jamk.fi

Valvontaympäristöjen hallinta

Joni Korpela

Opinnäytetyö
Toukokuu 2021
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), Tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Korpela Joni	Opinnäytetyö, AMK	Huhtikuu 2021
	Sivumäärä 47	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Valvontaympäristöjen hallinta

Tutkinto-ohjelma
Tieto-ja viestintätekniikka

Työn ohjaaja(t)
Tarja Lappalainen-Kajan, Mika Rantonen

Toimeksiantaja(t)
Toimeksiantaja

Tiivistelmä

Valvontaympäristöjen hallinta on olennainen osa verkko ja konesaliympäristöjen palveluita tarjoavien yritysten työssä. Tuotannossa olevat laitteet vaativat aktiivista hallintaa ja mukautuvuutta ympäristön ylläpidon ja kehityksen aikana. Uusien asiakkaiden laitteita valvonnan piiriin lisättäessä täytyy ymmärtää laajaa kokonaisuutta niin viitekehyksien kuin käytettävän teknologioiden kannalta.

ITIL viitekehyksestä on perehdytty service operation puoleen ja siinä käytettyihin määritelmiin, jotka ovat olennainen osa hallinnan puolta. Valvonta-alustoja on vertailtu laadullisen tutkimuksen menetelmin ja kahden erilaisen ympäristön etuja ja hyötyjä pyritty tuomaan esille käytännön kannalta. IT service management (ITSM) tikettijärjestelmiä ja niiden toiminnallisuutta on tutkittu, sekä käyttäjän että palveluntarjoajan näkökulmasta. Myös teknisessä mielessä valvonnan peruskomponentteja on tutkittu ja tunnistettu mistä elementeistä valvontaympäristö koostuu.

SL1 ja Servicenow alusta erottuu positiivisesti Netcool ja Maximo alustaan verrattuna ja antaa laajasti mahdollisuuksia toteuttaa modernien työkalujen avulla paljon edistyneitä toimenpiteitä erityisesti automatisoinnin osalta. Koska Servicenow työkaluun on asiakkailla pääsy omaan näkymään, niin helpottaa tämä nopeaa kommunikointia ongelmien kanssa ja mahdollistaa tapausten nopean käsittelyn. Netcoolin huonoin puoli on siinä, että se vaatii 24/7 resurssin hälytysten käsittelyyn ja myös hyvin paljon ammattitaitoa tikettien luojalta. Erilaisten asiakasympäristöjen sopimukset tulee tuntea ja varsinkin laitteiden nimeämispolitiikka, jotta tiketöinti tulee tehdyksi oikein. Molemmissa järjestelmissä on kuitenkin omat hyvät puolensa ja SL1 sekä Sciencellogic antaa paljon mahdollisuuksia tulevaisuudessa kehittämiseen, kun järjestelmää on muokattu enemmän tarpeisiin sopivaksi.

Avainsanat (asiasanat)

SL1, Servicenow, Netcool, Maximo, ITSM

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Korpela Joni	Bachelor's thesis	April 2021
		Language of publication: Finnish
	Number of pages: 47	Permission for web publication: x

Title of publication
Control of monitoring environments

Degree programme
Bachelor's Degree Programme in Information and Communications Technology

Supervisor(s)
Tarja Lappalainen-Kajan, Mika Rantonen

Assigned by
Client

Abstract

The management of control environments is an integral part of the work of companies providing IT services. Equipment in production requires active management and adaptability during the maintenance and development of the environment. When adding new customers' equipment to the scope of supervision, it is necessary to understand the broad entity in terms of both the framework and the technologies used.

The ITIL framework is familiar with the service operation side and the definitions used in it, which are an integral part of the management side. Control platforms have been compared using qualitative research methods and efforts have been made to highlight the benefits and advantages of two different environments from a practical point of view. IT service management (ITSM) ticket systems and their functionality have also been studied, from the perspective of both the user and the service provider. In a technical sense, the basic components have been studied.

The SL1 and Servicenow platform stands out positively compared to the Netcool and Maximo platform and offers a wide range of possibilities to implement many advanced measures with the help of modern tools, especially in terms of automation. Because the Servicenow tool gives customers access to their own view, this facilitates quick communication with problems and allows cases to be handled quickly. The downside of Netcool is that it requires a 24/7 resource to handle alerts and, also a great deal of professionalism from the ticket creator. Agreements in different customer environments need to be known and especially the equipment naming policy in order, for ticketing to be done correctly. Both systems have their own advantages, and SL1 and Sciencelogic offer many opportunities for future development as the system is more adapted to the needs of enviroment.

Keywords/tags (subjects)
SL1, Servicenow, Netcool, Maximo, ITSM

Miscellaneous (Confidential information)

Sisältö

Kuviot

1 Lähtökohdat

1.1 Toimeksiantaja

Opinnäytetyön toimeksiantajan toimi alalla toimiva Yritys. Yritys on toiminut pitkään erillaisten konesalien ja pilviteknologioiden sekä verkkoratkaisujen edelläkävijänä. Toimeksiantaja toteuttaa laajasti ja räätälöidysti vaativia asiakasratkaisuja tietoverkkojen, konesali- ja pilvipalveluiden sekä tietoturvan osa-alueilla. Tällä hetkellä yrityksessä työskentelee satoja, joilla on liki tuhat sertifikaattia.

Toimeksiantaja tarjoaa yrityksille hallinta- ja valvontapalveluja yli 40 asiantutijan voimin 24/7. Tämä pitää sisällään verkkoyhteyksien, laitteiden, liikenteen, ja sovellusten monitorointia. Näin asiakkaalle voidaan tarjota reaaliaikainen tilannekuva IT-palveluiden suorituskyvystä, käyttöasteesta ja toiminnasta sekä reagoidan asianmukaisesti ongelmatilanteisiin.

Palvelukeskus toimii asiakkaan ensisijaisena kontakti ja eskatointi kanavana. Tyypillisesti täällä käsitellään vianhallinnan näkökulmasta tapauksia, mutta myös pienemmät muutostyöt ja konfiguroinnit tehdään palvelukeskuksen toimesta. Karkeasti palvelukeskus jakautuu verkko ja palvelin osaajiin, jotka palvelevat asiakkaita ja valvovat ympäristöjä ympäri vuorokauden. Työ tapahtuu 24/7 vuorokierrossa ja asiantujijat ovat tavoitettavisa ympärivuorokauden sekä reagoivat asianmukaisesti jatkuvasti hälytyksiin ja asiakkaiden muutos sekä palvelupyyntöihin. Näin toimimalla yritys tuo lisäarvoa asiakkaiden liiketoimintaan vähentäen asiakkaiden tarvitsemaa IT hallinnan kuormaa ja saamalla apua moninaisiin kehitys ja ylläpitotehtäviin.

1.2 Motiivi

Yrityksessä eletään mielenkiintoista vaihetta, koska ympäristöjen valvontoja ollaan siirtämässä Netcool valvonnasta ScienceLogic valvontaan. Tällä hetkellä valvontaa suoritetaan molemmissa ympäristöissä, mutta pitkän ajan tavoite on siirtyä

kokonaan Sciencelogic ja SL1 puolelle. Opinnäytetyön kirjoitushetkellä yrityksessä iso osa laitteista on vielä IBM Netcoolin valvontojen alla, mutta siirtyminen ScienceLogic puolelle on jo hyvässä vauhdissa. Tässä työssä perehtytään molempien järjestelmien valvontojen hallintaan, koska nämä toimivat koko jatkuvien palveluiden yksikön keskiössä.

1.3 Tavoitteet

Työn tavoitteena on tutkia valvontaympäristöjen hallintaan liittyviä aiheita ja kahden erilaisen valvonta ympäristön eroja käytännön kannalta. Vertailemalla Netcool ja ScienceLogic välisiä eroavaisuuksia ja hyödyllisyyttä pyritään saamaan kuvaa kehityksen suunnasta siirtyessä alustasta toiseen. Molemmista alustoista tutkimuksen kohteena on sen sisältämät komponentit ja näiden ymmärtäminen.

Tarkastelussa on myös ITIL, koska tämä toimii yleisenä toimintaohjeena ja perustana palveluiden hallinnan kannalta. Valvontaympäristöjen hallinnan teoreettiset lähtökohdat ja tarpeet joiden ympärille se rakentuu voidaan helposti ymmärtää tämän pohjalta.

Lopussa käymmme läpi myös eri valvontojen tyyppejä ja näiden käyttämiä yleisiä protokollia, joka mahdollistaa kommunikaation laitteiden ja valvontaympäristön välillä.

1.4 Tutkimusmenetelmät

Opinnäytetyössä käytetään kvalitatiivista eli laadullista tutkimusta, sekä vertailevaa tutkimusta, koska tarkoituksena on käydä läpi kahta erilaista valvontaympäristöä ja niiden soveltuvuutta yrityksessä. Työssä on pyritty ymmärtämään valvontaympäristöjen hallintaa kokonaisuudessa ja näin työssä on tutustuttu aiheeseen, niin ITIL viitekehysten, tekniikan kuin protokollien puolelta. Laadullisen tutkimuksen avulla on saatu hyvin tuloksia havainnoimalla, miten käytännön työ sujuu eri järjestelmien

avulla ja mitä parannettavaa niissä on valvontaa harjoittavan toimijan puolella. Kvalitatiivisen tutkimuksen avulla pystyttiin tutustumaan kohteen ympäristöön, taustaan, tarkoitukseen ja merkitykseen yrityksessä.

2 ITIL ja Palveluiden hallinta

Valvontaympäristöjen hallintaan liittyy olennaisesti ITIL viitekehyksistä löytyvät määritelmät, siitä miten valvontaa suoritetaan ja miten erilaisiin tapahtumiin vastataan valvontaa suorittavan organisaation puolelta. Jotta käytännön valvontatyötä voi ymmärtää niin on hyvä tietää ITIL viitekehyksessä käsiteltäviä käsitteitä.

ITIL on maailmanlaajuisesti käytössä oleva 80-luvulla kehitetty viitekehys IT palvelujen kehittämiseen, valvontaan, suunnitteluun, käyttöön, palvelun siirtymiseen ja strategiaan. Sen tarkoituksena on helpottaa yrityksiä linjaamaan omia vaatimuksia ja tarpeitaan IT-palveluiden osalta. Uusin versio V4 on julkaistu 2019 alkupuolella.

ITIL kehitettiin Britannian hallituksen toimesta, kun se halusi laajentaa laskenta infrastruktuuria ja huomasi, että julkinen ja yksityinen sektori olivat molemmat kehittäneet omat kehyksensä IT palveluiden hallintaan, joka johti kalliisiin eskalaatioihin ja turhaan systeemien monimutkaisuuteen. Yhteistyö oli tämän vuoksi hankalaa varsinkin sen vuoksi, että IT infrastruktuuri kasvoi nopeasti globaaleissa organisaatioissa. Tämän johdosta hallitus aloitti kehittämään palvelun hallinnan käytäntöjä, jotka tunnetaan IT Infrastructure library eli ITIL nimellä. Ensimmäinen ITIL v1 julkaistiin vuonna 1989. (ITIL methodology)

2.1 ITIL

Valvontaympäristöjen hallinnan kannalta olennaisimpia ja näkyvimpiä kohtia ITIL viitekehyksestä ovat Palvelun hallinnan käytännöt. Näissä käsitellään yleisimpiä käsitteitä ja termejä, joiden avulla yksilöt ja organisaatiot voivat ylittää palvelun hallintaan liittyviä haasteita. Käsitteet ovat yleispäteviä eivätkä liity johonkin tiettyyn teknologiaan, vaan niitä voidaan soveltaa käytännössä hyvin laajasti erilaisissa ympäristöissä. ITIL v4 määrittelee palvelun hallinnan kokoelmaksi erikoistuneita organisaation kykyjä luoda arvoa asiakkaalle palveluiden muodossa.

2.1.1 Availability management

Saatavuuden hallinta pitää sisällään erilaisia monitoroinnin työkaluja, joiden avulla voidaan monitoroida ja analysoida laitteiden ja prosessien toimintaa, sekä tämän tiedon pohjalta suunnitella parannuksia tulevaisuutta mielessä pitäen. Tätä varten täytyy suunnitella infrastruktuuri, jolla saadaan dataa komponenteista ja palveluista järjestelmissä. Tällaisia järjestelmiä ovat mm. Netcool ja ScienceLogic, jotka agenttien, probejen, trappien ja muiden avulla keräävät ja lähettävät dataa palvelimille. Palvelimilta data nostetaan esiin valvonnanhallinta järjestelmiin.

