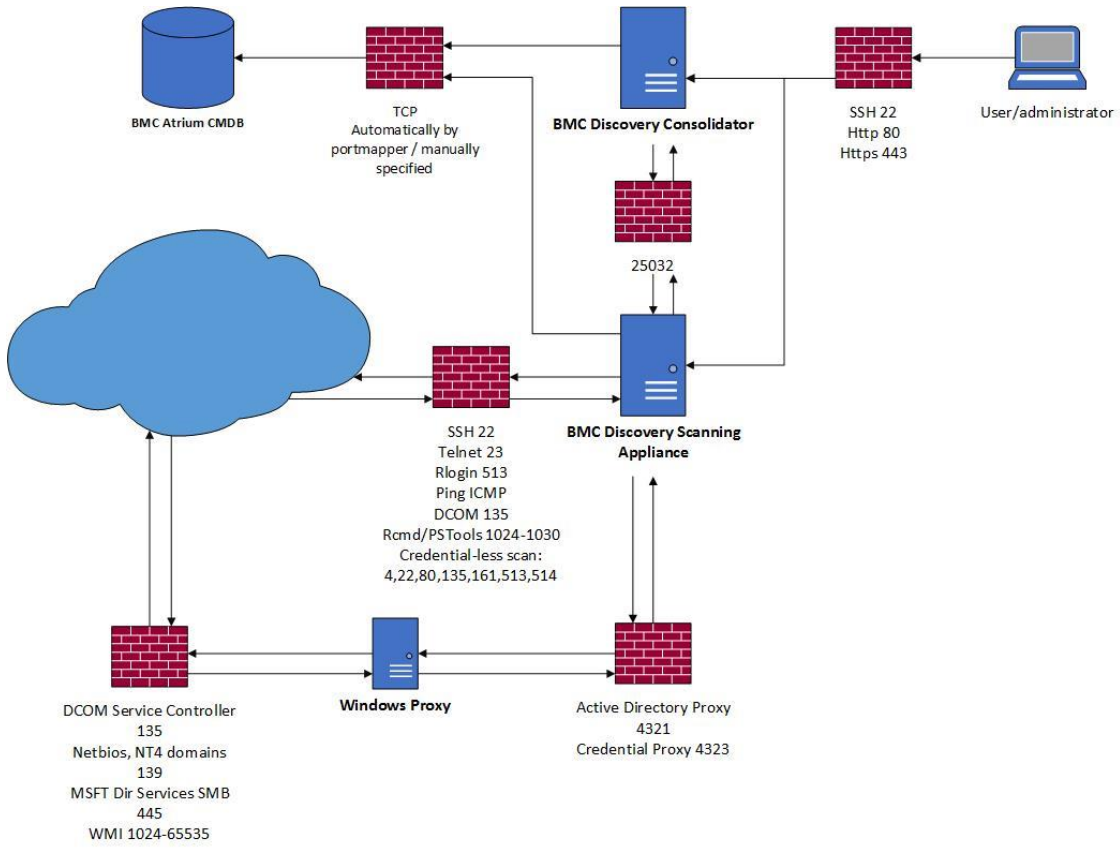
BMC Discoveryn käyttäjän tai ylläpitäjän koneelta Discovery-palvelimelle tulee olla sallittuna seuraavat verkkoportit:

- TCP: 22 – ssh, salattu konsoliyhteys käyttöjärjestelmän hallintaa varten
- TCP: 80 – http, salaamaton selainyhteys Discoveryn käyttöliittymää varten
- TCP: 443 – https, salattu selainyhteys Discoveryn käyttöliittymää varten

Suositeltavaa tietoturvan kannalta on asettaa Discoveryn asetuksista ohjaus salaamattomasta HTTP-yhteydestä salattuun HTTPS-yhteyteen.

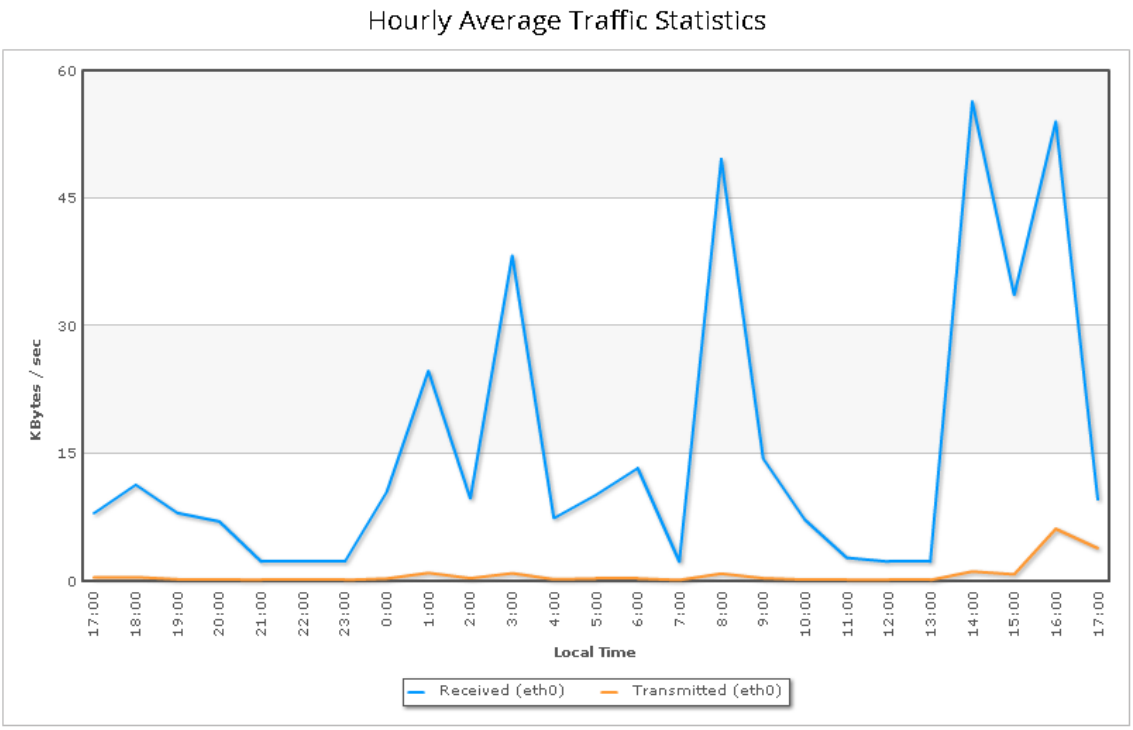
Skannerin ja konsolidaattorin välinen liikenne tapahtuu oletuksena portissa 25032 [17].

Skanneri ja Active Directory Proxy keskustelevat portin 4321 kautta ja Credential Proxy portin 4323 kautta [15]. Kuvassa 6 ovat hahmoteltuna kaikki tarvittavat oletuksena olevat verkkoportit Discovery sovelluksen käyttämiseen ja sillä toimimiseen. [17.]