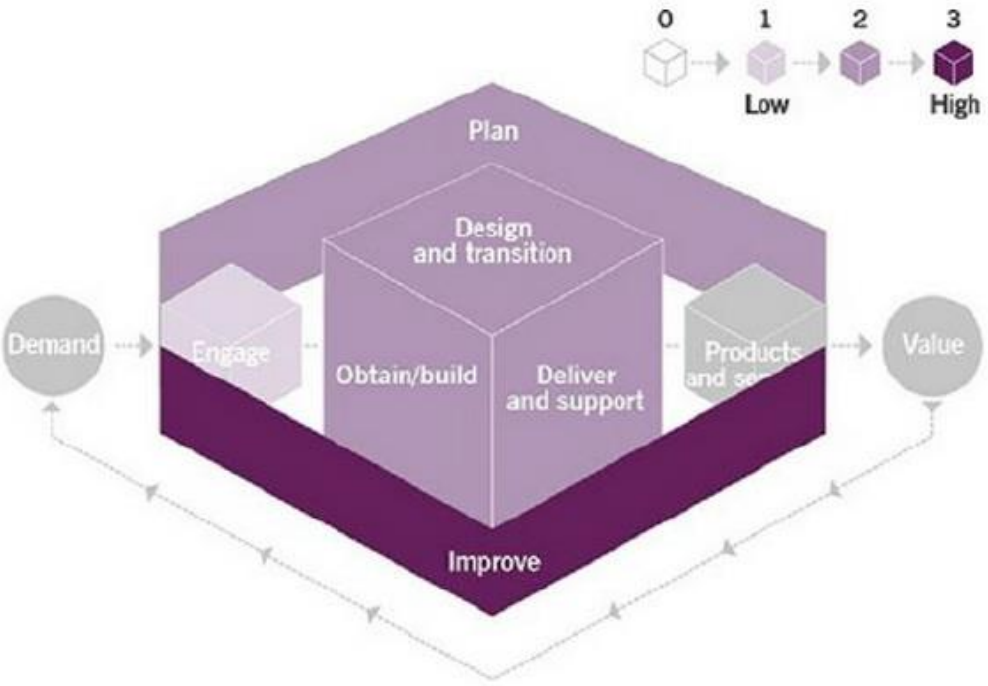
Saatavuuden hallintaa suunnitellaan prosessi, laite ja järjestelmäkohtaisesti. Kriittisyydeltään kaikissa edellä mainituissa on suuria eroja ja tämän vuoksi on äärimmäisen tärkeää tietää missä kohdassa palvelun nopeus on sitä luokkaa, että järjestelmän toiminta heikentyy ja mitkä laitteet ovat vastuussa palvelun toiminnasta. (Jouravlev, R., Anand, A., Orbezo, J., Casteel, E., Corona, M., DuMoulin, T., Hearsum, P., Hunnebeck, L., Leach, M., Rae, B., Rance, S., Yagi, T., Macdermind, K., 2019. ITIL Axelos – ITIL foundation 4 edition-Axelos 2019)

2.1.2 Capasity and performance managment

Kapasiteetti ja suorituskyvyn valvontaa suoritetaan asiakkaan vaatimusten ja tarpeiden mukaan. Palvelun suorituskyky on tärkeä osa asiakaskokemusta ja sen vuoksi on olennaista suorittaa jatkuvaa analyysiä siitä, miten laitteisto selviää siltä vaadittavista toimenpiteistä. Tuloksien valossa voidaan suorittaa parannussuunnitelmia, joiden

pohjalta voidaan rakentaa palvelujen kannalta kestäviä ratkaisuja. Analyysiä voidaan myös käyttää ennusteiden luontiin, joka auttaa kehitystyössä.

Suorituskyky on riippuvainen laitteiston kapasiteetista, joka määritellään maksimi suoritustehona, jota palvelu tai laite voi tuottaa. ITILv4 teoksessa on jaettu kapasiteetti ja suorituskyvyn hallinta kuuteen osa-alueeseen: Suunnittelu, kehittäminen, suorittaminen, transitio ja suunnittelu, hankinta ja rakentaminen sekä toimittaminen ja tuki. Alla näemme (Kuvio 1) lämpökartan arvoketjun aktiviteeteista. (Jouravlev ym. 2019.)



Kuvio 1. Arvotaulu.

Palveluiden jatkuva kehittäminen on erittäin tärkeä osa niin palveluntarjoajan, kuin asiakkaan näkökulmasta ja väin varmistetaan palveluiden laadun jatkuva paraneminen.

2.1.3 Muutoksen hallinta (Change control)

Muutoksen hallintaan kuuluu useita osa-alueita, kuten infrastruktuuri, applikaatiot, dokumentaatio, prosessit ja kaikki muut osat, jotka vaikuttavat tuotteeseen tai palveluun. Kaikki muutokset arvioidaan niiden ihmisten kesken, joilla on kyky ymmärtää riskit ja mahdolliset hyödyt. Ennen muutoksien käyttöönottamista ne täytyy hyväksyttää siihen nimettyjen henkilöiden kautta.

ITIL jakaa muutokset kolmeen eri tyyppiin: standardi muutos, normaali muutos ja hätämuutos. (Jouravlev ym. 2019.)

Standardimuutos

Tähän kuuluvat pieni riskiset, hyvin ymmärretyt ja dokumentoidut sekä ennalta hyväksytyt muutokset. Kun standardi muutosta suoritetaan, niin täytyy olla aina riskiarviointi ja hyväksyntä mille tahansa muulle muutokselle, jota mahdollisesti suoritetaan ohessa. Riskiarviointia ei täydy tehdä joka kerta uudelleen muuta kuin silloin jos tapa tehdä muutos muuttuu. (Jouravlev ym. 2019.)

Normaalimuutos

Nämä ovat muutoksia, jotka on aikataulutettu, arvioitu ja hyväksytty prosessin mukaisesti. Normaali muutokset voivat olla niin pieniä kuin isojakin muutoksia. Muutos malli voi olla esimerkiksi automatisoitu ajastettu muutos palvelimelle tai yrityksen luoma CM tiketti järjestelmään integraation kautta. (Jouravlev ym. 2019.)

Hätämuutos

Hätämuutokset ovat kiireellisiä toimenpiteitä, jotka täytyy ottaa käyttöön välittömästi. Näitä ei tyypillisesti ole aikataulutettu muutoskalenteriin etukäteen vaan korjaavia toimenpiteitä suoritetaan aina nopealla aikataululla. Hätämuutoksiin sovelletaan mahdollisuuksien mukaan samanlaista testausta, arviointia ja hyväksyntää, kuin

normaali ja standardimuutokselle. Yleensä hätämuutoksien varalle on olemassa erillinen nimetty henkilö, joka kykenee hyväksyttämään ja ymmärtämään näiden vaikutuksia erilaisissa ympäristöissä. (Jouravlev ym. 2019.)

2.1.4 Incident management

Incidenttien hallinnalla on suuri merkitys asiakkaiden ja palveluntuottajan välillä. Yleensä asiakkaalla on pääsy organisaation portaaliin, missä voidaan seurata erilaisia tapahtumia ja niiden historiaa. Kaikki tapaukset kirjataan ja hoidetaan erikseen sovittujen sopimusten mukaisesti, joissa on määritelty käsittely ja ratkaisu ajat. Erityisen tärkeää valvontojen kannalta on tunnistaa kriittiset prosessit ja laitteet, jotta priorisointi voidaan määritellä vastaamaan sen tärkeyttä tuotannossa. (Jouravlev ym. 2019.)

Organisaatioiden tulee suunnitella Incidenttien hallintaa varten oikeanlainen hallintaympäristö ja määrätä oikea määrä henkilöstöä vastaamaan erilaisista incidenteistä. Erilaisia tapauksia käsitellään mahdollisimman tehokkaasti, jotta työ ei vie liikaa resursseja. Tämän vuoksi tapauksia tallennetaan kantoihin sopivilla työkaluilla ja näistä voidaan tapahtuman uusiutuessa katsoa mallia, miten edellisellä kerralla tapahtuma on ratkaistu. (Jouravlev ym. 2019.)

Kommunikointi ja eskalointi

Tehokas tapahtuman valvonta vaatii hyvien, toimivien valvontojen lisäksi tapahtumien ratkaisuun laajaa kommunikointia eri tahojen kesken, jotta erityyppiset ongelmatilanteet voidaan ratkaista tehokkaasti. Tyypillisesti valvontaa suorittava taho on yhteydessä mm. seuraaviin: asiakas, tiimiläiset, eskalaatiokanavat, laite valmistajat, operaattorit ja paikallisiin kolmannen osapuolen toimijoihin. (Jouravlev ym. 2019.)

Yrityksessä valvonnan seurannasta ja tarvittavista toimenpiteistä vastaa palvelukeskus, jonka kautta kaikki tapahtumat, joko ratkaistaan tai eskaloidaan eteenpäin. Palvelukeskuksessa työskentelevillä henkilöillä on pääsy valvontatyökaluihin ja asiak-

kaan ympäristöihin, jossa voidaan suorittaa korjaavia toimenpiteitä, sekä arvioida tilanne ja tarvittaessa eskaloida se tilanteen vaatimalla tavalla tarvittaessa eteenpäin tai korjata itse.

Koska asiakkaita on runsaasti, niin asiakkaista täytyy löytyä kattava dokumentaatio työn tueksi, jotta tapahtumien ratkaisu on sujuvaa. Näihin kuuluu mm. ohjeet laitteille pääsyyn, ympäristökuvaus, asiakaskohtainen palveluopas ja muita asiakasympäristön hallinnan kannalta olennaisia asioita.

2.1.5 Monitorointi ja eventtien hallinta

Tapahtumien hallinnalla tarkoitetaan osaa, jossa keskitytään tallentamaan ja hallinnoimaan tilamuutoksia tapahtumista, joista organisaatio on kiinnostunut ja joiden avulla voidaan tunnistaa ja korjata ongelmia. Jotta tapahtumien hallinta on mahdollista, niin valvontaa suoritetaan laajasta määrästä dataa, mutta kaikki data ei johda kuitenkaan toimenpiteisiin ja näin niitä ei välttämättä nosteta tapauksiksi (Incident).

Tapahtumat voidaan jakaa kolmeen osaan, jotka ovat: informaationaaliset, varoitukset ja poikkeukset. Informaatio tapahtumat eivät vaadi välittömiä toimenpiteitä, mutta niitä voidaan käyttää datan analysoinnissa myöhemmässä ajankohdassa. Varoitus tapahtumat mahdollistavat ennalta ehkäisevien toimenpiteiden suorittamista, ennen vakavamman tapahtuman ilmaantumista. Poikkeus tapahtumat vaativat toimenpiteitä, mutta tämä ei välttämättä tarkoita, että tällä poikkeuksella olisi vielä suoraa vaikutusta esimerkiksi asiakkaan järjestelmiin. (Jouravlev ym. 2019.)

Onnistuneessa tapahtumien hallinnassa täytyy ottaa huomioon useita prosesseja ja käytäntöjä, joista tärkeimpiä ovat seuraavat. Tunnistetaan mitä palveluita, järjestelmiä, laitteita jne. tulee monitoroida, jotta strategia toteutuu. Käyttöönotto ja ylläpito monitorointien osalta tukee setä natiiveja monitorointi ominaisuuksia, että erikseen tiettyyn järjestelmään suunniteltuja työkaluja. Kynnykset hälytyksien nousemiselle tapahtumiksi on asetettu niin, että ne sopivat esimerkiksi informaatio, varoitus tai poikkeus kategorioihin. Varmistetaan prosessien toimivuus kaikissa kategorioissa,

sille kuuluvalla vakavuudella. Automatisoinnin toteutuksessa prosessien tulee vastata tarvittavia kriteerejä, raja-arvoja sekä politiikkaa. (Jouravlev ym. 2019.)

Kun monitorointeja pystytetään, niin on tärkeää ottaa jo suunnittelu vaiheessa mukaan erilaisista erikoistumisen osa-alueista ja myös varmistaa erilaisten ryhmien pääsy tarvittavaan dataan.

2.1.6 Problem management

Kaikissa järjestelmissä ja laitteissa on omat viat, haavoittuvuudet ja heikkoudet, jotka voivat aiheuttaa tapauksia. Monet viat tunnistetaan jo ennen käyttöönottoa, mutta joitakin heikkouksia saattaa päätyä tuotantoon ja näin ne ovat riskejä. Näistä ITIL käyttää nimitystä ongelmat ja niille pätee omat hallinta käytänteet.

Tapahtumien tautalla saattaa olla ongelma, ja näissä tapauksissa on syytä analysoida ja tunnistaa syyt sekä kehittää ratkaisu pitkä aikaisen vian syntymiseen. Näin toimimalla voidaan vähentää huomattavasti tapahtumien syntymistä pitkällä aika välillä.

Ongelmien tunnistaminen pitää sisällään seuraavia toimenpiteitä. Suoritetaan analyysiä tapahtumista ja seurataan mitä trendejä sieltä voidaan löytää. Tunnistetaan duplikaatit ja toistuvat tapaukset. MIM tapauksissa tunnistetaan riski siitä, että tapahtuma voi toistua. Analysoidaan toimittajilta yhteistyökumppaneilta saatua dataa. Analysoidaan sisäisten ryhmittymien, kuten projekti ja kehittäjien tuomamaa dataa. On myös muita tapoja tunnistaa ongelmia ja työ näiden kanssa on jatkuvaa ja vaatii panostusta yritykseltä. Usein ongelmien syyt ovat hyvin monimutkaisia ja tapahtumien sattuessa tulisi käydä läpi laajasti näiden syitä, jotta tulevaisuudessa vältytään vahingoilta. (Jouravlev ym. 2019.)