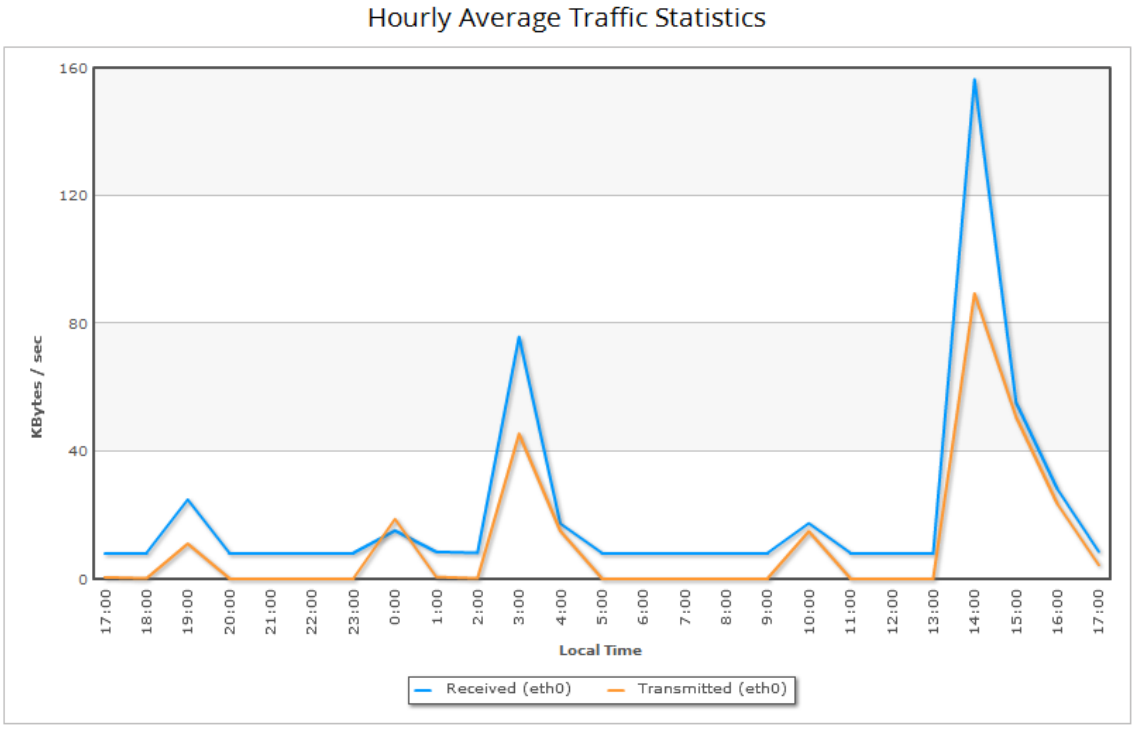


Kuva 6. Oletuksena tarvittavat verkkoportit Discovery sovelluksen käyttämiseen ja kohdeverkon skannaamiseen [17].

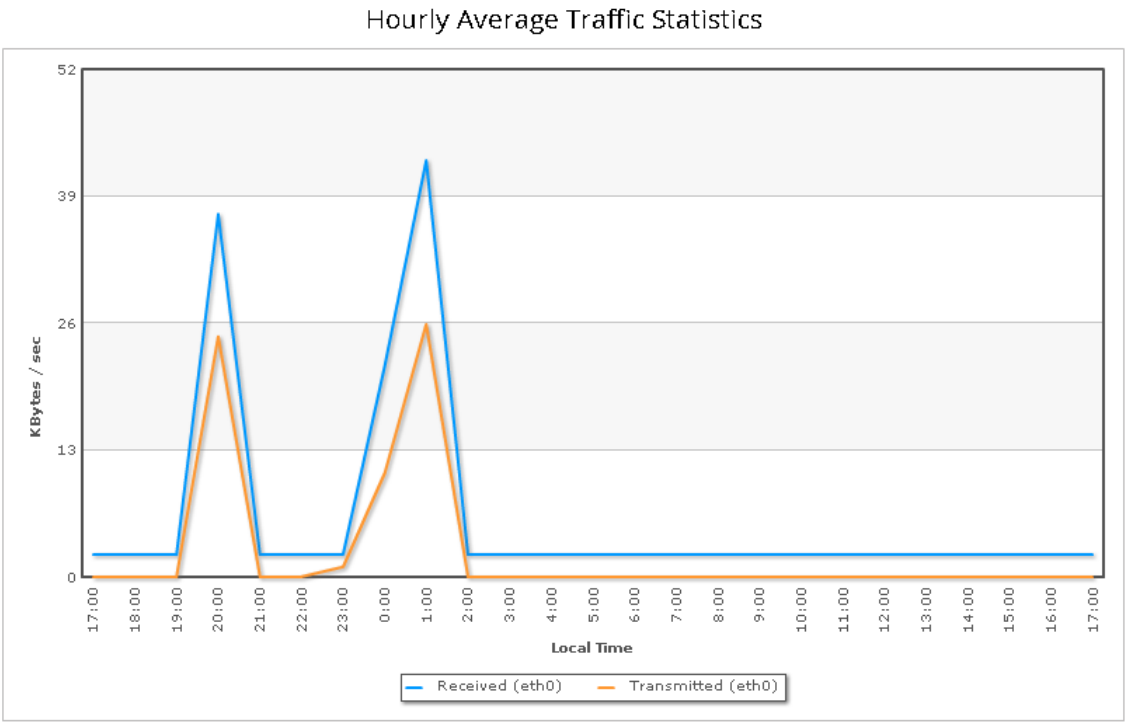
BMC:n mukaan Discoveryllä tyypillinen verkonkuormitus piikkinä on noin 3 megabittiä sekunnissa, mutta verkonkuormitus skannerilla tai konsolidaattorilla vaihtelee skannattavan ympäristön mukaan. Suurin osa verkkoliikenteestä muodostuu kohdelaitteilta saapuvasta datasta skannerille. [18.] Kuvissa 8–11 näkyy todellisia lähetetyn ja vastaanotetun verkkoliikenteen määriä Discovery kokonaisuudesta, jossa on kolme skanneria ja konsolidaattori. Tiedot on otettu jokaisen Discovery-palvelimen suoritustehoraporteista saman tunnin sisällä, eikä niitä voida pitää tarkkoina mittaustuloksina. Ne antavat kuitenkin osviittaa verkkoliikenteestä tavanomaisessa tilanteessa, jossa kartoitettavat ympäristöt ovat pääosin entuudestaan tunnettuja eivätkä ajot tuota kovin paljoa uutta tietoa. Tämän takia skannausten ja konsolidoinnin tuottama verkon kuormitus on hyvinkin maltillinen. Tilanne olisi toinen, jos mitattaisiin tilannetta, jossa skannattaisiin ennalta tuntematonta ympäristöä.



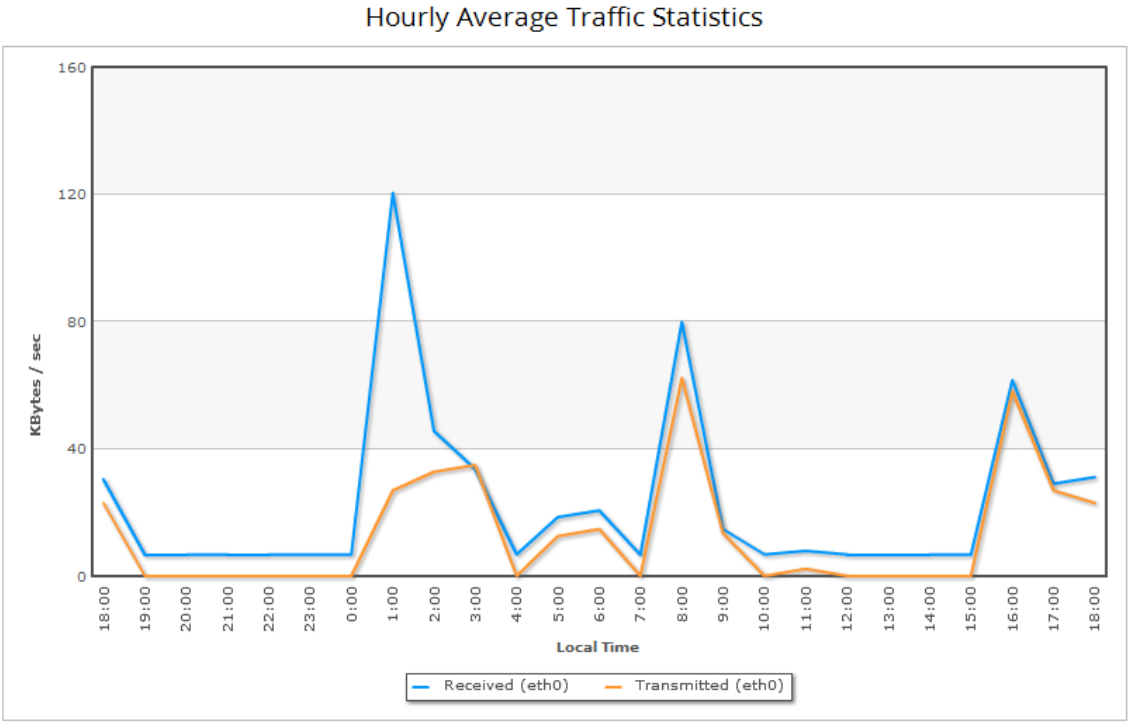
Kuva 7. Tilastoa konsolidaattorin kolmelta skannerilta vastaanottamasta ja sen itse lähettämästä liikenteestä 24 tunnin ajalta.



Kuva 8. Tilastoa ensimmäisen skannerin vastaanottamasta ja sen muun muassa konsolidaattorille lähettämästä liikenteestä 24 tunnin ajalta.



Kuva 9. Tilastoa toisen skannerin vastaanottamasta ja sen muun muassa konsolidaattorille lähettämästä liikenteestä 24 tunnin ajalta.



Kuva 10. Tilastoa kolmannen skannerin vastaanottamasta ja sen muun muassa konsolidaattorille lähettämästä liikenteestä 24 tunnin ajalta.

4.3 Havaintoprosessi

Discovery sisältää kaksi pääasiallista skannaustapaa. Alustavan ensiskannauksen (engl. Sweep Scan) tarkoituksena on käydä nopeasti läpi annettu IP-osoite tai -osoitteet, aliverkko tai osoiteavaruus ja selvittää pintapuolisesti, onko kussakin osoitteessa jokin laite, sekä yrittää selvittää sen tyyppi. Näin saadaan alustavaa raakadataa (engl. DDD, Directly Discovered Data) ympäristöstä ja sen pohjalta Discovery pystyy nopeammin suorittamaan täyden skannauksen. Eniten hyötyä ensiskannauksella saadaan, kun kartoitetaan ennalta tuntematonta aliverkkoa tai osoiteavaruutta. Näin voidaan alustavasti kartoittaa tutkittavaa ympäristöä. Discovery saa näin tietoonsa, mitkä osoitteet ovat mahdollisesti tyhjiä ja voidaan mahdollisesti ohittaa. Lisäksi saadaan tietoa, millaisia laitteita ja käyttöjärjestelmiä ympäristö sisältää ja miten niihin kirjaudutaan.

Täydellinen skannaus (engl. Full Scan) aloittaa samoilla alustavan skannauksen toiminnoilla ottaen huomioon mahdollisesti aiemmin tallennetut tiedot ja jatkaa päättelykoneen ja määriteltyjen kaavojen avulla kohdejärjestelmän analysointia. Pohjatietojen perusteella se kerää tarkemmat järjestelmätiedot ja sillä suorituksessa olevat prosessit, asennetut paketit ja ohjelmat sekä niiden mahdolliset yhteydet muihin sovelluksiin, laitteisiin tai järjestelmiin.

Havaintoprosessi lähtee liikkeelle siitä, että Discoveryyn ajastetaan joko kerran ajettava tilannekuvaus (engl. Snapshot) tai ajastettu ajo, jolloin syötetään yksi tai useampia IP-osoiteita tai kokonaisia aliverkkoja. Jokaisen IP-osoitteen kohdalla Discovery suorittaa järjestyksessä alla mainitut ja kuvassa 11 esitetyt toimenpiteet, riippuen siitä, millaisen vastauksen kukin tuottaa. Esimerkiksi kun jokin alla mainituista toimista saa ”positiivisen” vastauksen, siirtyy Discovery tarkempaan skannaukseen, ellei osoite ole merkitty kannassa esteellisenä. [19.]

1. Tarkistaa, löytyykö osoite sulkulistalta.

2. Tarkistaa osoitteeseen liittyviä ennestään tallennettuja tietoja.

3. Tarkistaa aikaisemmat onnistuneet kirjautumistiedot, ja jos sellaisia löytyy, käytetään samaa kirjautumismetodia ja suoritetaan hakukomentoja kohdejärjestelmässä.

4. Suorittaa porttiskannauksen tunnettujen kirjautumiseen käytettävien porttien osalta. Jos tämä ei tuota vastausta, ohitetaan osoite. Tästä eteenpäin seuraavat toimenpiteet käydään läpi järjestyksessä, ja jos jokin on onnistunut, siirretään tiedot käyttöjärjestelmä-heuristiikalle.

5. Yrittää kirjautumista ensin SSH:lla (engl. Secure Shell), jos se epäonnistuu, kokeillaan Windows-kirjautumista käyttäen Windows Proxya. Jommankumman onnistuessa ajetaan kohdejärjestelmässä hakukomentoja.

6. Suorittaa SNMP get -komennon SysObjectId-tietojen saamiseksi. Ne sisältävät valmistajan identifikaatiotietoja järjestelmästä ja sen tyypistä. [20.]

7. Suorittaa SNMP get -komennon SysDesc OID -tiedon saamiseksi, jonka pitäisi sisältää sanallinen kuvaus järjestelmästä.

8. Tarkistaa aikaisemmista varmistustiedoista (engl. fallback information) aiemmat onnistuneet SNMP-tiedot kohteelle.

9. Yrittää avata Telnet-yhteyden mahdollisen bannerin lukemiseksi.

10. Yrittää yhdistää z/OS-järjestelmän porttiin.

11. Yrittää HTTP HEAD -metodilla saada otsikkotietoja.

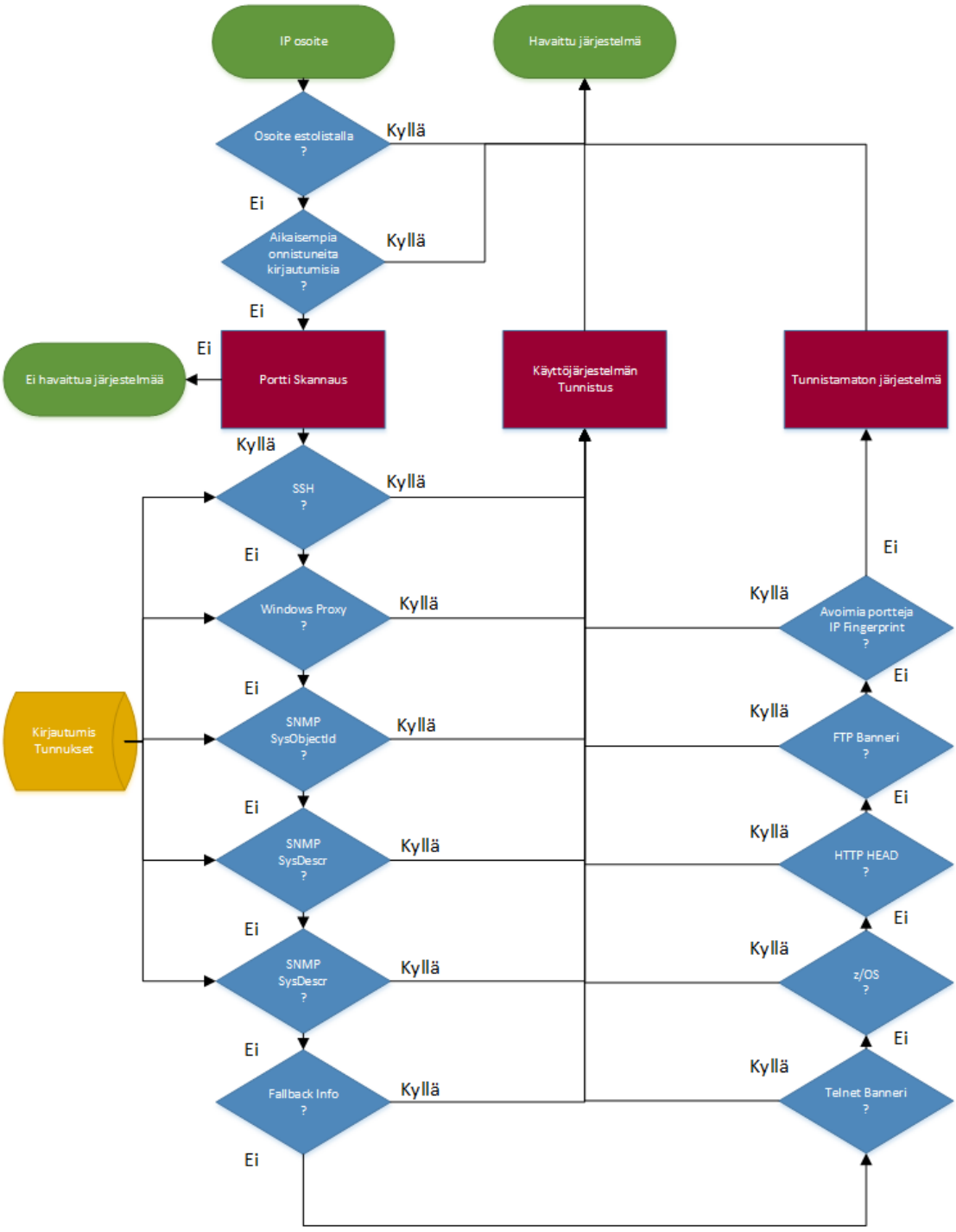
12. yrittää avata FTP-yhteyden mahdollisen bannerin lukemiseksi.