2.2 Service level agreement (SLA)

Palvelusopimus tehdään palveluntarjoajan ja asiakaan välille yhteystyön alkaessa ja tässä voidaan määritellä hyvinkin tarkkaan, millaista palvelua odotetaan saatavan ja määritellään mittareita, joilla voidaan katsoa, onko palvelu tuotettu sovitulla tavalla. SLA on hyvin tärkeä dokumentti ja sitä luodessa täytyy olla tarkkana, että palvelu vastaa odotuksia ja tarpeita. Palvelusopimus on aina yksilöllinen ja niissä esiintyy hyvin laajasti eroja. Palvelusopimuksen tarkoituksena on suojata molempia osapuolia. Toisaalta SLA määrittelee mitä tavoitteita palvelun tulee saavuttaa kuin, että mitä palvelusta voidaan laskuttaa. Jos tavoitteita ei saavuteta niin palvelusopimuksessa on määritelty korvatta summa tai palveluiden alennus. (SLA template examples)

Esimerkkejä sopimuksen sisällöstä

Alla on yksi mahdollinen sisällysluettelo (Kuvio 2). Monitoroinnin ja tapauksien vasteajan kannalta olennaiset asiat löytyvät kuvion kohdasta 3. Tämän kappaleen sisältö voi tyypillisesti sisältää useita komponentteja niiden alaosioita.

Table of Contents

Kuvio 2. SLA sisältö

SLAn mitattavat arvot riippuvat siitä, mitä palvelua kyseinen sopimus koskee. Alla on (Kuvio 3) esimerkkitaulukko 3.3 kohdasta, jossa on hahmoteltu priorisointeja ja vasteaikoja palveluille. Tasolla 6 olevaa tietoa säilötään ja käytetään ongelmanratkaisun apuna, mutta niitä ei nosteta tiketeiksi välttämättä Maximo ja Servicenow alustoille incidenteiksi. 4 ja 1 tasojen hälytykset nousevat / nostetaan tiketeiksi ja näiden osalta tehdään tarvittavat toimenpiteet vaste aikaa kunnioittaen. Prio 1 tiketit vaativat välitöntä huomiota ja kyseessä on aina jokin vakava tilanne, jonka ympärille perustetaan välittömästi asiantuntija tiimi hoitamaan tapausta. Näistä puhutaan myös Major Incident Managemment (MIM) prosesseista, joissa on tietyt toimintamallit, joita harjoitellaan työntekijöiden toimesta aina väliajoin.

Severity Level	**Description**	**Target Response**
1. Outage	SaaS server down	Immediate
2. Critical	High risk of server downtime	Within 10 minutes
3. Urgent	End-user impact initiated	Within 20 minutes
4. Important	Potential for performance impact if not addressed	Within 30 minutes
5. Monitor	Issue addressed but potentially impactful in the future	Within one business day
6. Informational	Inquiry for information	Within 48 hours

Kuvio 3. Prioriteetti esimerkki.

Yllä olevan (Kuvio 3) esimerkkitaulukon avulla voidaan hahmottaa monitoroinnissa käytettävää priorisointia ja näiden avulla konfiguroidaan valvonnan prioriteetit hälytyksiin ja saavutetaan palvelusopimuksessa määritellyt tavoitteet vasteajoista. Resurssien ja prosessien toimiminen on hyvin tärkeää, jotta tavoitteisiin päästään palveluntarjoajan puolelta. Hyvän dokumentaation tärkeys tavoitteisiin pääsemisestä on suuri, kun vasteajat ovat lyhyitä ja tämän vuoksi ohjeet erilaisissa tilanteissa toimimiseen täytyy olla selkeät valvontaa suorittavalle taholle.

2.3 Palvelukeskus ja järjestelmät

Toimeksiantajan palvelukeskus toimii asiakkaan ensisijaisena yhteyspisteenä, ja yksikössä työskentelevät henkilöt ottavat vastaan vikatilanteita / konfiguraatioita koskevat puhelut, sekä hoitavat hälytyksistä syntyvät / asikkaiden luomien tikettien alkututkinnan / ratkaisemisen tai eskaloivat tarpeen vaatiessa eteenpäin. Sekä Maximo että Servicenow järjestelmiin tulevat asiakkaiden luomat Incident tiketit kuuluvat palvelukeskuksen vastuualueisiin ja myös palvelupyynnöt ohjataan eteenpäin tai ratkaistaan itse.

Koska palvelukeskus hoitaa laitteiden konfigurointia ja viantutkintaa, niin kyseinen tehtävä vaatii laajan dokumentointi järjestelmän tuekseen, josta löytyy asiakaskohtaiset dokumentaatiot ympäristöistä. Suuren datan vuoksi näitä kutsutaan wikipedioiksi, josta hallintaan tarvittava materiaali säilötään. Esimerkiksi verkkokuvat ovat hyvin käytännöllinen apu ongelman selvityksessä, ja näitä täytyy pitää ajan tasalla aktiivisesti muutoksien tapauksessa.

Jatkuva priorisointi

Koska ITSM pyörii SLA aikojen ympärillä niin täytyy ongelmien selvitystä ajoittaa niin, että sopimuksissa määrätyissä ajoissa pysytään mahdollisimman hyvin. Suuri osa ti-

keteistä on Incident tyyppisiä ja ratkaisuajat riippuvat ongelman tyypistä 15 minuutista muutamaan päivään. Puhelimen välityksellä tulee tämän lisäksi välitöntä huomiota vaativia tapauksia kuten asentajan soittoja paikanpäältä, jolloin päästään konsoli kaapelin avustuksella konfiguroimaan laitteita. Myös asiakas eskalaatioita erilaisista ongelmista otetaan työn alle puhelimesta ja tarpeen vaatiessa viedään tapausta eteenpäin eri asiantuntijoille.

3 Valvonnan työkaluja

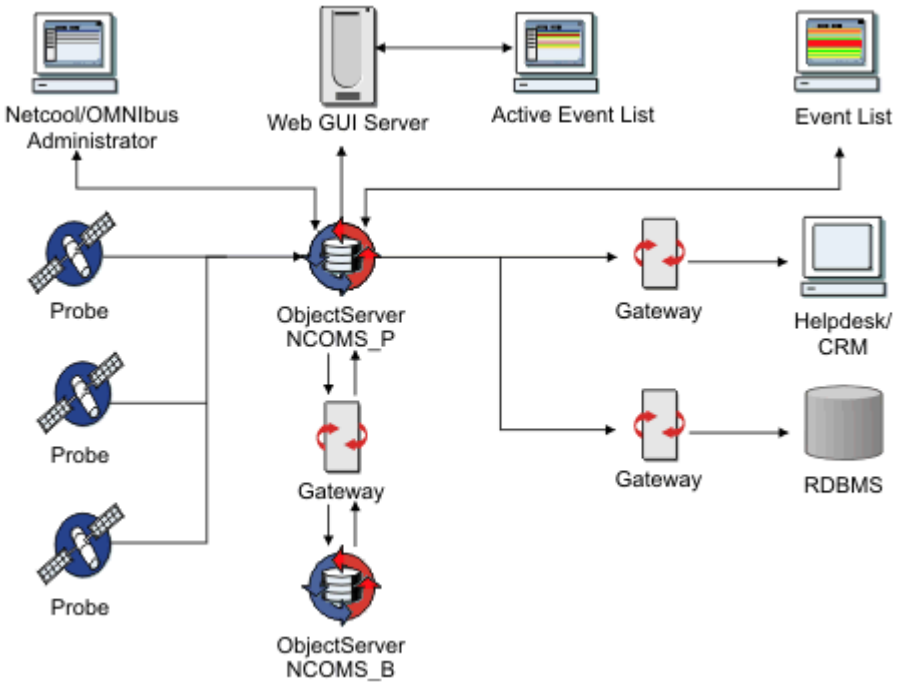
Laajojen verkko ja konesaliympäristöjen valvonta vaatii runsaasti tietoa laitteista ja niiden kunnosta, suorituskyvystä, saatavuudesta ja erilaisista toiminnoista. Koska valvontaa suorittavien yritysten verkoissa on tyypillisesti satoja tuhansia laitteita niin manuaalinen infrastruktuurin valvonta on mahdotonta ilman sopivien ohjelmistojen apua. Kasvava IT infrastruktuurin monimutkaisuus tekee vian selvityksestä vaikeaa ilman moderneja ohjelmistoja, koska palveluihin vaikuttavat mm. laitteet, verkko, sovellukset, tietokannat, käyttöliittymät ja rauta. Vikatilanteen sattuessa syyn etsintä voi olla haastavaa ilman oikeita työkaluja ja strategioita. (Infrastructure monitoring tools)

3.1 Tivoli Netcool/OMNIbus

Tivoli Netcool/OMNIbus on ITSM (Service management level) alusta, joka tuottaa reaaliaikaista, keskitettyä monitorointia moninaisista verkkolaitteista ja palvelimista sekä niiden tapahtumista. Järjestelmä seuraa hälytysinformaatiota verkoista ja sen laitteista sekä esittää informaation eri filttereiden ja näkymien kautta, joita voidaan muuttaa erikseen. Tivoli Netcool/OMNIbus omaa automatisoinnin ominaisuuksia, joilla voidaan luoda älykkäitä ominaisuuksia hälytyksien valvontaan. Järjestelmä on ollut yrityksessä pitkään käytössä ja sen vuoksi sitä on muokattu hyvin toimivaksi työkaluksi päivittäisten vikatilanteiden ja muiden tapahtumien seurannassa.

Netcool komponentit

Tivoli Netcool/OMNIbus koostuu seuraavista komponenteista (Kuvio 4): Objectserver, probes, gateways, työpöytä työkalut, admin työkalut ja web GUI visualisointi komponentista. Seuraava kuva näyttää esimerkki topologian, jossa probet lähettävät hälytyksiä Objectserverille ja gateway replikoi nämä hälytykset toiselle Objectserverille toimien fail overina. Kahdesta muusta gatewaysta toinen välittää tietoja Customer Service Managmentille (CRM) työkaluille ja toinen relation management systemeille (RDBMS). Ylhäällä (Kuvio 4) näemme muita configuroituja työkaluja, kuten admin consolin ja sekä web GUI event listan sekä työkalulla avattavan event list työkalun. (Tivoli Netcool / OMNIbus components)



Kuvio 4. Netcool komponentit.

Object Server

Yllä (Kuvio 4) näkemämme objectserver on in-memory tietokanta ja se on Tivoli Netcool/OMNIbus järjestelmän ydin. Eventti tiedot välitetään objectserverille probeilta ja gatewayltä. Tämä tieto tallennetaan ja näytetään ulkoisissa ohjelmissa kuten event list työkalussa. Haittapuolena on se, että vikatilanteessa kaikki tieto häviää. Objectserver käyttää hyötynä deduplikaatio ominaisuutta, jolla varmistetaan, että

sama eventti ei lähde kahtena erillisenä hälytyksenä vaan lisää sen alkuperäiseen hälytykseen (count arvoon). Tämä toiminto säästää muistiin tallennetun datan määrää. Object serverille voidaan myös konfiguroida automaattisia toimintoja, joka vähentää huomattavasti hälytysten kokonaismäärää ja näin helpottaa operoijan työtä. (Tivoli Netcool / OMNIbus components)

In-memory tietokanta tallentaa tietoa vain muistiin ja lähettää sen eteenpäin, joka mahdollistaa jopa mikrosekuntien vasteajan. Muistitietokannan hyötynä on se, että vasteaika on minimaalinen, koska tarvetta levyn lukuun tai kirjoittamiseen ei ole. (In memory)

Probes

Probet ovat yhteydessä eventtien lähteeseen ja voivat näin saada tietoa, jota lähetetään edelleen objectserverille eventteinä. Probet käyttävät ennalta määriteltyjä sääntöjä, jolla voidaan muokata elementtejä ennen muuntamista niitä eventeiksi objectserverin alert.status pöytään. Jokainen probe on suunniteltu erikseen sopimaan kyseiseen ympäristöön ja sillä voidaan hankkia tietoa mistä tahansa laitteesta, tietokannasta tai log tiedostosta. Probeja voidaan myös konfiguroida muokkaamaan tai lisäämään tietoa eventti dataan. (Tivoli Netcool / OMNIbus components)

Gateway

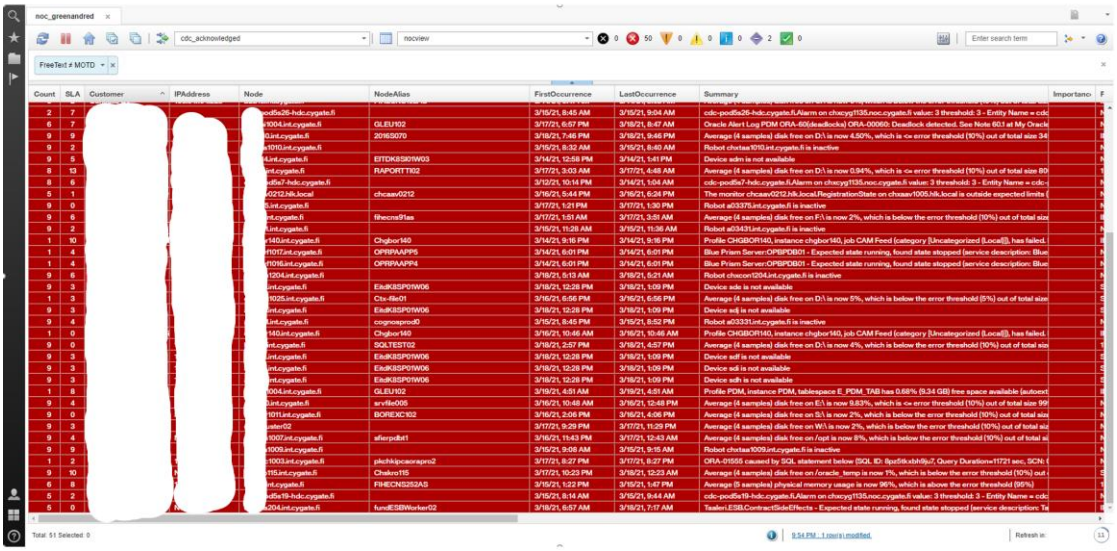
Gatewaytä käytetään mahdollistaan kommunikaatio objectserverin ja kolmannen osapuolen aplikaatioiden välillä. Kuten kuvan (Kuvio 4) topologiassa näimme, niin on mahdollista käyttää useita gatewaytä välittämään tietoa eri sijainteihin, työkaluihin ja tietokantoihin. (Tivoli Netcool / OMNIbus components)