13. Vertaa avoimia portteja (engl. IP fingerprint) määrittääkseen käyttöjärjestelmän tyypin. [19.]

Discovery onnistuu useimmiten selvittämään kohteen käyttöjärjestelmän ja version ilman kaikkien edellä mainittujen toimenpiteiden läpi käymistä. Tarpeelliset tiedot kerättyään Discovery siirtyy seuraavaan osoitteeseen tai jää odottamaan seuraavaa ajastettua skannausta. [19.]

Laitteet, joihin Discovery ei onnistu kirjautumaan, pyritään tunnistamaan käänteisnimipalveluhaulla (engl. Reverse DNS lookup), telnetillä, SNMP-kyselyillä ja IP-sormenjälkitunnistuksella – jos sellainen on sallittu – saatujen tietojen perusteella. Dis-

covery luo tietokantaansa merkinnän isäntäkoneesta (engl. Host) vain, kun siitä on onnistuneesti kerätty tarpeeksi tietoa, jotta Discovery voi todeta sen olevan uniikki järjestelmä. Yleensä tämä tarkoittaa sitä, että kohteeseen on onnistuneesti kirjauduttu. Jokaisesta skannatusta osoitteesta jää kantaan merkintä riippumatta siitä, tuottiko osoite mitään vastausta tai virheilmoituksen. [19.]



Kuva 11. Discoveryn käyttämä heuristiikka kohdelaitteen tunnistamiseksi [19].

Discoveryn päättelykone ja sen käyttämät kaavat astuvat kuvaan havaintoprosessissa käytännössä heti, kun kohdejärjestelmän käyttöjärjestelmä on tunnistettu. Kun Discovery tietää, mikä käyttöjärjestelmä osoitteessa on, se osaa sen pohjalta käyttää oikeita komentoja selvittääkseen kohteen perustietoja, kuten nimen, verkkoadapterit ja niiden mahdolliset osoitteet, sen spesifikaatiot, kuten muistin tai prosessorien määrän, mitä prosesseja on käynnissä ja mitä paketteja tai ohjelmia on asennettuna. Näiden tietojen pohjalta se siirtyy suorittamaan uusia kaavoja ja niiden pohjalta jatkokyselyitä laitteelle ja koostaa näistä tiedoista kokonaisuuden, joka on yhteydessä skannattuun osoitteeseen.

Windows

Koska Discovery-järjestelmä on rakennettu Unix-pohjaisen käyttöjärjestelmän päälle ja koska BMC on valinnut WMI-protokollan Windows-laitteiden kanssa kommunikointiin, on Windows-ympäristöissä käytettävä välityspalvelinta. Tämä tarkoittaa Windows-palvelimelle asennettavaa Discovery Proxy Manager -sovellusta, joka suorittaa Discoveryn antamia WMI-komentoja Windows-laitteilla.

BMC Discovery Proxy Manager -sovelluksella hallitaan AD- ja Credential Proxy-palveluita, mutta kaikki skannaukseen liittyvät muutokset tehdään vain skannerilta. Yhdelle Windows-palvelimelle voi olla asennettuna yksi Discovery Proxy Manager, ja sillä voidaan hallita useita AD Proxy- tai Credential Proxy -instansseja. Mutta skannausten suorituskyky saattaa kärsiä, jos useaa välityspalvelua käytetään tiheästi ja samaan aikaan. [21.]

Active Directory Proxya suoritetaan AD-tunnuksella, ja samaa tunnusta käytetään kohdelaitteeseen yhdistettäessä saman toimialueen (engl. domain) sisällä. AD-tunnuksia ei ole tallennettu skannerin käyttäjätunnustietokantaan, vaan ne ovat vain välityspalvelimella. Yksi AD Proxy sisältää yhden AD-tunnuksen. [22.] Periaatteessa jokainen toimialue vaatii oman AD Proxynsä ja oman AD-tunnuksensa. Poikkeuksena on mahdollista käyttää yhtä tunnusta, kun kahden tai useamman toimialueen välillä on luottosuhde, jolloin tällä yhdellä tunnuksella voidaan autentikoitua näiden toimialueiden sisällä.

Credential proxya suoritetaan paikallisilla pääkäyttäjän tunnuksilla (engl. local administrator user). Nämä tunnukset on tallennettu skannerin käyttäjätunnustietokantaan, ja ne haetaan sieltä tarvittaessa. [22.] Paikallisia tunnuksia ja Credential Proxyä tarvitaan

toimialueeseen kuulumattomiin Windows-laitteisiin kirjauduttaessa. Paikallistunnuksia voidaan myös käyttää toimialueeseen kuuluviin koneisiin.

AD-tunnus tai lokaali tunnus tulisi konfiguroida niin, ettei se lukkiudu useamman kirjautumisyrityksen takia. Jos jokin kohdejärjestelmä on konfiguroitu väärin skannausta varten, lukkiutuvat AD-tunnukset muutaman yhteysyrityksen jälkeen, jolloin skannaus epäonnistuu kaikilla laitteilla joihin samaa tunnusta käytetään kirjautumiseen. Kumpaa tahansa tunnusta käytettäessä sen tulisi kuulua ryhmään, joka oikeuttaa ylläpitäjän oikeuksiin kohdejärjestelmässä, koska monet suoritettavat komennot vaativat niitä. Lisäksi on huomioitavaa, että verkkoalueen ohjainpalvelinta (engl. Domain controller) skannatessa tulee tunnuksella olla käytännössä Domain Admin -oikeudet. Lisäksi lokaalia tunnusta käytettäessä käyttäjätilin valvonta (engl. UAC, User account control) tulee olla pois päältä. [23.]

Windows-laitteissa tiedonhaku toteutetaan järjestyksessä seuraavilla protokollilla:

- Ensisijaisesti käytetään WMI-kyselyitä sekä rekisteriin kohdistuvia kyselyitä.
- RemQuery-ohjelmalla suoritettavia komentotulkkikomentoja käytetään, jos WMI kyselyt epäonnistuvat. Käytettäessä se kopioidaan ja asennetaan kohteen admin$ kansioon ja käynnistetään palveluna. Skannauksen loppuessa palvelu lopetetaan ja sen asennus poistetaan, mutta suoritettava tiedosto jää kohdekoneelle seuraavaa skannausta varten.
- Komentotulkkiskriptejä (engl. shell scripts) käytetään vain, kun käytössä on SSH- tai Telnet-tietoliikenneyhteys.
- SNMP-protokollan käyttö on viimeinen vaihtoehto, ja se toimii käytännössä kaikilla laitteilla, joissa se on sallittuna. [23.]

Vaikka WMI-kyselyt ovat pääasiallinen tapa Windows-käyttöjärjestelmien kartoittamiseen, käytetään RemQueryä tiettyihin toimintoihin, kuten sovellusten ja ohjelmien syvempään skannaamiseen, koska WMI ei niihin kykene. Ilman RemQuerya ei voida esimerkiksi päätellä verkkoyhteystietoja kohteelle tai kommunikointia kohteen ja muiden laitteiden välillä, eikä sovellusmalleja voida luoda ilman verkkoyhteyksiä. [24.]

Windows-laitteiden kartoittamiseen vaaditut verkkoportit ja -protokollat ovat:

- 135 – DCE/RPC, DCOM Service Control
- 1024–1030 – Rajoitettu DCOM. Yhtä porttia käytetään yhteysneuvottelun jälkeen. (Käytetään vain jos halutaan rajoittaa avointen DCOM-porttien määrää.)
- 1024–65535 – Rajoittamaton DCOM. Yhtä porttia käytetään yhteysneuvottelun jälkeen (oletus).
- 139 – Netbios Session Service
- 445 – Microsoft Directory Services SMB. [17.]

Lisäksi Windows-koneille voidaan ladata Discoverysta erikseen asennettava itsenäinen (engl. Standalone) skannaussovellus, joka asennetaan kohdejärjestelmään, ja sillä suoritetaan laitetietojen keräys. Tiedot tallentuvat tiedostoon, jotka sitten kopioidaan manuaalisesti kohdejärjestelmästä ja siirretään Discoveryn tietokantaan. Työkalun tarkoituksena on kerätä tietoja laitteesta, johon ei voida yhdistää etäyhteydellä.

Unix

Unix-pohjaisten laitteiden skannaamiseen riittää yleensä tavallinen käyttäjätunnus lukuoikeuksilla (engl. Read rights), jotta saadaan kerättyä oleellinen tieto laitemerkinnän luomiseksi Discoveryn tietokantaan. Jotkin käyttöjärjestelmät vaativat toisia enemmän oikeuksia käyttäjältä, jotta voidaan suorittaa tiettyjä komentoja, esimerkiksi saadakseen joitakin oleellisia laitetietoja, kuten laitteen sarjanumeron ja fyysisen muistin määrän. Tunnus voi olla joko tavanomaisesti salasanalla suojattu tai salasanan sijaan käytetään SSH-avainta, joka turvallisempi ratkaisu. SSH-avain voidaan luoda esimerkiksi skannerin käyttöjärjestelmässä käyttäen komentotulkkia. Avaimia saadaan kaksi, ja niiden luomiseen suositellaan käytettävän vahvaa salasanaa. Salainen avain tallennetaan web-käyttöliittymän kautta skannerin salasanakantaan, ja julkinen avain asetetaan kohdejärjestelmään skannaukseen käytettävälle tunnukselle tunnistautumisavaimeksi. Skannerin tunnuksien ylläpidon helpottamiseksi on suositeltavaa, että käytetään samaa SSH-avainparia esimerkiksi kaikille yhden asiakkaan Unix-laitteille, jolloin tunnuksia ei kerry suurta määrää ja niitä on helpompi hallita. Tämä kuitenkin riippuu organisaation tietoturvakäytänteistä.

Unix-laitteiden skannaamista varten Discovery yhdistää ja kirjautuu laitteisiin käyttäen ensisijaisesti SSH-protokollaa, ja sen epäonnistuessa yritetään telnet- tai rlogin-

protokollia. Jos mikään mainituista ei onnistu, Discovery kokeilee viimeiseksi SNMP-protkollaa. [17.]

Unix-pohjaisten järjestelmien skannaamiseen tarvitaan jokin alla mainituista verkkoporteista ja protokollista. Jos tiedetään, että laitteilla on käytössä vain SSH-protokolla yhdistämistä varten, ei muita portteja tarvitse avata.

- 22 – SSH
- 23 – Telnet
- 513 – Rlogin. [17.]

VMware

VMware ESX- ja ESXi-palvelimet voidaan havaita ja skannata joko suoraan yksi kerrallaan palvelimen omalla IP-osoitteella tai epäsuorasti havaitsemalla ne vCenter-hallintapalvelimen skannauksen ohessa. Epäsuoran skannauksen etuina on, ettei jokaisen ESX-palvelimen IP-osoitetta tarvitse olla tiedossa valmiina. Riittää, että tiedossa on vCenter-hallintapalvelimen osoite ja lukuoikeuksilla varustettu vCenter-käyttäjätunnus.

Discoveryn havaitessa normaalin skannauksen yhteydessä palvelimella vCenter-sovelluksen tai vCenter-valmisjärjestelmän, se yhdistää tähän palvelimeen käyttäen porttia 443 (HTTPS) ja vSphere-sovellusrajapintaa ja kirjautuu vCenter-käyttäjätunnuksella vCenter-palveluun. Vcenteristä kerätään lista sen hallinnoimista ESX-isäntäkoneista. Lisäksi se listaa ja lisää niiden IP-osoitteet alkuperäisen skannaustoimeksiannon sisältämiin osoitteisiin merkinnällä ”epäsuorasti skannattu IP-osoite” (engl. implicitly scanned IP address). ESX-palvelinten skannaus tapahtuu tässä yhteydessä vCenterin välityksellä keskitetysti. [25.]

Jos ESX-palvelinta ei ole ennestään skannattu vCenterin välityksellä ja havaitaan portin 902 vastaavan vSpere API -kyselyyn, yhdistetään kohteeseen HTTPS-protokollalla ja kun validit vSphere-tunnujset löytyvät, kirjaudutaan niillä ja suoritetaan tarvittavat kyselyt tietojen keräämiseksi. [25.]

Discovery käyttää vSphere API -versiota 2.5, joka tukee seuraavia tai uudempia versioita:

- ESX/ESXi 3.5
- vCenter Server 4.0
- VirtualCenter 2.5 [25].

Viimeisenä vaihtoehtona havaita ESX-palvelin mainittujen metodien epäonnistuessa on suorittaa skannaus SSH-protokollalla portissa 22 tai muussa kyseistä protokollaa varten konfiguroidussa portissa. SSH-protokollaa käytettäessä kirjautumiseen tulee tunnuksella olla pääkäyttäjän oikeudet. Ilman niitä käyttäjä ei voi sulkea yhteyssessioita oikein, jolloin ne jäävät roikkumaan kohdepalvelimelle passiivisina ja voivat aiheuttaa ongelmia sen toiminnassa. Lisäksi SSH-protokollaa käyttettäessä Discovery ei voi kerätä tietoja verkkoadaptereista ”netstat”-komentoa vastaavan komennon puuttuessa. [25.]

SNMP

SNMP-protokollaa (engl. Simple Network Management Protocol) käytetään kohdelaitteiden skannaamiseen viimeisenä mahdollisuutena, kun kaikki muut järjestelmään kirjautumismetodit ovat epäonnistuneet. Tämä vaatii tietenkin, että kohdejärjestelmään on SNMP-protokollan verkkoportti 161 (UDP) avoinna. Jos kohdejärjestelmä on aiemmin skannattu vain SNMP-protokollaa käyttäen, Discovery tarkistaa aina, löytyykö jotain muuta voimassa olevaa kirjautumistunnusta kyseiselle järjestelmälle ja jos sellainen löytyy, käytetään sitä ensisijaisesti jatkossa. SNMP-protkollaa käyttäen kohteesta saadaan vain yksinkertaisimmat tiedot, kuten nimi, tietoja verkkoadaptereista ja suoritettavista prosesseista, sekä asennetuista paketeista. Sillä ei voida suorittaa tiedostojen skannausta tai käyttöjärjestelmäkohtaisia käskyjä. [26.]

Skannerille tarvitse määritellä SNMP-parametit, jos kohdejärjestelmissä on konfiguroituna jonkin muu kuin julkinen yhteisöavain (engl. public read community). Eri kohdejärjestelmille voidaan konfiguroida omat SNMP-parametrit. SNMP-versioita 1 ja 2 käytettäessä tarvitaan voimassa oleva yhteisölause/-avain (engl. Community String), jolla on lukuoikeudet kohdejärjestelmissä. SNMPv3-protokollaa varten tulee skannerille ja kohdejärjestelmille konfiguroida käyttäjätili (engl. Security Name), salauksen taso (engl. Security Level), autentikointiprotokolla (engl. Authentication Protocol), autentikointiavain (engl. Authentication Key), salausprotkolla (engl. Privacy Protocol) ja [27.]

salauksen avain (engl. private key). Joissakin tapauksissa kohdejärjestelmissä on lisäksi konfiguroitu asiayhteystieto (engl. Context). [27.]

4.4 Tiedon siirto konfiguraatiotietokantaan

BMC Discovery ja CMDB-synkronointi (engl. CMDB Synchronization) tukee valmisratkaisuna (engl. Out of the box solution) havaitun tiedon synkronointia omaan tuotteeseensa Atrium CMDB-konfiguraatiotietokantaan. Lisäksi Discovery tukee tiedon vientiä suoraan relaatiotietokantaan (engl. Relational database, RDB) tai järjestelmiin, jotka tukevat CSV-tiedostoformaattia (Comma-separated-values file format). [28.]