Työpöytätyökalut

Työpöytätyökalut ovat paketti graafisia työkaluja, joilla käsitellään eventtejä, sekä konfiguroidaan mitä informaatiota halutaan nähdä. Työkalu vastaanottaa kaiken datan ja näin tietoa tulee sekunnissa valtaisa määrä, kun laitteita on esimerkiksi tuhansia. Tämän vuoksi työkalu konfiguroidaan suodattamaan vain kyseisessä tehtävässä tarvittavaa dataa. Esimerkiksi L1 tason datasta tarvitaan käytännössä vain tieto siitä,

onko yhteys esimerkiksi porttiin, päätelaitteeseen, Access pointtiin, reitittimeen, kytkimeen, palvelimeen aktiivinen. Tyypillisesti kuitenkin event listalta halutaan useaa erilaista tietoa niin sovelluksista kuin CPU / muistinkäytöstä. (Tivoli Netcool / OMNIbus components)

Desktop työkalu on käytettävissä vain Windows OS, mutta Linux OS voidaan käyttää web GUI työkalua, joka on ominaisuuksiltaan hyvin lähellä työpöytätyökalua. Web GUI hyötynä on se, että siihen voidaan saada yhteys useista eri lähteistä (Kuvio 5). Kätevä ominaisuus on myös, että web versio pitää sisällään enemmän graafisia ominaisuuksia.



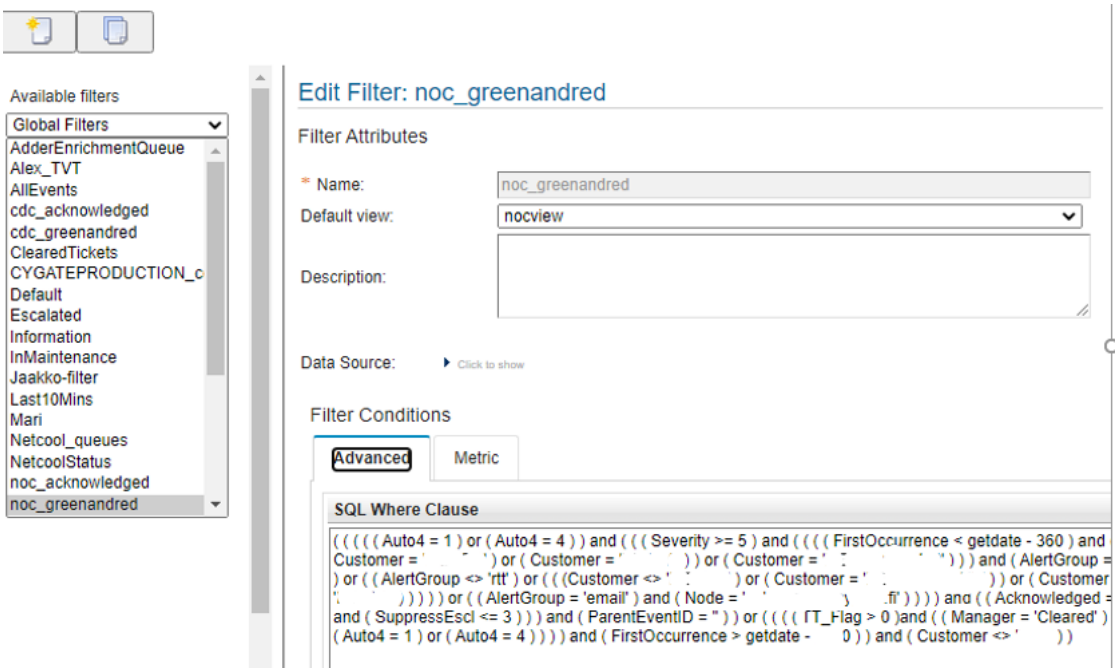
Kuvio 5. Netcool

Yllä (Kuvio 5) näemme hälytystaulun näkymän, jota lukemalla ”hälyhenkilö” avaa tarvittaessa tiketin Maximoon käsiteltäväksi. Tärkein seuratta kenttä tässä on summary, jossa on informaatio hälytyksestä ja tämä tieto määrittää käytännössä luotavan tiketin prioriteetin ja, koska tämä tehdään käsityönä, niin täytyy tiketin tekijän olla hyvin tietoinen sen kriittisyydestä. Tilanteet, jossa työkaluun tulee runsas määrä hälytyksiä tietystä paikasta, niin täytyy tunnistaa korkeimman prioriteetin laite ja liittää muut

hälytykset tämän alle. Esimerkiksi jos toimipaikalla hälyttää node unreachable palomuuri, reititin, kytkin ja AP niin tiketti luodaan palomuurista, koska tämä on reunimmaisin laite ulkoverkkoon topologiassa.

Administrator työkalu

Administrator työkalussa on graafinen käyttöliittymä ja sitä käytetään mm. objectserverin ja tietokannan muokkaukseen. Objectserver pitää sisällään SQL käyttöliittymän, jolla voidaan muokata relaatiotietokannan objekteja, kuten pöytiä ja näkymiä. Alla (Kuvio 6) näemme GUI työkalun filter ehdot, joilla se kyselee tietoa tietokannalta.



Kuvio 6. Filtteri.

Confpack apuohjelmalla voidaan tehdä import ja export toiminnot, joten konfigurointien kopiointi toiseen defaultgatewayhin onnistuu helposti. Myös objectserverin konfiguraation osia voidaan kopioida helposti, joka helpottaa toisen objectserverin automaation ja event listojen luomista.

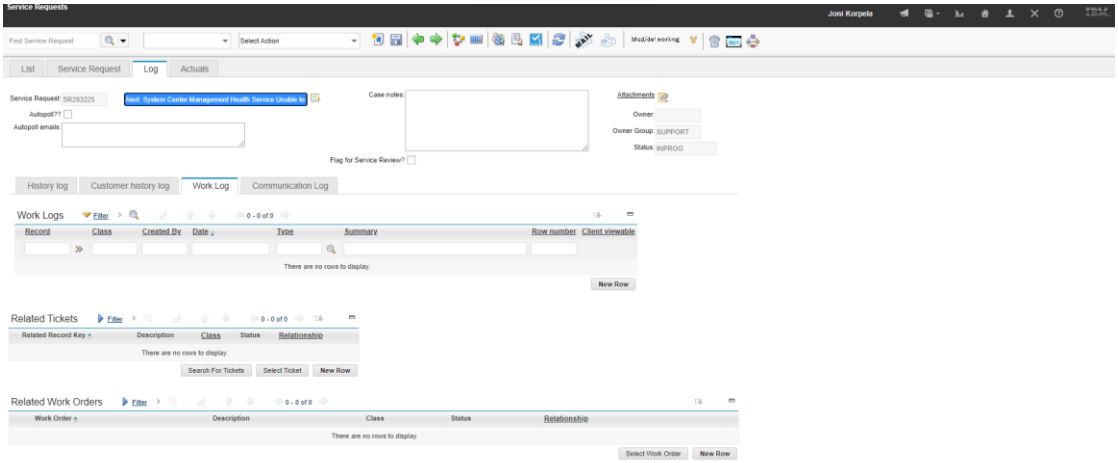
Prosessi kontrolli systeemi pyörittää ulkoisia automaatio prosesseja, jolla voidaan havaita objectserverin muutoksia ja hallita niin sisäisiä kuin ulkoisiakin prosesseja. Ulkoisia prosesseja ovat agentit, joita voidaan asentaa hosteille hallintaa varten. (Tivoli Netcool / OMNIbus components)

3.2 Maximo

Maximo on tikettien hallinta järjestelmä, johon Netcool hälytysten valvonnasta luodaan tikettejä. Nämä ovat tyypiltään IM (Incident management) tikettejä. Kuten aiemmin kävimme ITIL osuudessa läpi niin ITSM mukaisesti Maximosta löytyy myös Change management (CM), Proble management (PM) ja Service request (SR) tyyppiset tikettimuodot. Nämä ovat asiakkaan kanssa sovittuja ja kirjallisesti Maximoon tehtyjä tikettimuotoja.

Maximon näkymiä voidaan muokata haluaman mukaan jokaiselle käyttäjälle omalla tavalla mieleiseksi, kuten luomalla näkymiä ja määrittelemällä näytettävän sisällön.

Hakutoimintoja voidaan suorittaa IM, SR, CM ja PM tiketeistä kantaan ja näin etsiä vanhoja tikettejä ratkaisun tueksi (Kuvio 7). Hakukenttinä toimivat tikettinumero / asiakas / avainsana jne. valikot ja etsiminen on helppoa ja toimivaa tällä tyylillä.



Kuvio 7. Maximo tiketti näkymä

Yllä (Kuvio 7) näemme SR tiketin eri valikot. Work Log välilehdelle kirjataan kaikki tutkimukset ja tehdyt toimenpiteet. Kirjauksille voidaan valita, onko tieto asiakkaalle näkyvä vai sisäisiä kommentteja. On hyvin tärkeää, että kaikki tutkimukset ja toimenpiteet kirjataan tiketille, koska näin vältetään turhia työtunteja, kun seuraava henkilö alkaa käsittelemään samaa tapausta. Actuals välilehdelle voidaan kirjata tuntimerkintöjä, jotka menevät laskutukseen. Maximo ei laske tikettiin käytettyä aikaa vaan se täytyy hoitaa erikseen kirjaamalla.

Maximo on mielyttävä käyttää ja näkymät ovat selkeitä ja ylipäänsä sen käyttö on hyvin intuitiivista ja helppoa. Ainut miinuspuoli Maximosta on, että se ei näytä miten-kään SLA aikoja, muuten kuin luonti aikaleiman muodossa ja tästä täytyy itse tietää paljonko aikaa, on jäljellä.

Tikettien hallinta

Kuten ITIL osuudessa lyhyesti kävimme läpi niin kaikki erityyppiset tiketit SR (service request), CM (change management), PM (problem management ja IM (incident management) työstäminen tapahtuu palveluntarjoajan puolesta SLA:ssa määriteltyjen aikojen puitteissa. Prioriteetit taas määrittelet kuinka paljon aikaa saa kulua tiketin ratkaisuun ja näin palveluntarjoaja välttää mahdolliset sanktiot.

Näkymät on jaettu eri service line väreihin, joita on neljä (keltainen, punainen, vihreä, sininen). Näin on helpompi löytää eri väreihin kuuluvien asiakkuuksien tiketit.

3.3 ScienceLogic

ScienceLogic on vuonna 2003 perustettu amerikkalainen ohjelmisto ja palvelutalo, joka tarjoaa moderneja ratkaisuja IT operaattoreille. Sen alusta on näyttänyt arvonsa palvelujen laadun, sekä hybrid/multi-cloud ympäristöjen optimisoinnin ja työkalujen modernisoinnin alueilla. Se on hoitanut näitä tehtäviä onnistuneesti osittain reaaliaikaisen data laken avulla, joka on suunniteltu erityisesti AIOPs vaatimuksia varten.