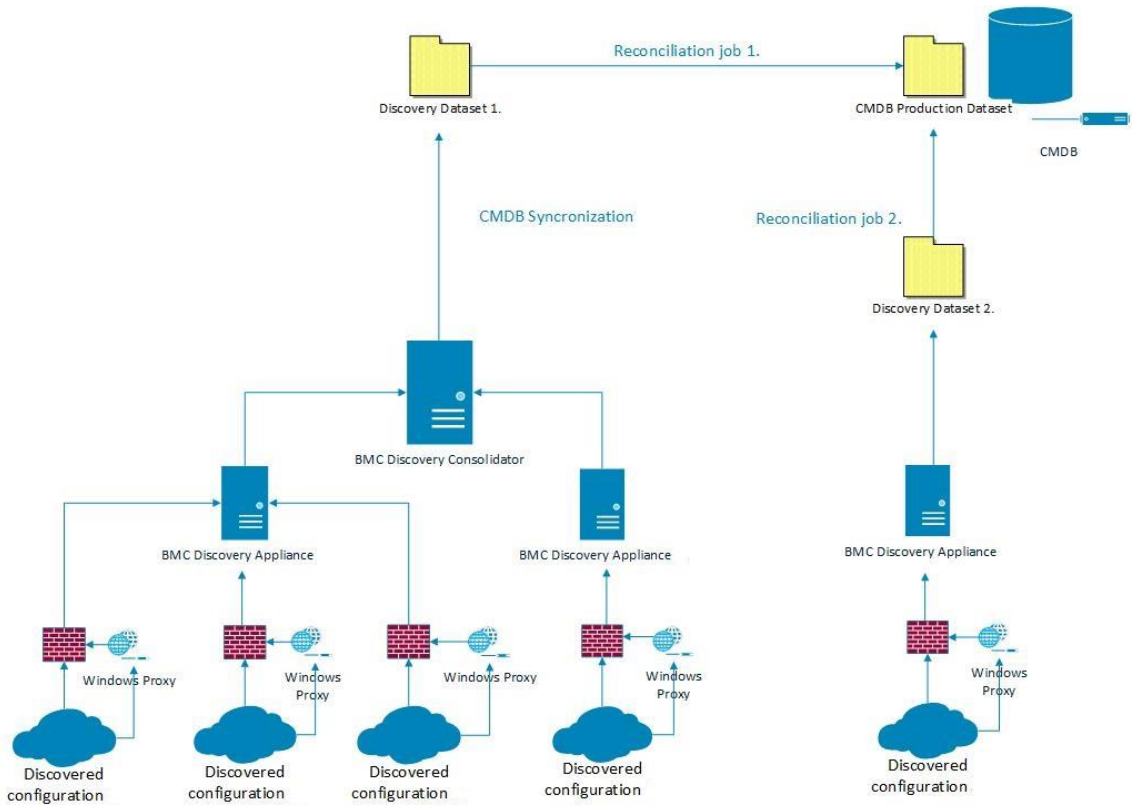
Tiedon vienti suoraan relaatiotietokantaan tai CSV-tiedostoon vaatii kartoitustiedoston (engl. Mapping file) luomisen, sekä vientiadapterin (engl. Export adapter) konfigurointia. Kartoitustiedosto sisältää hakuehdot, mitä tietoa haetaan Discovery-tietokannasta, ja mallin (engl. Schema), mihin muotoon tämä tieto muokataan, jotta vastaanottava järjestelmä osaa hyödyntää sitä. Vientiadapteri – CSV-adapteri tai RDB-adapteri – sisältää parametrit yhteyden muodostamiseksi kohdejärjestelmään. Vientiadaptereita ja kartoitusmalleja voidaan luoda useampia eri kohteita ja käyttötarkoituksia varten. [29.]

Kartoitetun tiedon synkronointi BMC Atrium CMDB -tietokantaan voidaan tehdä suoraan Discovery-sovelluslaitteelta (engl. Discovery Scanning Appliance) tai voidaan käyttää Discovery-konsolidaattoria (engl. Discovery Consolidator appliance), joka keskitetysti synkronoi kerätyn tiedon. Synkronointi tapahtuu kuitenkin molemmissa tapauksissa täsmalleen samalla tavalla.

Koska BMC Discoveryn tietomalli on erilainen kuin Atrium CMDB:ssä, tarvitaan sitä varten mekanismi sovittamaan data Atrium CMDB:n vaatimaan malliin. Discoveryn CMDB-synkronointi vastaa tästä. Tietomallin sovittaminen CDM-tietomalliin tehdään synkronointikaavojen avulla. Samalla tavalla kuin skannauksessa käytettäviä kaavoja voidaan näitäkin luoda uusia tai muokata olemassa olevia TPL-kaavakielellä. Tämä voi esimerkiksi olla tarpeen, mikäli jompaakumpaa tietomallia on personoitu. [30.]

Jokaisella erillisellä skannerilla tai konsolidaattorilla kuten millä tahansa muulla tietoa tuottavalla lähteellä, joka vie sitä Atrium CMDB:n tietokantaan, tulee olla määriteltynä oma erillinen tietokokonaisuutensa (engl. Dataset) Atrium-järjestelmässä. Kuvassa 12 on havainnollistettu tiedon vientiä kahdesta erillisestä skannattavasta ympäristöstä.

Discovery ylläpitää jokaiselle konfiguroidulle erilliselle Atrium CMDB-yhteydelle omaa hallitsevaa tietokokonaisuuttaan, joka on varjokopio Atrium CMDB-järjestelmässä sijaitsevasta tietokokonaisuudesta. Tähän Discovery-järjestelmässä sijaitsevaan tietokokonaisuuteen se synkronoi skannatun tiedon sitä mukaa, kuin sitä skannauksista saadaan käsiteltyä. Tiedot varjokopiosta synkronoidaan taas Atrium CMDB:ssä sijaitsevaan tietokokonaisuuteen. Jotta skannattu tieto lopulta näkyy käyttäjälle Atrium CMDB -järjestelmässä, suoritetaan Atrium CMDB:ssä täsmäytysajo (engl. Reconciliation Run) Discoveryn tietokokonaisuuden ja CMDB:n tietokokonaisuuden välillä. [30.]



Kuva 12. Discovery- ja CMDB-synkronointikokonaisuus.

4.5 Tietoturva

Koska Discoverylla ja senkaltaisilla havaintotyökaluilla on niin kattava näkyvyys tutkittavaan IT-ympäristöön ja ne tuottavat tarkkaa ja arkaluontoistakin tietoa siitä, on BMC:llä suuri vastuu tietoturvan takaamiseksi, ettei samaa tietoa tai työkaluja käytetä väärin. Käytännössä Discoveryn suorittamiin skannauksiin tarvittavilla eri tunnuksilla on pääsy ja oikeudet lähes mihin tahansa tutkittavassa ympäristössä, mikä luo suuren riskin. Tämän takia BMC Discoveryssa on otettu huomioon useita seikkoja tietoturvan näkökulmasta. Myös organisaation omien tietoturvakäytäntöjen tulee olla ajantasaiset ja oikein toteutettu, jotta tietoturvariskit saadaan minimoitua.

Tietoturvasyistä BMC on päätynyt luomaan Discoverysta ennemmin valmisjärjestelmän (engl. Appliance) kuin ohjelman, jolloin se voi itse huolehtia Discoveryn vahventamisesta käyttöjärjestelmätasolta lähtien. Näin Discoverysta on voitu jättää pois kaikki ylimääräinen mikä ei ole välttämätöntä sen toiminnan kannalta. Näin karsitaan tietoturvariskejä joita käytännössä kaikki järjestelmässä suoritettavat ohjelmat ovat. [31.] Myös se, että Discovery on agentiton järjestelmä eli kohdejärjestelmiin ei tarvitse asentaa erillisiä ohjelmia, vähentää tietoturvariskejä.

Discovery on vahvennettu sitä rakennettaessa muun muassa seuraavasti:

- Käyttöjärjestelmän asennuksessa on käytetty vain välttämättömiä paketteja.
- Vain välttämättömät palvelut ovat käytössä.
- Palomuuri on konfiguroitu vain Discoveryn tarpeisiin.
- Ylimääräiset käyttäjätunnukset on poistettu.
- Vain SSH-protkolla on sallittu yhdistämiseen. Telnet- ja FTP-protokollat on estetty.
- Etäyhteydellä ei voi kirjautua pääkäyttäjänä (engl. root).
- Käyttöjärjestelmän ytimeen (kernel) on määritelty erityisiä rajoituksia, kuten ICMP echo broadcast.
- Lokitukselle, cronin käyttöön ja konfigurointiin vaaditaan erityisoikeuksia.
- Massamuistin käyttöönotto on sallittu vain tietyille operaatioille ja osioille.
- Salasanoille on määritelty kriteerit [32].

- Tietyiltä sovelluksilta on poistettu SETUID-oikeudet, mikä estää suoritettavan sovelluksen, tiedoston tai koodin suorittamisen sen omistajan oikeuksilla. [32.]