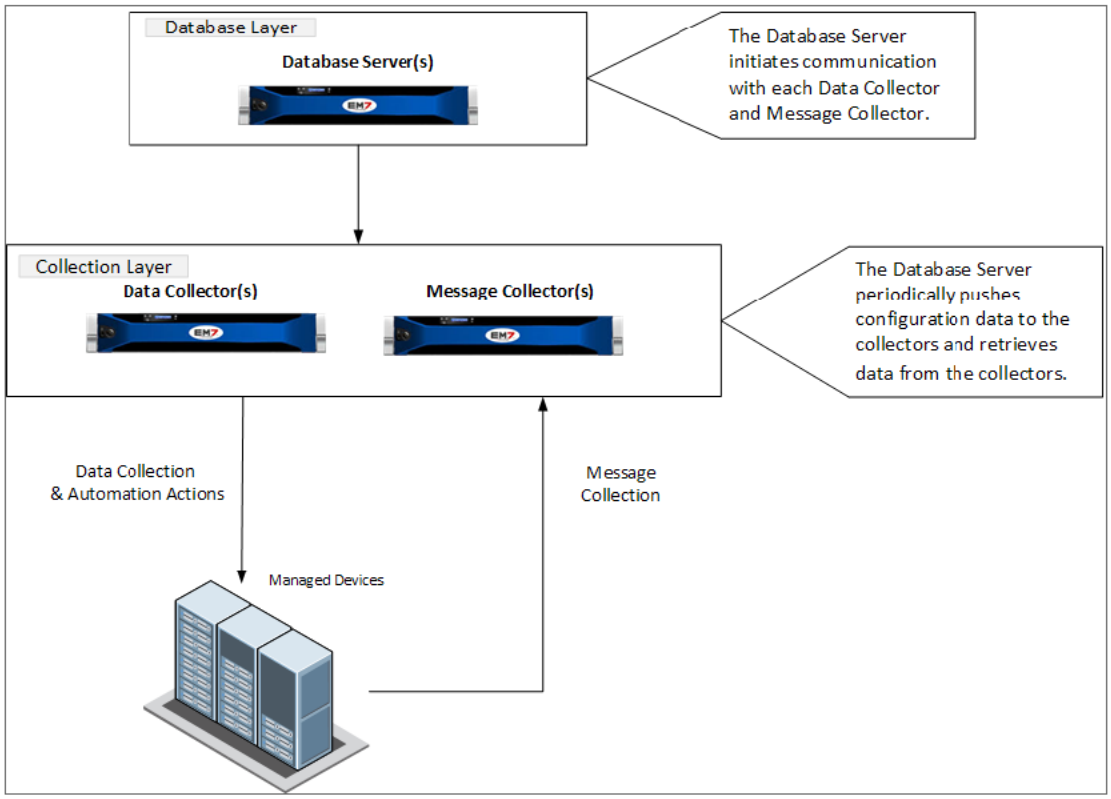
ScienceLogic SL1 alusta on nimenomaan suunniteltu Managed Service Provider (MSP) ja suurille yrityksille, jotka vaativat datan keruuta ja työkaluja parantaakseen AI/ML (Artificial Intelligence / Machine Learning) prosesseja. Arvosteluissa se on saanut huippupisteitä alustan toimivuudesta ja arkkitehtuurista. (Ema radar)

ScienceLogic on myös nimetty DoDIN (U.S Department of Defence Indormation Network) hyväksyttyjen tuotteiden listalle (APL). ScienceLogic on ensimmäinen end-to-end IT infrastruktuurin monitorointi yritys, joka on mukautunut vaativiin turvallisuus ja yhteensopivuus vaatimuksiin, joita DoDIN vaatii. (Datasheet-SL1-Platform-Security, 2020)

3.3.1 SL1 komponentit

SL1 jakautuu neljään osaan: käyttöliittymä, tietokantaserveri, Data ja message collector. On mahdollista myös asentaa kaikki yhdelle laitteelle (All-In-One Appliance), joka on hyvä ratkaisu pienemmissä ympäristöissä.

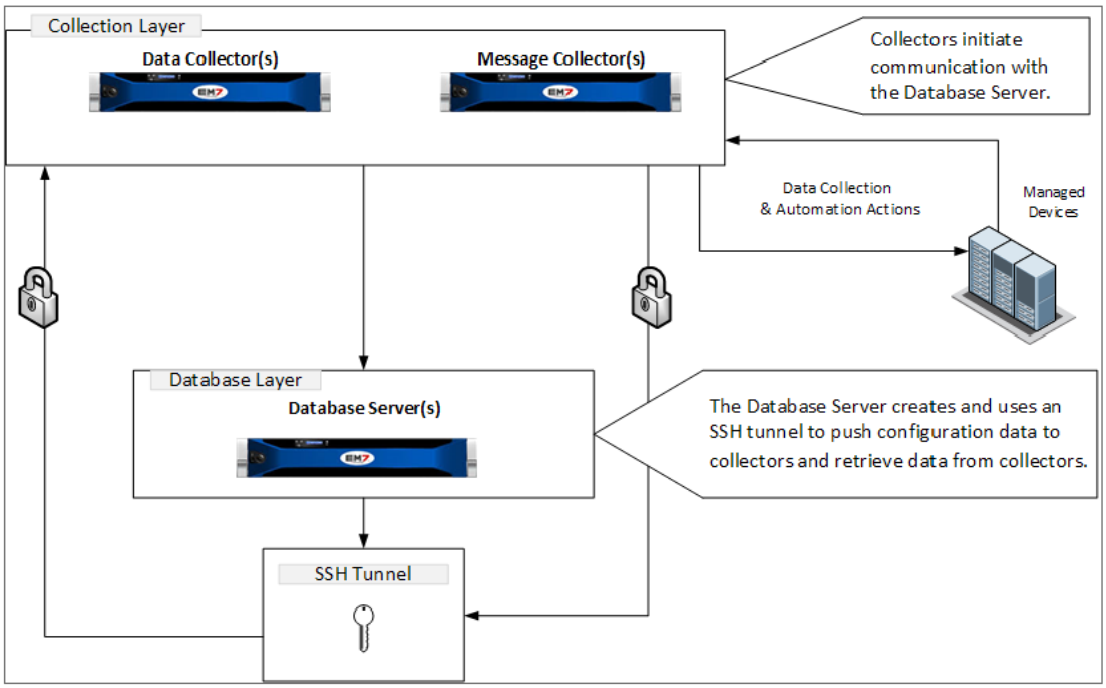
Alla esimerkki (Kuvio 8) perinteisestä topologiasta, jossa database server aloittaa kommunikoinnin jokaisen data ja message collectoring kanssa. Database server voi työntää konfiguraatiota data ja message collektoreille, sekä noutaa dataa näiltä. (Sciencelogic integration service servicenow)



Kuvio 8. Tyypillinen SL1 topologia.

Tämän tavan etuna on se, että database serverin kommunikaatio on rajattua ja näin se pysyy paremmin suojassa, sekä piilossa.

Toinen tapa rakentaa ympäristö on käyttää PhoneHome metodia (Kuvio 9), jossa Data ja Message kontrollerit aloittavat kommunikoinnin Database serverille. Data ja message kontrollerit luovat SSH tunnelin serverin suuntaan, jonka avulla voidaan työntää konfiguraatioita ja myös noutaa tietoa. (Sciencelogic integration service servicenow)



Kuvio 9. PhoneHome.

Tämän metodin hyötynä on, että palomuuriin ei tarvitse lisätä sääntöjä ja TCP portit ovat auki data kollektorit sisältämässä verkossa. Konfiguraatio käyttää public / private key tunnistautumista pitääkseen yllä turvallisen yhteyden database serveriin. Database serverillä jokainen SSH yhteys on rajattu ja ei pidä sisällään esimerkiksi lupaa kirjautumiselle, mahdollisuutta päästä shelliin tai ajamaan execute komentoja. (Sciencelogic integration service servicenow)

Käyttöliittymä

Niin pääkäyttäjä kuin muutkin käyttäjät käyttävät web selaimessa käyttöliittymää. Käyttöliittymän avulla voidaan mm. tarkastella kerättyä dataa, luoda raportteja, määritellä policyt, tutkia eventtejä ja luoda tikettejä. Käyttöliittymää voidaan käyttää joko All-In-One Appliancelta tai erilliselle laitteelle asennetulta Database serveriltä / admin portal aplikaatiolta. Admin portalin käyttöliittymän erona on, että se kommunikoi pelkästään Database serverin kanssa käyttäen molempiin suuntiin salattua liikennöintiä. (Sciencelogic integration service servicenow)

Database server

Database serverillä on useita tehtäviä: prosessointi, automaatiot, Email vastaanotto ja lähetys sekä tiketöinti, tallentaa kaiken konfiguraatio datan, policy datan, performance datan ja kyselee sekä vastaanottaa tietoa muilta SL1 laitteille tarvittaessa. Kyseessä on siis koko järjestelmän sydän. (Sciencelogic integration service servicenow)

Data collection

Tällä tarkoitetaan LS1 laitetta, joka hakee dataa valvottavilta laitteilta. Tässä vaiheessa voidaan myös suorittaa jo datan esikäsittelyä automatisoiduilla toimenpiteillä. Data voidaan kerätä joko käyttämällä SL1 agenttia, data collectoria tai molempia. Tyypillisesti nämä data collectorit asennetaan collector grouppeihin, joka varmistaa datan keruun yhden noden kaatuessa normaalisti. Data collectori voi myös toimia messgae collectorina. (Sciencelogic integration service servicenow)

Message collection

Tämä SL1 laite käsittelee asynkronista syslog viestejä sekä trappeja valvottavilta laitteilta. Tämä osa voidaan asentaa minkä tahansa muun osan yhteyteen. Poikkeuksena hajautetut topologiat, jossa Message controllerin täytyy olla erillinen laite eikä Data collector / message collector. (Sciencelogic integration service servicenow)

3.3.2 SL1 Extended komponentit

Extended SL1 systeemissä on 4 peruskomponentin lisäksi 4 lisäkomponenttia, jotka tukevat SL1 agenttia ja tuovat lisää skaalautuvuutta ympäristöön. Huomioitavaa on, että näitä lisäkomponentteja ei voida käyttää aiemmin mainitussa All-In-One ratkaisussa, jossa kaikki neljä peruskomponenttia on asennettu yhdelle laitteelle. (Sciencelogic integration service servicenow)

Compute

Compute nodet ovat SL1 laitteita, jotka kuljettavat, prosessoivat ja käyttävät dataa data collectoreilta ja SL1 agenteilta. SL1 käyttää Dockeria ja Kubernetesia näiden servicien pystyttämisessä ja hallinnoimisessa. Seuraavat servicet käyttävät compute ominaisuutta hyväkseen:

Expanded agent capabilities toiminnolla tarkoitetaan tiedon viemistä compute clusterin kautta ja näin saadaan käyttöön laajempaa tiedon keruuta ja applikaatioiden monitorointia. Näin tehtynä agentti välittää tiedon.

Data pipeline toiminnolla voidaan siirtää ja samalla muuttaa dataa rikastamalla sitä metadatalla, kokoamalla dataa ja mallintamalla dataa hälytyksiä, sekä automaatiota varten. Data pipelinet käyttävät viestijonoja ja kommunikoivat käyttäen salattuja web servicejä.

Puplisher mahdollistaa SL1 sisältä kommunikoinnin esimerkiksi tietokannan kanssa, johon voidaan tallentaa kerättyä dataa tai lähettää sitä, vaikka muille käytössä oleville sovelluksille analysointia ja raportointia varten.

Graph database tallentaa dataa sovellusten suhteista toisiinsa sovelluksia ja infrastruktuuria varten. Tämän käyttö on tarpeellista, jos käytössä on SL1 kuvannus teknologiaa. (Sciencelogic integration service servicenow)

Load balancer

SL1 laite, jonka välittää compute clusterissa pyöriviä servicejä compute nodeille. Kaikille koneille klusterissa voidaan määrätä Kubernetesin avulla yksi tai useampia servicejä pyöritettäväksi. (Sciencelogic integration service servicenow)

Storage

SL1 extended mahdollistaa storage clusterien käytön, johon kuuluu useampia storage nodeja ja nämä tarjoavat NoSQLn vaihtoehdoksi ralaatio tietokannan rinnalle. Näin tekemällä saadaan hyvin skaalautuvia tietokantoja, koska tämä vähentää monimutkaisten suurien tietokantojen käytön tarvetta ja mahdollistaa datan säilömisen laajasti. (NoSQL explained)

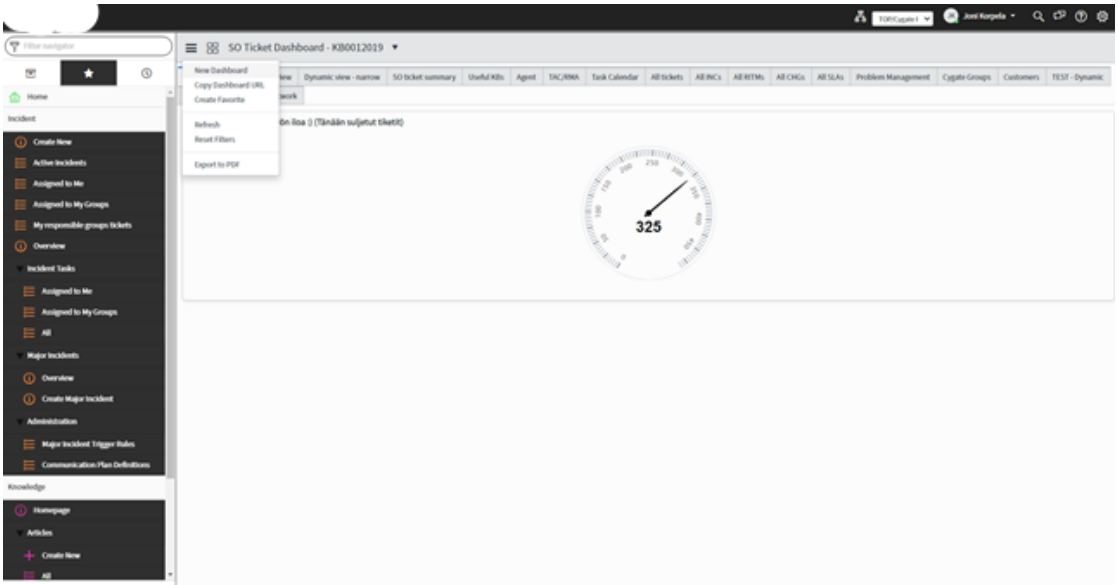
Management

Management nodella voidaan hallita ja päivittää compute clusterin nodeja, storage-nodeja ja kuormanjakajia. (Sciencelogic integration service servicenow)

3.4 Servicenow

Servicenow on työkalu johon SL1 kautta tehdyt tiketit tulevat näkymään. Tämä toimii myös kommunikaatio alustana asiakkaiden kanssa. Servicenow (Pulsar) työkaluun on rakennettu Knowledge base ohjetietokanta, josta työntekijät voivat helposti etsiä tietoa tiketeistä, ohjeista, ympäristön kuvauksista jne. Tämä on parempi vaihtoehto verrattuna Maximoon, jossa ei ole mahdollisuutta tehdä tämän tyyppisiä sivustoja. Perustoimenpiteet ovat kuitenkin vastaavia tiekttien käsittelyn osalta kuin maximossa. Yksi hyvistä ominaisuuksia etusivun suhteen on se, että se nostaa ylhäällä sijaitsevaan palkkiin 1 prioriteetin tiketit ja näin ne saavat huomion nopeasti. Myös SLA breach sarake on hyödyllinen erikoisuus Maximoon verrattuna.

Alla on kuva kirjautumissivun näkymästä, jossa voimme nähdä eri välilehtiä, joita on luotu eri tehtäviä varten sekä päivän aikana suljetut tiketit mittarin (Kuvio 10).



Kuvio 10. Servicenow

3.5 Flow designer

Flow designer on työkalu, jolla voidaan suunnitella ja luoda automaatio prosesseja. Tästä esimerkkinä on SL1 valvonnan hallinta työkaluun tulevien hälytysten nostaminen Pulsar (Servicenow) työkaluun.

Flow on automatisoitu prosessi, joka pitää sisällään triggerin ja tämän jälkeen tapahtuvat toimenpiteet. Subflow pitää sisällään automatisoidun jakson uudelleen käytettäviä actions, data input ja output toimenpiteitä. Ero Flow komponenttiin on, että subflow ei pidä sisällään triggeriä, vaan se etenee flown, subflown tai scriptin mukana.

Action on osa uudelleen käytettävää operaatiota, joka mahdollistaa Now Platform ominaisuuksien käyttämisen ilman koodaamista. Esimerkiksi Create Record toimenpide mahdollistaa process analystin luomaan merkinnän tauluun tietyillä muuttujilla, kun joku ehto täyttyy. Action step mahdollistaa taas taulun ja kenttien lisäämisen luonnin aikana. (Flow designer)

4 Monitoroinnin tyypit ja protokollat

On useita tapoja mitata verkon ja sen osien suorituskykyä. Network performance monitoring (NPM) käyttää, sekä aktiivista, että passiivista ja näiden sekoitusta antaakseen paremman kuvan verkon suorituskyvystä. Yleensä molemmat ovat käytössä, koska tämä antaa laajasti tietoa laitteista / suorituskyvystä ja mahdollisesti tarpeesta muutoksille, jotta vahinkoja voidaan ennaltaehkäistä. (Passive vs active)

4.1 Passiivinen valvonta

Passiivinen valvonta tarkastelee liikennettä sen ohi mennessä ja näitä voidaan asentaa niin kytkimille, reitittimille kuin hosteillekin. Esimerkkejä tämän tyyppisistä valvonnoista ovat Remote Monitoring (RMON), Simple Network Monitoring protocol (SNMP) ja netflow. Passiivisessa monitoroinnissa SNMP kohdalla laitteelle lähetetään tietyin väliajoin kyselyjä, jonka tulokset vastaanottava laite välittää Management Information Bases (MIB) tietokannasta kyselyn suorittaneelle laitteelle ja näin saadaan tietoa verkon suorituskyvystä ja tilasta. Hyötynä passiivisessa valvonnassa on, että tämä ei rasita verkkoa mittauksen ajankohdalla. Kuitenkin kerätty data, trapit ja hälytykset kaikki luonnollisesti luovat liikennettä verkkoon. Varsinkin kaikkien pakettien kaappaaminen liikenteestä on hyvin raskasta ja rasittaa verkkoa runsaasti. Kuitenkin vianetsinnässä tämä tapa antaa parhaat mahdollisuudet tarkkojen päätelmien tekemiseen. (Passive vs active)

Seuraavaksi tutustumme paremmin kahteen yleisimpään protokollaa (SNMP ja ICMP), mutta näiden lisäksi tunnettuja protokollia ovat myös CDP (Cisco discovery protocol), IPFIX (IP Flow Information Export), Sample Flow ja JFlow.

Simple network management protocol (SNMP)

SNMP on hyvin yleinen protokolla, jota käytetään datan hankkimiseen erilaisilta laitteilta, kuten kytkimet, kontrollerit, reitittimet, serverit ja muita verkossa olevia laitteita. SNMP soveltuu hyvin tiedonvälitykseen eri NMS (Network management systems) välillä ja hallinnan aplikaatioiden, sekä agenttien kesken verkossa. MIB pitää yllä objekteja yksilöidyillä tunnisteilla ja näillä voidaan hakea tarvittavaa informaatiota aina tarpeen vaatiessa. (Types of network monitoring protocols)

SNMP lähettää Protocol Data Unit (PDU) viestejä verkossa oleville laitteille, jotka ”puhuvat” SNMP:tä ja näitä kutsutaan SNMP get pyynnöiksi. Näillä get viesteillä hallintaa suorittava taho voi pitää silmällä kaikkea dataa mitä halutaan tarkkailla, kuten bittejä, paketteja, virheitä lähetyksessä / vastaanotossa, lähetys nopeutta laitteiden välillä jne. (SNMP basics what it and how it works)

Arkkitehtuuri koostuu hallittavasta laitteesta, agentista ja verkon hallinta asemasta. Hallittava laite voi olla kytkin, reititin, printteri jne. Hallittavalle laitteelle voidaan asentaa ja konfiguroida SNMP nodeja, joiden avulla kommunikointi onnistuu verkon muiden komponenttien kanssa. Agenttien avulla paikallisilta laitteilta saadaan kerättyä ja lähetettyä kerättyä dataa. Agentit ovat siis ohjelmia, joilla keräys ja tallennus suoritetaan. Hallinta asema toimii arkkitehtuurin juurena ja täällä tarjotaan tarvittava muisti ja prosessoriteho hallinnan suorittamiseen. (SNMP basics what it and how it works)

Käytännössä laitteilta siis saadaan SNMP avulla haluttua dataa ja saadulle datalle valvontaympäristössä annetaan raja-arvoja, jotka tuottavat hälytyksen, kun määritelty taso ylitetään tai alitetaan. Datan avulla hallintaa suorittava taho saa arvokasta tietoa ympäristön suorituskyvystä ja tämän avulla moninaisia ongelmia voidaan ratkaista.

Internet control message point ICMP

ICMP on suunniteltu erityisesti virheilmoitusten raportointiin. Verkkolaitteet käyttävät hyväkseen ICMP:tä virheilmoitusten lähettämisessä esimerkiksi yhteyden katketessa tai silloin kun pyydettyä informaatiota ei ole saatavilla. Toisin kuin SNMP niin ICMP ei osallistu tiedon välitykseen eri systeemien välillä. Valvontaa ICMPn avulla voidaan suorittaa mm. porttien, CPUn käytön, kaistan ja latenssin osalta. Verkkoprotokollana ICMP on olennainen osa monitorointia ja antaa nopeasti tarkan kuvan lähteestä ja sen sisältämistä virheistä verkon perustoiminnan osalta. (Types of network monitoring protocols)

Jotta ICMP protokollaa voidaan ymmärtää, niin täytyy tarkastella sen header kenttää (Kuvio 11), joka löytyy IP-otsikosta protokollanumerolla 1 tai 58 (ICMPv6).

	Bit 0–7	Bit 8–15	Bit 16–23	Bit 24–31
0	Type	Code	Checksum	
32	Header Information			

Kuvio 11. ICMP.

Ensimmäiset 8 bittiä kertovat ilmoituksen tyypin (type) kentässä ja tämä tieto taas voidaan tarkentaa code kentässä, joka on myös 8 bittinen. Checksum kentällä varmistetaan saadun tiedon oikeellisuus ja tämä seuraa viestin tyyppi kenttää. Tämä tapahtuu samalla tavalla kuin IP, UDP ja TCP protokollissa.

Koska ICMP käyttää 8 bittistä kenttää niin periaatteessa tämä mahdollistaa 256 erilaista viestiä, joista noin 40 on käytössä tällä hetkellä. Internet Assigned Numbers Authority (IANA) on vastuussa numeroiden varaamisesta. Alla (Kuvio 12) on lueteltu tärkeimpiä ja yleisimpiä pakettityyppejä.

Kaikkein tunnetuin ICMP käyttökohde lienee verkon ping toiminto, joka voidaan ajaa laitteiden komentokehotteesta / terminaalista. Ping lähettää IP paketin, joka pitää sisällään ICMP (v6) Echo Request, joka on tyyppiä 8 tai 128. Kun paketti on vastaanotettu niin laite vastaa lähettämällä ICMP Echo Request tyypillä 0 tai 129. Jos laite on tavoittamattomissa, niin viimeinen verkossa vastaava laite lähettää vastaus paketin.

Reitittimet käyttävät ICMP protokolla mainostamiseen (ICMP type 9 ja 134) ja nopeimman reitin valintaan (type 5 ja 137). ICMP lähettää tietyin väliajoin paketteja verkkoon, joiden avulla laite voi tehdä päätöksiä. (What is ICMP protocol and how does it work)

ICMP type	ICMPv6 type	Type name	Code	Description
3	129	Echo Reply		Test for presence by answering a network ping
	1	Destination Unreachable	0–15	An ICMP message that informs, among others things, the inaccessibility that specific components (network, protocol, port, host) in the field “code” have with routing problems or firewall blocking.
5	137	Redirect Message	0–3	Notifying the redirection of a packet for the specified network (0), the specified service and the network (2), or the specified service and host (3).
8	128	Echo Request		Network ping
9	134	Router Advertisement		Used by routers to communicate with different network clients.
11	3	Time Exceeded	0 oder 1	Status reports, that either report the lifespan (time to Live, TTL) of a packet (0), or the waiting time until the assembly of fragmented packets (1) has expired.
13	13	Timestamp		This provides the corresponding IP packet with a time stamp, which corresponds to the dispatch time and serves the synchronization of two computers.
14	-	Timestamp Reply		Response message an ICMP timestamp that the addressee sends after receiving one.
30	-	Traceroute		An outdated ICMP message type used to track the path of a data packet in the network: today, email requests and repetitions are mainly used for this purpose.

Kuvio 12. ICMP tyypit.

4.2 Aktiivinen valvonta

Aktiivinen valvonta käyttää hyödyksi testipaketteja, joita se lähettää verkkoon ja seuraa sen kulkua samalla mitaten saatujen palveluiden laatua. Koska liikenne ja parametrit ovat keinotekoisia niin se ei luo ylimääräistä liikennettä. Liikenteen kokoa ja parametreja voidaan säätää mielen mukaan, mutta jo pienillä määrillä voidaan saada mielekästä mittaus dataa. Hallinnoimalla erilaisia parametrejä kuten liikenteen muodostumista, näytteenottoa, ajoitusta, taajuutta, pakettien kokoa jne. voidaan emuloida hyvin erilaisia mahdollisia tilanteita ja näin testata esimerkiksi SLA ja Quality of Service (QoS) toimintaa käytännössä. (Passive vs active).

Vaikka aktiivinen monitorointi ei mittaa todellista liikennettä niin se voi silti antaa tärkeää dataa mahdollisten ongelmien syntymisestä ennen kuin ne näkyvät käyttäjällä. Proaktiivinen ote ongelmanratkaisussa onkin iso valtti palveluntarjoajan näkökulmasta. Mielessä aktiivisen monitoroinnin osalta täytyy pitää, että se ei anna 100% tarkkuudella tuloksia, varsinkaan jos mitataan useita verkon osia kerralla, mutta yksittäisistä parametreistä sillä saadaan hyviä tuloksia. (Active monitoring and passive monitoring whats the difference)

5 Valvonnan kohteita ja huomioita

Tässä luvussa käymme läpi eri laitteiden roolia ja niiden tärkeyttä palveluiden toiminnan kannalta sekä katsomme joitain vikatyyppejä ja niiden näkymistä hälytyksinä valvontaympäristöissä. Valvontoja asentavan henkilön tulee olla tietoinen asiakasympäristön vaatimuksista ja myös muokata niitä vastaamaan asiakassopimuksia. Valvottavia kohteita lisätään valvontojen piiriin aina sopimuksien mukaan ja näissä sopimuksissa myös määritellään, kuinka nopeasti tilanteisiin tulee reagoida sekä ongelmien ratkaisuajat.

Asiakaskohtaisia erikoisuuksia on niin verkon kuin palvelinten puolella. Hallinnointia suorittava tahon on aina tärkeää olla tietoinen valvottavan ympäristön erikoisuuksista, koska esimerkiksi pelkkä portti hälytys voi vaikuttaa suuresti yrityksen tuottavuuteen suuressa tuotantolaitoksessa tai prosessin jumiutuminen palvelimella katkaista tärkeän järjestelmän toiminnan ja aiheuttaa suuria vahinkoja tuottavuuteen yrityksessä. Tämän vuoksi prioriteettien määrittely ja asiakasympäristön erikoisuuksien tunteminen on oltava kunnossa. Tässä osassa on esitetty muutamia herkästi huomiotta jääviä asioita niin verkko kuin palvelin ympäristöistä ja arvioitu mahdollisia priorisointeja kokemuksen kautta.