Lisäksi Discoveryssa on avoimen lähdekoodin Tripwire-ohjelmaan perustuva monitorointijärjestelmä (baseline monitoring system), joka voidaan konfiguroida reagoimaan automaattisesti luvattomiin muutoksiin Discoveryssa [32].

Discovery-järjestelmän käyttäjähallintapalvelu vastaa ISO 27002-standardin mukaisia ohjeistuksia:

- Käyttäjänhallinta on olemassa.
- Salasanoille on käytänteet määrittämään niiden vahvuuden, kierrätettävyyden ja elämänkaaren.
- Salasanat on suolattu ja tallennettu 256-bittisenä SHA-tiivisteenä tiedostoon.
- Käyttäjäryhmien oikeudet on säikeistetty eri tasoille.
- Käyttäjätilien käyttö estetään autentikoinnin epäonnistuessa.
- Käyttäjätilit lukkiutuvat automaattisesti.
- Sessiolla on automaattinen aikakatkaisu. [32.]

Lisäksi käyttäjien hallinta voidaan integroida organisaation LDAP-ratkaisuun, kuten esimerkiksi Microsoftin Active Directoryyn.

Salasanat ja käyttäjätunnukset, joita käytetään kohdelaitteiden ja järjestelmien skannaamiseen, CMDB-synkronointiin sekä tiedon vientiin on tallennettu salasanaholviin (engl. Credential Vault), joka on salattu 256-bittisellä AES:lla CBC-moodissa. Salaukseen on käytetty rakennusvaiheessa oletus salalausetta (engl. passphrase), joka on 256-bittinen avain, ja se on generoitu 64 satunnaismerkistä 512 bitillä. Avain on siis kaikissa Discovery-asennuspaketeissa, joten on suositeltavaa vaihtaa se uuteen vähintään yhtä vahvaan avaimeen. Jos salasana holvi on lukittu eikä salausavainta ole käytössä, ei sitä voida enää avata. [33.]

Uusimmassa Discoveryn versiossa 11.1. on myös mahdollista integroida kolmannen osapuolen CyberArk Enterprise Password Vault, joka mahdollistaa organisaation salasanahallinnan keskittämisen yhteen järjestelmään sen sijaan, että Discoveryn tunnuksia hallitaan erikseen. [34.]

Tietenkin tämä edellyttää, että organisaatiolla on käytössä CyberArk. CyberArk-integraatiolla voidaan vähentää ylimääräistä työtä salasanojen hallinnassa, ja se mahdollistaa helpomman salasanahallinta käytänteiden toteuttamisen. [34.]

Kohdejärjestelmistä havaittujen prosessien tiedoissa on aina mukana tieto siitä, millä komennolla prosessi on suoritettu, ja joissakin tapauksissa se saattaa sisältää käyttäjätunnuksen, salasanan tai muuta arkaluontoista dataa selkokielisenä. Lisäksi on mahdollista lukea havaittujen tiedostojen sisältöä selkokielisenä, ja ne voivat myös sisältää arkaluontoista tietoa. Sen estämiseksi Discoveryssä on mahdollista ottaa käyttöön arkaluonteisen tiedon suodattimia, joiden avulla naamioidaan prosessien tai tiedostojen sisältämästä tiedosta MD5 tiivisteitä. Näitä tiivisteitä verrataan aikaisempiin versioihin, ja näin määritetään, onko tieto muuttunut, lukematta sitä selkokielisenä. [35.]

Discovery sisältää oman palomuurin, ja sillä on sisään tulevan liikenteen osalta sallittu vain seuraavat TCP-portit, jotka ovat olennaisia käytön kannalta:

- 22 – Secure Shell Login (SSH) on sallittu Discoveryn käyttöjärjestelmän etäyhteyttä varten
- 80 – HTTP-protokolla on sallittu, jos https protokollaa ei ole konfiguroitu web-käyttöliittymää varten
- 443 – HTTPS-protokolla sallittu salatun yhteyden muodostamiseksi web-käyttöliittymään
- 25030-25032 – CORBA-protokolla TLS-salauksella on sallittu Discovery-klusterin solmujen väliseen liikenteeseen
- 25032 – CORBA-protokolla TLS-salauksella on sallitty skannerin ja konsolidaattorin väliseen liikenteeseen
- 4321 ja 4323 ovat oletusportit Windows-välityspalvelimen ja skannerin väliseen liikenteeseen. Poikkeuksena muihin, niiden välinen liikenne tapahtuu vain skannerin aloitteesta [36].

Järjestelmän palomuuria ja sallittuja portteja hallitaan web-käyttöliittymän kautta, eikä palomuurin asetuksiin tulisi koskea käyttöjärjestelmä-tasolta, koska muutokset katoavat, kun käyttöjärjestelmää päivitetään. [36.]

Windows-yhteyspalvelimen ja RemQueryn välinen liikenne on Windows-käyttöjärjestelmästä riippuen salattu ensisijaisesti AES:lla ja 256-bittisellä avaimella. Windows 2000 taas ei tue AES:a, joten DES salaus on käytössä silloin. Windows NT ei tue kumpaakaan, joten liikenne on salaamatonta. [37.]

BMC on amerikkalaisena yrityksenä ottanut huomioon Yhdysvaltojen puolustuslaitoksen vaatimat DISA Secure Technical Implementation Guidlines (STIG) -suositukset teknisille toteutuksille ja rakentanut Discoveryn yhteensopivaksi niiden kanssa. STIG-suositukset ovat julkista tietoja, ja jos organisaation tietoturva vaatimukset vastaavat näitä suosituksia, voidaan Discovery konfiguroida vastaamaan niitä Red Hat -käyttöjärjestelmän ja Apache-web-palvelun osalta. [38.]

Discovery voidaan myös asentaa FIPS (engl. Federal Information Processing Standard) -moodiin, jolla taataan Yhdysvaltain liittovaltion tiedonkäsittelystandardien – julkaisu 140-2 – mukaisten salausalgoritmien ja avainten käyttö, mutta tällöin muutamat Discoveryn toiminnot eivät ole tuettuina. Vaikka Discoverya ei olisikaan asennettu FIPS-moodiin, se käyttää silti saman standardin mukaisia käytäntöjä, kun se vain on mahdollista. [39.]

5 Yhteenveto

BMC Discovery on tehokas ja yleisesti kattava työkalu erikokoisten IT-infrastruktuurikokonaisuuksien kartoittamiseen. Yksinkertaisimmillaankin ja suhteellisen vähäisellä työmäärällä sillä saadaan luotettavasti ja nopeasti tuotua konfiguraatiotietokantaan uusia laitteita, kuten palvelimia ja tietoa niistä, ilman valtavaa käsin kirjaamisen vaivaa. Automaattisena havaintotyökaluna BMC Discovery säästää satoja työtunteja työaikaa sellaisessa organisaatiossa, jossa tarvitaan esimerkiksi vain ajantasaista laitetietokantaa, ja sen ylläpidossa on tuhansia fyysisiä ja virtuaalisia palvelimia, verkkolaitteita, varastointijärjestelmiä ja valmisjärjestelmiä. Jo yksinkertaisten laitetietojen ylläpitäminen manuaalisesti vaatii jatkuvasti muuttuvassa kokonaisuudessa paljon aikaa ja toimivia prosesseja järjestyksen ylläpitämiseksi. Discovery automatisoi osan tästä ylläpitotyöstä, ja se tekee sen käytännössäkin hyvin. Erityisesti se auttaa laitetietokannan ylläpidossa, kun organisaatiokulttuuriin ei ole vielä täysin sisäistetty konfiguraatiotietokannan tarpeellisuutta ja sen ylläpitämiseen ei ole täysin sitouduttu, jolloin sen paikkansapitävyys ja luottamus siihen äkkiä rapistuu. Se ei kuitenkaan pelasta huonosti suunniteltua konfiguraationhallintaa, tai vaikka se olisikin hyvin suunniteltu, ei edes huonosti toteutettua kokonaisuutta.