5.1 Prioriteetit

Valvontaa suorittava taho hallitsee tapahtumia, palvelupyyntöjä, muutoksia jne. sopimuksissa olevien SLA aikojen mukaisesti. Korkean prioriteetin tapauksissa vasteajat ovat yleensä lyhyitä ja myös vaikutukset asiakkaan järjestelmiin näkyviä sekä tuotantoa haittaavia. Ison laitoksen pysähtyminen esimerkiksi kuudeksi tunniksi voi aiheuttaa merkittäviä rahallisia tappioita ja tämän vuoksi on äärimmäisen tärkeää varmistaa valvonnan toimivuus useiden käyttöönottotestauksien kautta, jotta voidaan varmistua hälytysten oikeanlaisesta aktivoinnista ja priorisoinnista sekä käsittelystä palvelua tarjoavan tahon puolesta. Tyypillisesti tuotantoon siirryttäessä hälytyksiä ja prosesseja testataan ennalta sopimattomilla testi vikatilanteilla, jolla varmistetaan oikeanlainen prosessien toiminta.

5.2 High availability HA

HA tarkoituksena on taata palvelun toiminta vikatilanteen sattuessa ja tavoiteltu operationaalinen aika on 99,999%, vaikkakin tämä on vaikea saavuttaa. Jotta 100% lukema saavutettaisiin, niin tarkoittaisi se sitä, ettei systeemi petä koskaan. Tämänkaltaisia verkko ja palvelinympäristöjä voidaan luoda, huolellisella suunnittelulla verkkojen, backup, failover ja tietokantojen osalta. (High availability)

Tyypillisesti yritysten verkko on kahdennettu tärkeimmistä kohdista, jolla varmistetaan palveluiden jatkuminen mahdollisten vikatilanteiden sattuessa. Laitteet voivat olla myös liitetty kahteen eri ISP verkkoon, jotta yhden Internet yhteyden tarjoajan vikaantuminen ei katkaise yhteyttä vaan voidaan siirtyä käyttämään varayhteyttä. Myös kriittiset palomuurit, reitittimet ja kytkimet ovat kahdennettuja yleensä ja näin yhden noden kaatuminen ei näy verkon käyttäjälle, mutta valvonnassa vika huomataan ja korjaavat toimenpiteet voidaan aloittaa välittömästi.

Hälytyksinä reitittimeltä HA voidaan havaita esimerkiksi BGP peer left established state tai portti hälytyksenä, jota saattaa myös seurata node unreachable hälytys vikaantuneelta laitteelta, jos nämä ovat molemmat valvonnassa.

5.3 Verkkolaitteet

Verkkolaitteet ovat olennainen osa jokaisen yrityksen työelämää ja tämän vuoksi asiakasvaikutukset ovat välittömiä ja tunteita herättäviä. Laitteiden tärkeyden tunnistaminen Netcool puolella on olennaista, jotta tapaukset saavat oikeanlaisen kohtelun. SL1 puolella tämä taas korostuu valvontojen asennuksen yhteydessä, koska toiminto on automatisoitu.

Valvontatyökaluilla on mahdollista nostaa kaikkea dataa valvonnan hallinnan näkymiin ja ongelma ei ole yleensä mitä voidaan valvoa vaan siinä mikä on olennaista dataa suoritettavien tehtävien ja sopimusten kannalta. Esimerkiksi Netcool työkalulla tämä voidaan havaita helposti, kun avataan live näkymä kaikesta datasta ja verrataan tätä hälytyshenkilönä toimivan henkilön käyttämään suodatettuun sisältöön.

Palomuurit

Palomuurit ovat hyvin kriittisiä laitteita valvonnan näkökulmasta ja näiden vikatiloilla on vakavia vaikutuksia ilman käytössä olevaa kahdennusta. Prioriteetilta tyypillisesti vikatilanteet ovat P1 tai P2 luokkaa riippuen toimipaikan koosta ja sen roolista verkossa.

Yleisiä hälytyksiä palomuureista valvontajärjestelmissä ovat HA tilamuutokset ja nämä tuleekin tutkia välittömästi ja päästä selvyyteen siitä, mikä on aiheuttanut aktiivisen muurin vaihdon. Syynä tilamuutokseen voi olla laitevika tai järjestelmän jumiutuminen korkean CPU / muistin käytön seurauksena ja näitä tyypillisesti seuraa, joko node unreachable tai korkeasta CPU / muistin käytön hälytys toiselta nodelta. Myös VPN tunnelit ovat yksi tyypillinen hälytysmuoto, jotka vaativat huomiota palomuurien osalta ja paikasta riippuen myös hyvin kriittisiä.

Reitittimet

Reitittimien availability hälytykset ovat kriittisiä verkon toiminnan kannalta ja ovat yleensä P2 tai P1 riippuen toimipaikasta.

Yleisimpiä hälytyksiä ovat porttihälytykset, kuten muillakin laitteilla, mutta esimerkiksi TenGigabitEthernet portit ovat yleensä hyvin tärkeitä liikennöinnin kannalta, ja näihin täytyy suhtautua isommalla vakavuudella, mitä kytkinten hälytyksiin. Reititykseen liittyvät hälytykset kuten BGP muutokset ovat myös kriittisiä ydin verkossa ja tyypillisesti ovat P2 tai P1 luokkaa, riippuen mikä naapuruus on kyseessä.

Erikoisuutena BGP hälyissä voi tulla vastaan Bogon BGP peer, joka tarkoittaa verkkoa, joka on varattu tiettyyn tarkoitukseen ja, jota ei olla vielä allokoitu asiakkaalle. Esimerkkejä IPv4 osoitteista voivat olla seuraavat:

- Private Networks (10.0.0.0 /8, 172.16.0.0 /12, and 192.168.0.0 /16)
- Loopback Addresses (127.0.0.0 /8, ::1 /128)
- Link-local Addresses (169.254.0.0 /16, FE80:: /10)
- Initialisation Addresses (0.0.0.0 /8)

Näiden osoitteiden lisäksi useat verkon blokit ovat allokoimatta palvelun tarjoajille tai loppukäyttäjille ja näitä listoja ylläpidetään IANAn ja RIR toimesta. (Bgp bogons and martians).

Kytkimet

Kytkinten hälytykset ovat P4, P3 tai P2 luokkaa, riippuen hyvin paljon ympäristöstä missä kytkin sijaitsee. Yleisimpiä hälytyksiä ovat porttihälytykset tai node unreachable. Myös kytkimissä on TenGigabitEthernet portteja ja tämä yleensä viittaa tärkeään yhteyteen, koska liikenteen mahdollinen kapasiteetti on korkea.

Hälytys näkymästä voidaan hyvin seurata esimerkiksi kirjautumisia laitteelle, porttimuutoksia, VLAN muutoksia jne.

Access Point

Asiakkaiden yhteydet muodostuvat WLAN ympäristössä AP kautta ja nämä ovat loppukäyttäjälle tärkeitä yhteydenmuodostuksen kannalta. Prioriteetiltaan AP hälytykset ovat P4 tai P3 luokkaa, koska vaikutus on yleensä pieni ja kohdistuu vain muutamaan käyttäjään. Yleensä tiloissa on useita tukiasemia ja tämän vuoksi yhden tippuminen verkosta ei katkaise yhteyttä kuin tietyltä osalta rakennusta.

5.4 Palvelimet

Palvelimien hälytyksien skaala on huomattavasti runsaampi ja vaikeampia tunnistaa, koska valvottavia prosesseja on miltei loputon määrä.

Yleisimpiä hälytyksiä palvelimista ovat CPU, fyysinen ja swap muistit ja levytilat. Edellä mainittujen hälytysten kanssa on aina tarkistettava mistä kyseinen hälytys on peräisin ja onko kyseessä esimerkiksi klusteri, hosti vai pelkästään palvelin. Yleensä näiden tunnistamiseen on kaikissa ympäristöissä oma nimi politiikka ja se tekee tunnistamisesta vaikeaa, jos tietty asiakkaan ympäristö ei ole ennalta tuttu.

Esimerkiksi Netcool valvontaan tulevat hälytykset toimivat robottien avulla, jotka välittävät tietoa palvelimen erilaisista valvottavista kohteista. Jos yhteys robottiin katkeaa, syntyy Node unreachable hälytys robotista ja nämä on aina tarkistettava nopeasti, jotta palvelimen tila saadaan tietoon. Monesti kyseiset hälytykset ovat peräisin robotin jumiutumisesta, joka korjaantuu servicen uudelleen käynnistämisellä.

5.5 Backups

Isoa roolia HA hallinnassa näyttelee varmuuskopioiden ylläpito. Esimerkiksi päivityksiä tai muita järjestelmään kohdistuvia isoja muutoksia varten tulee varmistua siitä, että voidaan järjestelmä palauttaa toimivaan tilaan nopeasti. Tämä takaa hallitun muutosten tekemisen ja turvaa palveluiden saatavuuden.

Suurimmassa osassa palvelimista ja tietokannnoista backupit otetaan päivittäin, mutta esimerkiksi verkkolaitteiden backupit on tarvetta ladata esimerkiksi watchereille vain ennen uusien päivityksien aloittamista. Epäonnistuneista backupeista syntyy hälytyksiä ja näiden tarkistaminen ja uudelleen ajaminen täytyy suorittaa uudelleen, jos esimerkiksi automatisoitu toiminto ei mene läpi. Tärkeydeltään backupit ovat P3 – P1 tasoa riippuen hyvin paljon laitteen roolista ja sen sisältämästä tiedosta.

5.6 Konesalit

Konesalin hälytykset ovat lähtökohtaisesti P1 – P2 tasoa, vaikka kyse olisi vain porttihälytyksestä ja yleensä portit ovat TenGigabitEthernet portteja.

Klusterit, hostit ja storaget ovat prioriteetiltaan P1 hälytyksiä, koska niiden vikatilanteiden vaikutus ulottuu laajalle. Klusterissa voi olla esimerkiksi 4 hostia ja hostilla 100 virtuaalikonetta ja jokaisella virtuaalikoneella kriittisiä tehtäviä yrityksen eri toimintojen kannalta. Kaikki nämä voivat käyttää vain muutamaa storagea tehden myös levyistä erittäin kriittisiä toimintojen kannalta.

SL1 soveltuu erityisen hyvin konesaliympäristöjen nopeaan vianselvitykseen tarjoamalla laajasti dataa hallintapaneelissa verrattuna Netcool ympäristöön. Esimerkiksi valvottavia logi tietoja voidaan lukea suoraan event välilehdeltä ja näitä saadaan myös graafeiksi näkymään eri ajanjaksoilta.

6 Vertailun tulokset

Valvontajärjestelmät ovat ydin asemassa palveluntarjoajan näkökulmasta, ja niihin liittyvät toiminteet tärkeitä ymmärtää kaikkien tuotannossa mukana olevien henkilöiden toimesta. ITIL antaa hyvän perus, ymmärryksen käsitteistä ja toimimisesta palveluntarjoajan sekä asiakkaan välillä.

Molemmat valvontajärjestelmät ovat osoittautuneet toimiviksi systeemeiksi tuotannossa ja näiden avulla on suoritettu menestyneesti valvontaa. Erot ovat kuitenkin selviä niin hälytys, kuin hallintajärjestelmän osalta. Tulevaisuus näyttää kuinka paljon automatisointia voidaan hyödyntää mielekkäästi ja toimivasti tuotannossa, mutta tie näyttää kuitenkin lupaavalta. Servicenow on kommunikointi alustana parempi, kuin Maximo ja asiakkaiden pääsy tiketeille helpottaa kaikkien kannalta ongelmien nopeaa käsittelyä. Maximon puolella vain osa asiakkuuksista on integroitu järjestelmään, ja tilapäivitykset menevät monilta osin vain sähköpostin välityksellä.

6.1 Vertailua käytännön toiminteista

Suurin ero Netcool ja SL1 välillä on, että SL1 on paljon pidemmällä automatisoinnin osalta. Käytännössä Netcool sekä Sciencelogic ottavat vastaan tietoja valvottavilta kohteilta ja nostavat näistä ennalta määriteltyjä ilmoituksia hälytysnäkymään. Hälytysnäkymästä Netcoolissa tiketöinti tapahtuu manuaalisesti, kun taas ScienceLogic avaa tiketin automaattisesti heti tapahtuman sattuessa. Manuaalinen käsittely vaatii aina osaavan henkilön, jolla on pääsy kaikkiin valvottaviin kohteisiin. Näin tehtynä työ on hyvin tarkkaa, koska vikatilanteet voidaan esikäsitellä ja tiketeille päivittää lisäinformaatiota tapahtumasta. Myös korkean prioriteetin hälytykset ohjautuvat helposti oikealle asiantuntijalle, kun henkilö hoitaa hälytysten luontia ja voi samalla eskaloida tehtyjä tikettejä. Automaation kautta tulevat tapahtumat taas tulevat, kun jokin tietty hälytyksen parametri on täyttynyt ja tästä avautuu tiketti. Tämän järjestelmän hyödyllisyys on siinä, että järjestelmä osaa myös sulkea tiketin, jos vikatilanne on mennyt ohi. SL1 osalla onkin erityisen tärkeää olla valvontoja asentaessa tietoinen laitteiden ja sen hälytysten prioriteetista ja näin vaikutuksesta ympäristöön.

Sulkumekanismi on myös yksi järjestelmän haittapuolista tällä hetkellä, koska tiketit menevät kiinni, vaikka tapaus on vielä osittain käsittelemättä. Esimerkkinä tällaisista ovat flappäävän portin tiketit tai palvelimen resurssien käyttö, joissa tiketille on merkitty tutkitut asiat ja laitettu jonoon odottamaan toimenpiteitä. Kun SL1 vaihtaa tiketin tilan resolved niin tämä toimenpide nollaa samalla responsible groupin.

Servicenow on osoittautunut varsin käteväksi siinä, että sillä voidaan luoda flow kuvioita tyypillisimmistä tehtävistä, kuten palvelimen luonti, levyn, muistin, CPUn jne. lisäys. Asiakas voikin erillisien sivuston kautta käydä suoraan itse tekemässä tarvittavia lisäyksiä perustoimenpiteiden osalta ja tämä vähentää palvelutarjoajan työkuormaa huomattavasti. Toisaalta taas automaation vaatii runsaasti huomiota alussa, jotta erilaiset ongelmatilanteet ja poikkeukset voidaan ohittaa ilman käsityötä. Tämä vaatii runsaasti muuttujien luontia, jotta yksinkertaisen kuuloinen toimenpide saadaan suoritettu automaattisesti.

Maximossa ei ole sisäänrakennettua mahdollisuutta pitää yllä wikipedioita, mutta Servicenow tarjoaa tälle hyvän alustan, ja tämä on osoittautunut erinomaiseksi ominaisuudeksi. Hakutoiminnolla löydetään yhdellä haulla sekä aiemmat tiketit, kuin siihen liittyvä dokumentaatio.

Ongelma SL1 puolella on myös tikettien ryhmittely. Netcool puolella käsin tehtynä tiketille voidaan lisätä hälytyksiä ja muokata otsikko käsin vastaamaan tilannetta. Esimerkiksi kun toimipaikka menee alas ja siellä on palomuuri, kaksi reititintä, 3 kytkintä ja 10 tukiasemaa niin Netcool puolella voidaan luoda palomuurista tiketti ja lisätä kaikki muut hälytykset tiketille ja lisätä otsikkoon SiteDown. Kun sama tapahtuu SL1 puolella niin syntyy pahimmillaan 16 erillistä tikettiä. Tämä on yksi suurimmista pullonkauloista käytännön operoinnin kannalta tällä hetkellä.

Sciencelogic tarjoaa ympäristönä laajempia mahdollisuuksia automatisoinnin osa-alueella ja tämä onkin yksi syistä, jonka vuoksi muutosta ollaan suorittamassa. Automaation astetta on mahdollista ottaa käyttöön hyvin laajasti, mutta kehittäminen niiden osalta on paljon resursseja, sekä aikaa vievää.

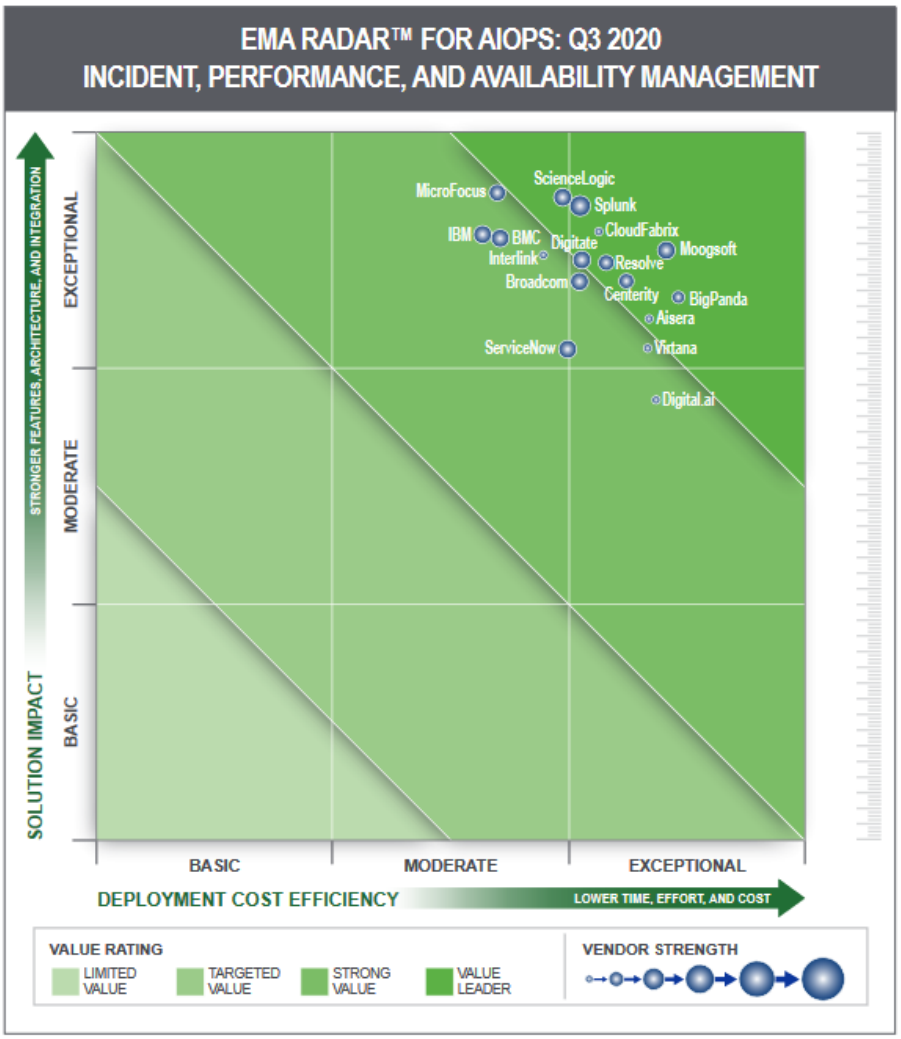
6.2 Mitä järjestelmistä puhutaan

Sekä Netcool/OMNIbus, että ScienceLogic järjestelmää käytetään ITSM alustana ja molemmat järjestelmät ovat käytössä useilla isoilla valvontaa suorittavilla toimijoilla.

Alla kuvassa (Kuvio 11) näemme EMA Radar for AIOPS: Q3 2020 vertailua kolmesta tärkeästä osa-alueesta: incident, performance ja availability managment. Molemmat pärjäsivät vertailussa erinomaisesti ollen 5 parhaan joukossa 17 verrokista suorituksen puolesta, mutta kustannuksiltaan molemmat sijoittuivat 6 kalleimman joukkoon.

Kyseisessä artikkelissa ScienceLogic saa kehuja mukautuvasta AIOPs alustastaan ja siihen saatavilla olevista ominaisuuksista. Yksi tärkeimmistä vahvuuksista on myös sen IT tuotannolle tarvittavan ylhäältä-alas näkyvyyden tarjoaminen. Sen kehutaan myös olevan vertailun yksi arvojohtajista Incident, performance, availability, change impact, capacity optimization osa-alueilla (Kuvio 13).

Artikkelissa IBM puolelta AIOPs arvioinnissa on erilliset Netcool työkalut IBM netcool OPs manager ja IBM telco network cloud manager. Kehuja IBM saa siitä, että se on viime vuosina onnistunut kehittämään automaatio, visualisointi ja koneoppimis työkalujaan uusien investointien ansiosta. (EMA-AIOps-2020-RRSUMMARY)



Kuvio 13. EMA radar.

7 Pohdinta

Aiheena valvontaympäristön hallinta on erittäin laaja aihe ja varsinkin tekniseen puoleen syvä sukeltaminen vaatisi oman kirjan tekemisen, koska huomioon otettavia asioita ja muuttujia on niin paljon käytännön toteutuksien ja konfigurointien kannalta. Hankaluutena aiheessa on ollut rajaaminen mielekkääksi kokonaisuudeksi ja vastaamaan silti alkuperäistä tavoitetta luoda kokonaiskuvaa valvontaympäristöistä teknisestä ja hallinnallisesta näkökulmasta.

Molemmat valvontaympäristöt ovat osoittautuneet toimiviksi ratkaisuksi, mutta Netcool edustaa silti yrityksessä niin sanottua vanhaa tuotantoa ja tulevaisuudessa siirtyminen tapahtuu kokonaan SL1 valvontojen piiriin, jossa automaatio on useissa toimenpiteissä osana arkea. Netcool valvonnanhallinta ja Maximo tiketti järjestelmä ovat olleet pitkään käytössä yrityksessä ja tämän vuoksi ne ovat myös hyvin hiottuja erilaisiin tarpeisiin. Myös klassinen taistelu Netcoolin ”hälymiehen” ja SL1 automatisoinnin välillä käy kuumana, mutta kehityksen myötä SL1 tulee tämän taiston vielä voittamaan, vaikka hälymiehellä on yhä tärkeä rooli niin kauan, kun Netcoolissa on valvottavia laitteita.

Valvontaympäristöjen hallintaan liittyy useita toimenpiteitä, joita täytyy jatkuvasti suorittaa, kun palveluita kehitetään, lisätään, poistetaan ja muokataan erilaisten sopimusten puitteissa. Asiakkaan ympäristön tarkka tunteminen on pääasemassa kaikissa vaiheissa ja on kriittistä varsinkin valvontojen asennuksen yhteydessä, koska prioriteettien on vastattava ympäristön tärkeyttä. Sopimukset ja sen sisältämät palvelun vaatimukset määrittelevät hyvin pitkälle valvonnan toteutumista ja sen pohjalta suunnitellaan valvonnat vastaamaan sovittuja päämääriä ja palvelun eri tasoja.

Lähteet

Active monitoring and passive monitoring whats the difference. N.d. Solutionsreview.com verkkosivulta. Viitattu 15.4.2021. https://solutionsreview.com/network-monitoring/active-monitoring-and-passive-monitoring-whats-the-difference/

Bgp bogons and martians. N.d. Networkdirection verkkosivulta. Viitattu 15.4.2021. https://networkdirection.net/articles/routingandswitching/bgp-bogonsandmartians/

Ema radar. N.d. sciencelogic.com verkkosivulta. Viitattu 15.4.2021. https://sciencelogic.com/product/resources/ema-radar

EMA-AIOps-2020-RRSUMMARY. N.d. irp-cdn.multiscreensite.com verkkosivulta. Viitattu 15.4.2021. https://irp-cdn.multiscreensite.com/3696c7a5/files/uploaded/EMA-AIOps-2020-RRSUMMARY-Interlink%20SW.pdf

Flow designer. N.d. Sercinow.com verkkosivulta. Viitattu 15.4.2021. https://docs.servicenow.com/bundle/quebec-servicenow-platform/page/administer/flow-designer/concept/flow-designer.html

High availability. N.d. searchdatacenter.techtarget.com verkkosivulta. Viitattu 15.4.2021. https://searchdatacenter.techtarget.com/definition/high-availability

Infrastructure monitoring tools. N.d. Dnsstuff verkkovisulta. Viitattu 15.4.2021. https://www.dnsstuff.com/infrastructure-monitoring-tools

In memory. N.d. aws.amazon.com verkkosivulta. Viitattu 15.4.2021. https://aws.amazon.com/nosql/in-memory/

ITIL methodology. N.d. chernwell.com verkkosivulta. Viitattu 15.4.2021. https://www.cherwell.com/it-service-management/library/blog/itil-methodology/

Jouravlev, R., Anand, A., Orbezo, J., Casteel, E., Corona, M., DuMoulin, T., Hearsum, P., Hunnebeck, L., Leach, M., Rae, B., Rance, S., Yagi, T., Macdermind, K., 2019. ITIL Axelos – ITIL foundation 4 edition-Axelos 2019. Viitattu 15.4.2021. https://fliphtml5.com/ensds/cphj/basic

NoSQL explained. N.d. mongodb.com verkkosivulta. Viitattu 15.4.2021. https://www.mongodb.com/nosql-explained

Passive vs active. N.d. Slac.stanford.edu verkkosivulta. Viitattu 15.4.2021. https://www.slac.stanford.edu/comp/net/wan-mon/passive-vs-active.html

Sciencelogic integration service servicenow. N.d. Sciencelogic.com verkkosivulta. Viitattu 15.4.2021. https://docs.sciencelogic.com/pdf/sciencelogic_integration_service_servicenow_2-4-0.pdf

Sciencelogic. N.d. percona.com verkkosivulta. Viitattu 15.4.2021. https://www.percona.com/about-percona/case-studies/sciencelogic

SLA template examples. N.d. bmc.com verkkosivulta. Viitattu 15.4.2021 https://www.bmc.com/blogs/sla-template-examples/

SNMP basics what it and how it works. N.d. Helpsystems.com verkkosivulta. Viitattu 30.4.2021. https://www.helpsystems.com/resources/articles/snmp-basics-what-it-and-how-it-works

Types of network monitoring protocols. N.d. liveaction.com-verkkosivu. Viitattu 15.4.2021. https://www.liveaction.com/blog/types-of-network-monitoring-protocols/

Tivoli Netcool / OMNIbus components. N.d. IBM.com verkkosivulta. Viitattu 15.4.2021. https://www.ibm.com/support/knowledgecenter/es/SSNFET_9.2.0/com.ibm.netcool_OMNIbus.doc_7.4.0/omnibus/wip/user/concept/omn_ovr_theobjectserver.html

What is ICMP protocol and how does it work. N.d. Ionos.com verkkosivulta. Viitattu 30.4.2021. https://www.ionos.com/digitalguide/server/know-how/what-is-icmp-protocol-and-how-does-it-work/