Jotta Discoverysta saataisiin käytännössä kaikki mahdollinen niin sanottu automatisoitu apu jo pelkkää laitetietokantaa ylläpidettäessä, tulee ottaa huomioon muutamia ennalta edistäviä asioita. Tällaisia ovat muun muassa skannaukseen tarvittavien tunnusten ja

oikeuksien jakelu ja tarvittavien palomuuriavauksien tekeminen heti laitetta käyttöön otettaessa, lisäksi tietenkin tarvittavien osoitteiden määrittäminen itse skannaavalle työkalulle. Nämä olivat muutamia yksinkertaisia asioita käytännössä, jotka ovat häirinneet Discoveryn mahdollistamaa osittaista automatisointia laitetietokannan ylläpitotehtävissä. Lääkkeenä on muun muassa käyttöönottoprosessien kehittäminen organisaatiossa. Discovery toimii jonkinlaisena laastarina välissä. Sen keräämiin tietoihin on voinut aina luottaa, koska se kerää ne aina suoraan laitteilta, niin kuin ne sinne on konfiguroitu. Jos on huomattu, että jonkin tieto on väärää tai puutteellista, on vika aina ollut jossain muualla kuin Discoveryssa: virhe on tapahtunut joko tutkittavan laitteen konfiguroinnissa tai sitten se on tapahtunut Atrium CMDB:n toiminnoissa, kuten tiedon täsmäytyksessä Discoveryltä Atrium CMDB -tietokantaan.

Tämän insinöörityön tavoitteiden mukaisesti kirjoitus- ja tiedonhakuprosessi ovat luoneet hyvää pohjaa ymmärtää konfiguraationhallinnan tärkeyttä ja sen prosesseja. Koska näistä ei ollut aikaisempaa tietopohjaa, on tietoon tutustuminen auttanut muun muassa jokapäiväisessä konfiguraationhallinnan ylläpitotyössä. Lisäksi noin vuoden mittaisen käytännön kokemuksen pohjalta kerätyt tiedot BMC Discoveryn käytöstä ja toiminnoista ja niiden yhdistäminen BMC:n viralliseen dokumentoinnista saatuun tietoon on auttanut konkreettisesti laajentamaan Discovery-skannauksien kattavuutta eri asiakasympäristöissä ja näin myös luonut korkeampaa tiedon luotettavuutta nykyisellään käytettävän Atrium CMDB -laitetietokannan sisällön osalta. Tältä pohjalta on hyvä jatkaa molempien työkalujen käytön hyödyntämistä ja kehittämistä pidemmälle seuraavaan vaiheeseen konfiguraationhallinnan kokonaisuudesta, jossa on laajemmin mallinnettu eri asiakkuuksien ympäristöjä. Näin mahdollisesti luodaan niihin lisää tuottavuutta. Lisäksi tätä työtä on mahdollista käyttää pienillä muutoksilla ja lisäyksillä koulutusdokumentaationa BMC Discoveryn käyttöön. Tarvittavia lisäyksiä olisivat muun muassa tarkemmat kuvaukset käytössä olevista Discovery-palvelimista ja niiden konfiguraatiosta, tarkat kuvaukset tarvittavista konfiguraatiosta yleisimmissä kohdejärjestelmissä niiden skannaamiseksi, kuvaus päivittäisistä, viikoittaisista tai kuukausittaisista ylläpitotehtävistä ja kuvaukset yleisimmistä ongelmatilanteista ja niiden ratkaisuista.

Lähteet

1 Hyvönen, Timo. 2008 Pitäiskö ottaa kolmonen? Verkkodokumentti. Timo Hyvönen. <http://www.itil.fi/2008/11/pitisk-ottaa-kolmonen.html> Luettu 3.4.2016.

2 ITIL ja parhaat käytännöt. Verkkodokumentti. itSMF Finland. <http://itsmf.fi/itil-parhaat-kaytannot/> Luettu 2.4.2016.

3 History of ITIL. Verkkodokumentti. IT Process Maps. <http://wiki.en.it-processmaps.com/index.php/History_of_ITIL> Luettu 2.4.2016.

4 The Official Introduction to the ITIL Service Lifecycle. 2007. Office of Government Commerce (OGC).

5 Klosterboer, Larry. 2008. Implementing ITIL Configuration Management. IBM Press ©.

6 BMC Step-by-Step Guide to Building a CMDB: Update for ITIL version 3. 2016. BMC Software Inc.

7 Lacy, Shirley& Borfolk, David. 2014. Configuration Management: Expert Guidance for IT Service Managers and Practitioners, Revised Edition. BCS ©.

8 BMC Software Inc history. Verkkodokumentti. BMC Software Inc. <http://www.fundinguniverse.com/company-histories/bmc-software-inc-history/> Luettu 11.4.2016.

9 About BMC Software. Verkkosivu. BMC Software Inc. <http://www.bmc.com/corporate/about-bmc-software.html> Luettu 11.4.2016.

10 Review of BMC ADDM. Verkkodokumentti. Sde0. <http://www.sde0.com/review-of-bmc-addm> Luettu 12.4.2016.

11 The Power Behind BMC Atrium Discovery and Dependecy Mapping. Verkkodokumentti. RightStar Systems. <http://www.rightstar.com/wp-content/uploads/2014/12/Power_Behind_ADDM_whitepaper.pdf> Luettu 13.11.2016.

12 Performance Data. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO83/Performance+data> Luettu 9.11.2016.

13 Licensing entitlement. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO110/Licensing+entitlement> Luettu 18.4.2016.

14 Factors affecting performance. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO83/Factors+affecting+performance> Luettu 9.11.2016.

15 Supported virtualization platforms. Verkkodokumentti. BMC Software Inc.<https://docs.bmc.com/docs/display/DISCO110/Supported+virtualization+platforms> Luettu 18.4.2016.

16 Sizing – initial guidelines. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO110/Sizing+-+initial+guidelines> Luettu 18.4.2016.

17 Discovery communication. Verkkodokumentti. BMC Software Inc.<https://docs.bmc.com/docs/display/DISCO83/Discovery+communication> Luettu 23.4.2016.

18 Network Usage. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO111/Network+usage> Luettu 20.11.2016.

19 Introduction to Discovery. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO83/Introduction+to+Discovery> Luettu 6.11.2016.

20 Hautaniemi, Mika. 1994. TKK/Atk-keskuksen TCP/IP-verkon valvonta ja hallinta. Diplomityö. .Teknillinen Korkeakoulu. Saatavilla verkossa: <https://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/SNMP.html> Luettu 6.11.2016.

21 Windows Proxy Deployment. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO110/Windows+proxy+deployment> Luettu 23.4.2016.

22 Windows Hosts. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO110/Windows+Hosts> Luettu 18.4.2016.

23 Windows operating systems. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO83/Windows+operating+systems> Luettu 25.4.2016.

24 Discovery Communications. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO111/Discovery+communications > Luettu 15.11.2016.

25 Discovering ESX and ESXi Hosts. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO111/Discovering+ESX+and+ESXi+hosts> Luettu 17.11.2016.

26 Discovering SNMP Devices. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO111/Discovering+SNMP+devices> Luettu 21.11.2016.

27 Adding Device Credentials. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO111/Adding+device+credentials> Luettu 21.11.2016.

28 Exporting Data. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO110/Exporting+data> Luettu 3.11.2016.

29 Understanding the export process. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO110/Understanding+the+export+process> Luettu 3.11.2016.

30 CMDB Synchronization. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO111/CMDB+synchronization> Luettu 2.11.2016.

31 Advantages of and appliance-based solution. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO111/Advantages+of+an+appliance-based+solution> Luettu 14.11.2016.

32 Appliance hardening. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO111/Appliance+hardening> Luettu 14.11.2016.

33 Information security. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO110/Information+security> Luettu 15.11.2016.

34 Integrating with CyberArk Enterprise Password Vault. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO111/Integrating+with+CyberArk+Enterprise+Password+Vault> Luettu 16.11.2016.

35 Masking sensitive data. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO111/Masking+sensitive+data> Luettu 16.11.2016.

36 System communications. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO110/System+communications> Luettu 15.11.2016.

37 User privileges and information access for Windows operating systems. Verkko-dokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO111/User+privileges+and+information+access+for+Windows+operating+systems> Luettu 15.11.2016.

38 DISA Secure Technical Implementation Guidelines. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO111/DISA+Secure+Technical+Implementation+Guidelines> Luettu 16.11.2016.

39 Running in FIPS compliant mode. Verkkodokumentti. BMC Software Inc. <https://docs.bmc.com/docs/display/DISCO111/Running+in+FIPS+compliant+mode> Luettu 16.11.2016.